|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name of malware | Basic Static | Basic Dynamic | Advanced Static | Advanced Dynamic |
| Ryuk Ransomware | ✔ (mabel) | ✔ (edward) | ✔ (edward) | Failed(mabel) |
| Dm.exe | ✔(edward) | Failed(mabel) | ✔(mabel) |  |
| Keylogger |  | ✔(mabel) |  |  |

# 1. Lab Setup

As analyzing malware can be very dangerous and there is a chance it might result in potential unwanted results, we have decided to make use of virtual machines to help us with our malware analysis. A virtual machine is considered a safe space for us to perform our analysis as whatever happens in the VM stays in the VM and it will not affect our host machine.

## 1.1. VMware Setup

Our VM setup is VMware Workstation 16 Pro, version 16.2.2 build-19200509. We will be installing two Operating Systems to perform our analysis, Windows 8 & Windows XP.

## 1.2. Network Diagram

Both guest machines are configured as shown below. Both systems will be configured to use the host-only mode in Vmware Workstation. This is to ensure that both the VMs won't be able to access the internet. This configuration also meant that the two VMs will only be able to communicate within their own network. This is to ensure that the malware is contained in the virtual environment and will not have any chance of spreading out.

## Diagram Description automatically generated

## 1.3. Network Configuration

As mentioned below, the two guest virtual machines will be configured to use the host-only mode. It will be connected to VMnet1, which is the Host-only Network. The guest machines will receive a private IP address from the VMware Workstations DHCP server. This Private IP address does not allow both the virtual machines to be able to connect to the internet.

A screenshot of a computer

Description automatically generated

Windows 8

Text

Description automatically generated

Windows XP

Text

Description automatically generated

In the pictures above, both Machines have been assigned a Private IP address from VMware Workstation’s DHCP Server.

# 2. Malware Analysis Tools

## 2.1. Basic Static Tools

### 2.1.1. WinMD5

MD5 is a small and easy tool that can be used to calculate the MD5 hash of a file. This tool works easily by dragging and dropping the file that we want to check the hash value for, into the tool. This tool will also allow us to check if the malware that we are analysing is the correct one, as we can then compare the hash value of the downloaded malware file to the original hash value of the malware file.

Table

Description automatically generated

### 2.1.2. PEiD

PEiD is an intuitive application that is used to detect most common portable executable (PE) packers, cryptors and compilers found in packed or encrypted PE files. It can also be used to detect more than 470 forms of different signatures in a PE file.

In the main interface, we can view the different information about a file by dragging and dropping the file into this PEiD tool. We can see some basic information such as, the EP section, compiler used, and indications whether if the file is packed or not from the compiler section which is the “Nothing found [Overlay]\*” field.

Graphical user interface, application, Word

Description automatically generated

Next, under the “EP Section”, we are also able to view the virtual and raw size of the file. This will be able to help us identify whether a file is packed or not.

Graphical user interface

Description automatically generated

Next, under the “First Bytes” section, we have the PE disassembler and we are able to view the assembly codes of the file.

Disassemblers are used to translate machine code into human readable format and aims to recreate a compiled high-level language program from machine code to its original format.

Different disassemblers also produce different results, thus, it is good to analyse assembly codes by making use of multiple different disassemblers.

Graphical user interface, text, application

Description automatically generated

Next, we have the menu, which will be able to give us more information as well on whether the file is a packed one or not. We can click on the “Normal Scan”, “Deep Scan” and “Hardcore Scan” to help us determine if a file is packed. This is because, if the file was a packed one, by going through all the scans, the compiler section which is the “Nothing found [Overlay] \*” field, could change to a common packers’ name, thus indicating that it is a packed file.

A screenshot of a computer

Description automatically generated with medium confidence

### 2.1.3. PEview

PEView refers to a viewer for portable executable (PE) files. It is a simple and compact lightweight program that views 32 or 64 bit portable executable files, showing headers and other basic information of a portable executable.

From this PEView, we are also able to get information such as, the date and time for when the file was created and more.

Text

Description automatically generated with medium confidence

Table

Description automatically generated

### 2.1.4. Dependency Walker

Dependency walker is a free program for Microsoft Windows that is used to list all imported and exported functions of a portable executable file. It is also able to display a recursive tree of all of the dependencies of the portable executable file. With dependency walker, we are then better able to analyse the portable executable file and better understand what the malware might be trying to do based on the different import libraries and API calls.

Graphical user interface, application, Word

Description automatically generated

### 2.1.5. BinText

BinText is a small, fast and powerful text extractor that can find Ascii, Unicode and Resource strings in a file. It is also able to allow us to view the different strings that exist in a portable executable file including the API calls made by the portable executable file.

Graphical user interface, text, application

Description automatically generated

## 2.2 Basic Dynamic Tools

### 2.2.1 ApateDNS

ApateDNS is an open source Graphical-User-Interface (GUI) tool that can be used to control the DNS responses. It spoofs DNS responses to a user-specified IP address by listening on UDP port 53 on the local machine. ApateDNS allows us to view the network connections the malware makes when it is executed in the system. Although, there may be some indication of these network connections shown in basic static analysis, using ApateDNS can allow us to verify that the malware is attempting to connect to the IP addresses or hostnames that were identified. It also allows us to discover additional network connections made. Thus, ApateDNS can be used as an effective method to locate network-based indicators for the malware.

Graphical user interface, text, application, email

Description automatically generated

In order to properly use ApateDNS, it is needed for the system to have a manually configured DNS server address. For the DNS server address, it was set to have an ip address of 127.0.0.1, which is also known as the loopback address or localhost. This can be done by going to “Internet Protocol Properties” in the “Control Panel”. With this DNS server address set, ApateDNS can detect and capture all network connections being made by the system.

Graphical user interface, text, application, email

Description automatically generated

### 2.2.2 Process Explorer

Process Explorer is a tool developed by Windows SysInternals. It is used to view all running processes on the systems and displays information about the handles and DLLs for each process. Process Explorer is a useful tool in identifying the activities of the malware as we can see what processes are activated and terminated when the malware is runned. This can be a tool used to help us gain a better understanding of the malware and should be used for basic dynamic analysis.

Graphical user interface, table

Description automatically generated

### 2.2.3 Process Monitor

Process Monitor is also a tool that is developed by Windows SysInternals. It is an advanced monitoring tool that shows live file system, registry and process activity. It combines two SysInternals utilities, Filemon and Regmon, together and provides additional features that will be useful in identifying the activities of the malware. Process monitor can be very useful, especially since it provides non-destructive filtering of data. It captures all data but users can filter the data according to information such as Process ID and Process Name. This allows the users to view only the activity of the malware which can be useful in identifying system changes made by the malware.

Graphical user interface, table

Description automatically generated

### 2.2.4 Regshot

Regshot is an open source registry compare utility that allows users to monitor for system changes. Regshot works by firstly taking a snapshot of the original registries and files on the system. Then after the malware is runned, a second snapshot can be taken. This allows for a comparison to be made for the first snapshot and second snapshot, which then allows malware analysts to identify changes made to the registries and files on the system. This tool is extremely important to use as the results made from Regshot usually allows one to gain some insight into what the malware is trying to achieve and its functionality.

Graphical user interface, application

Description automatically generated

### 2.2.5 Netcat

Netcat is an utility program that supports a wide range of commands to manage networks and monitor traffic flow between systems. It is able to perform many activities such as port listening, port scanning, transferring files and can create a web server. For malware analysis, port listening can be very useful as it can help detect what TCP/UDP connections are being made by the malware. Thus, netcat will be listening on port 80 and port 443 as these are the ports which will be used by the system to make a connection to external networks. If a connection is made by the malware, the details of the connection will be shown in the command prompt.

Text

Description automatically generated

### 2.2.6 Wireshark

Wireshark is a popular open source network protocol analyser. It has many features such as troubleshooting networks, tracing connections and network analysis. Wireshark allows users to see what is happening on the network in real-time which can prove to be useful in detecting network connections made by the malware. Thus, wireshark can be used to identify network-based indicators of the malware and can also be used to track all connections the malware made.

Graphical user interface, text, application, table, Excel

Description automatically generated

## 2.3 Advanced Static Tools

### 2.3.1 IDA Pro

Interactive Disassmbler Professional (IDA pro) is usually used to analyse nefarious programs. It is a disassembler that is capable of creating maps of their execution to show the binary instructions that are executed by the processor in assembly language. It has multiple uses such as malware and vulnerability analyses, debugging and for reverse engineering. It also supports a wide variety of file formats such as Portable Executable (PE), Common Object File Format (COFF) and Executable and Linking Format(ELF). IDA Pro also uses code signatures in Fast Library Identification and Recognition Technoloy (FLIRT) which means that it can recognise and label disassembled functions accurately. IDA Pro has many types of interface and windows that help aid the analysis of the program. It has a text interface, which shows function names, comments, and subroutine numbers.

Graphical user interface, text, application

Description automatically generated

It also has a graph interface, which shows the assembly language used in each jump location. From there, malware analysts are able to see what the malware is doing as they can see the function calls the malware makes. If the malware analysts are proficient in assembly language as well, the malware analysts can have a better and clearer understanding of what the malware is trying to do.

Graphical user interface, text

Description automatically generated

There are useful window tabs that IDA Pro provides to help with analysts. These window tabs are the “Functions Tab”, “Names Tab”, “Strings Tab”, “Imports Tab”, and “Exports Tab”. The functions tab lists all functions in .exe and the length of the function. The names tab lists every address,including functions, named code and data, and strings, with a name. The strings tab shows all strings which are longer than five. The imports tab shows the list of all imported functions and can easily allow users to locate these functions in use. The export tabs show the list of all exported functions and can allow users to locate these functions in use easily.

Graphical user interface, application

Description automatically generated

## 2.4. Advanced Dynamic Tools

### 2.4.1. OllyDbg

OllyDbg is an x86 debugger that emphasises on binary code analysis. This tool is extremely useful for when the source code is not available as it is able to trace registers, recognise procedures, API calls, switches, constants, strings, and more. It is even able to locate routines from object files and libraries. This tool can also be used to evaluate and debug malware.

A picture containing text

Description automatically generated

It can then be used to step out, step over and more, where we can specify how we want the malware to run. Ollydbg has the ability to debug multithread algorithms and attach to running programs. It provides malware analysers a safe space to run the malware without infecting the host system. In order to help with the debugging of the malware, breakpoints can be set to examine the values of the variables in the code so as to help make users better understand what the malware is doing. Ollydbg supports many types of breakpoints such as conditional, logging, memory and hardware breakpoints. It also traces program execution and logs arguments of known functions so as to aid in the debugging process.