INTRODUCTION TO MALWARE ANALYSIS

PREPARED FOR BEGINNERS

LetsDefend

TABLE OF CONTENTS

MALWARE AND MALWARE TYPES

Malware is a word derived from the words MALicious SofWARE. Software that targets a malicious purpose that will harm the integrity and safety of the system is called malware.

Today, cyber threat actors use complex malware. These types of malicious software contain techniques that make analysis difficult.

MALWARE TYPES

Malware is divided into many types according to their characteristics / behaviors. As a result of the analysis, the type of malware is determined by taking the capabilities of the malware into consideration.

Some types of malware and their descriptions are below:

- **Backdoor**: Leaving a backdoor on the device where the malware is installed, it allows the attacker to access the system through this backdoor. For example, by opening a network port connected to the shell, it enables the attacker to connect to the system through this port.

- **Adware**: It often comes with downloaded software, causing unwanted advertisements to be displayed on the device. While not all adware is harmful, some change the default search engine.

- **Ransomware**: It is a type of malware that has been on the world agenda for the last few years. It demands ransom from people by encrypting and exfiltrating all files on the device.

MALWARE TYPES

- **Worm:** Since this type of malware spreads from infected devices to other devices, it is named worm. WannaCry, a worm malware exploiting MS17-010 vulnerability, caused panic around the world

- **Rootkit:** It is a type of malware that disguises itself by providing access to a high level of authority on the device.

- **RAT (Remote Access Trojan):** It is a type of malware that provides full control over the device to the threat actor.

- **Banking malware:** A type of malware that targets banking applications and causes money to be stolen from the victim.

A malware may contain more than one feature, so a malware can belong to more than one type. For example, WannaCry malware includes both worm and ransomware malware features.

VIRTUAL MACHINES

You do not want to analyze malware on the device where all our personal files and data are stored. For this reason, we need isolated devices for malware analysis.

You can install a virtual operating system inside your own device using virtualization softwares. In this way, you can create your isolated system without the need to purchase a physical device.

There are several virtualization environments that you can use for a fee or for free. The most popular of these are VMware Workstation by VMware and VirtualBox by Oracle company. Both virtualization softwares will meet your needs for analyzing malware.

There are some disadvantages of using the virtualization softwares.

- The virtual operating system you will install will not work as well as a physical computer since it runs on your main operating system.
- Since virtualization softwares are also software, vulnerabilities may arise in these softwares. A malware that exploits these vulnerabilities can escape from the virtual environment and infect your main operating system. For this reason, you may want to keep your virtualization software constantly updated!
- In order for virtualization software to work, it needs to install its own drivers into virtual operating systems and create various configuration files / registries. Malware can make analysis difficult by checking such indicators and checking whether it works in a virtual environment.

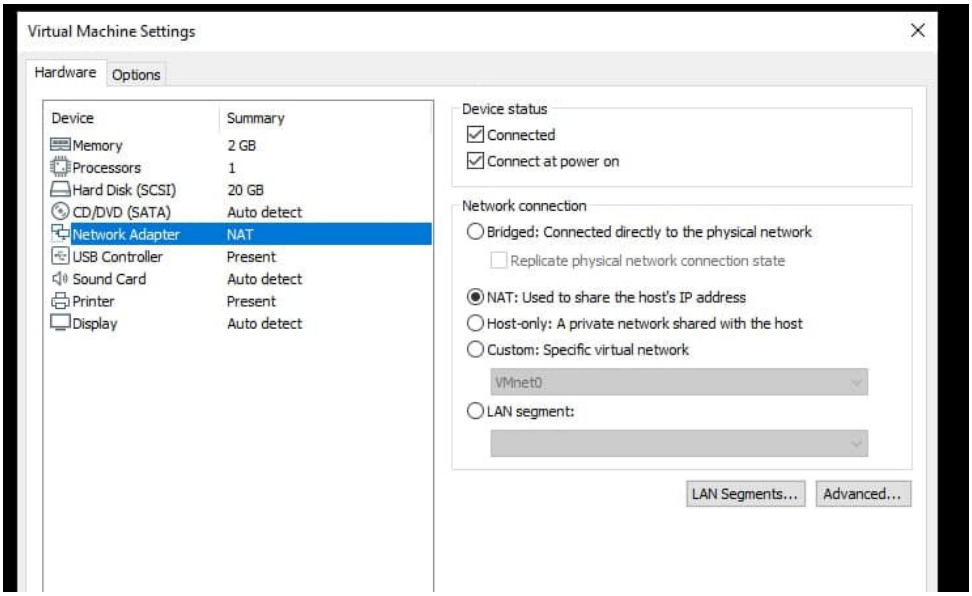
We will use the VMware Workstation product in this tutorial. Some features may differ.

ADJUSTING VIRTUAL MACHINE

You should make the virtual operating system suitable for malware analysis, otherwise the malware can infect other devices in the same network.

1) Network Settings

In order to prevent the malware that we will analyze from infecting other devices on the network, we must change the network settings of the operating system we have installed from the virtualization software. We have to enter the "Network" settings from the settings section and select the "Custom" option here.



- **NAT:** Allows you to access the Internet through the network interface of your physical device.
- **Bridge:** Allows you to access the internet by obtaining its own IP address from your modem like your physical device.
- **Custom:** It is included in the private network created by the virtualization environment. Internet access is not available in this option.

In order to prevent the malware we will run from spreading to other devices in the network, we must restrict the network access of our virtual operating system, so we should choose the "Custom" option.

ADJUSTING VIRTUAL MACHINE

2) Disable Anti-Virus Software

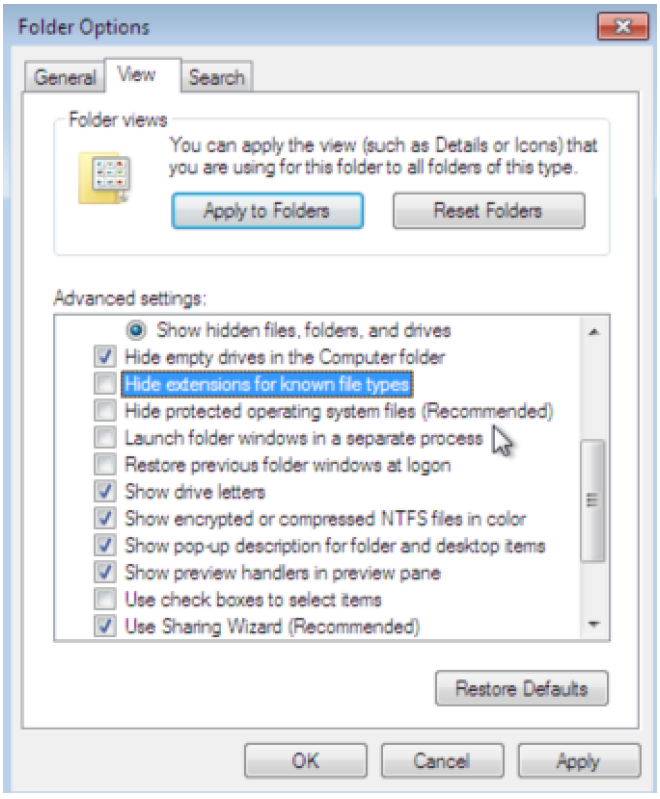
We need to disable anti-virus software to prevent anti-virus software from interfering to our analysis by blocking or removing the malware we want to analyze.

3) Disable Updates

Malware may be exploiting various vulnerabilities. During our dynamic analysis, we must prevent our virtual operating system from receiving security updates so that the malware can successfully exploit such vulnerabilities and continue to run. For this reason, we must disable the automatic update option of our operating system.

4) Disable Hidden Extensions

By default, known file extensions are hidden in the Windows operating system. We need to disable this feature in order to see the exact name of the file we want to analyze.



LetsDefend

ADJUSTING VIRTUAL MACHINE

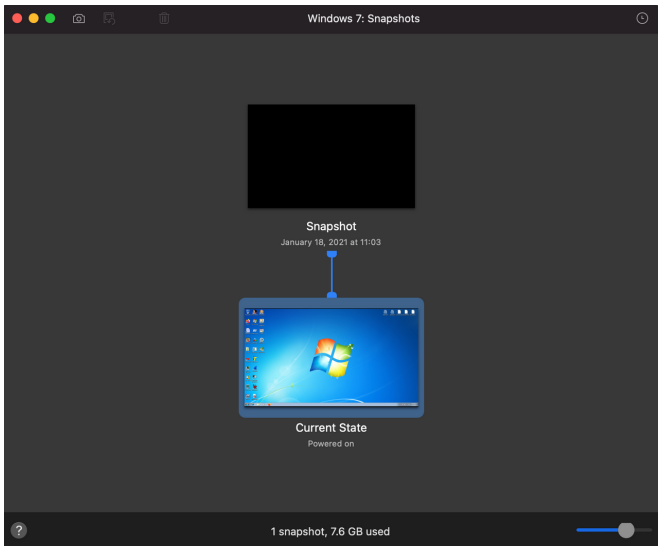
5) Disable Hidden Files and Folders

Hidden files are not displayed by default in the Windows operating system. Malware makes it difficult to detect by taking advantage of this feature. In order to see what is happening in the file system exactly, we need to disable this feature.

Snapshots

When we run malicious software, it makes various changes on the system. If you do not revert the operating system to its original state, you may confuse it with the malware you used to run while analyzing a new malware.

It will be very difficult to install a new virtual operating system every time we want to analyze malware. The Snapshot feature of virtualization software makes our job very easy.



When you take a snapshot of your virtual device through the virtualization environment, it saves the current state of the device. You will then return to this snapshot and restore the device.

After installing the necessary tools for malware analysis, you can take a snapshot and return to this snapshot after the analyzing malware and return original state of the operating system.

LetsDefend

MALWARE ANALYST'S TOOLBOX

Let's take a look at what tools are there that can make our job easier for analyzing malicious softwares.

In order to create a mind map, I divided the tools that we can use during malware analysis into 5 different categories.

There are many useful tools that we did not write and that can be used in malware analysis. This article consists of the tools we frequently encounter and use in malware analysis.

1) Disassemblers

In order for a program written in many languages (compiled languages such as C, C ++) to be run by machines, it must be converted to 0 / 1s that the machine can understand. This process is called compile.

When we want to analyze a malware, it is almost impossible to analyze this malware on 0 / 1s. Disassembler software converts the compiled software to assembly language into a format that can be read and analyzed.

Because of its ease of use, capabilities and support for many file formats, IDA Disassembler software of Hex Rays is widely used.
It is a must-have software in your toolbox.

2) Debuggers

Debuggers are software that allow us to monitor and modify the operation of a program step by step, and to monitor and control the registers and stack of the program at runtime.
Some of the most popular debuggers used are below.

LetsDefend

MALWARE ANALYST'S TOOLBOX

1. IDA Debugger
2. Immunity Debugger
3. OllyDbg
4. Windbg
5. x64dbg

We will often use debuggers in our malware analysis.

3) File Viewers, Editors and Identification Tools

P.E. File Editors display the information in the files in Portable Executable File Format in readable format.

Portable Executable File Format contains information that may be important to a malware analyst. For example, by looking at the "Machine" information in the Image File Header, you can find out whether the created malware targets 32-bit operating systems or 64-bit operating systems.

Below are some tools that you can use.

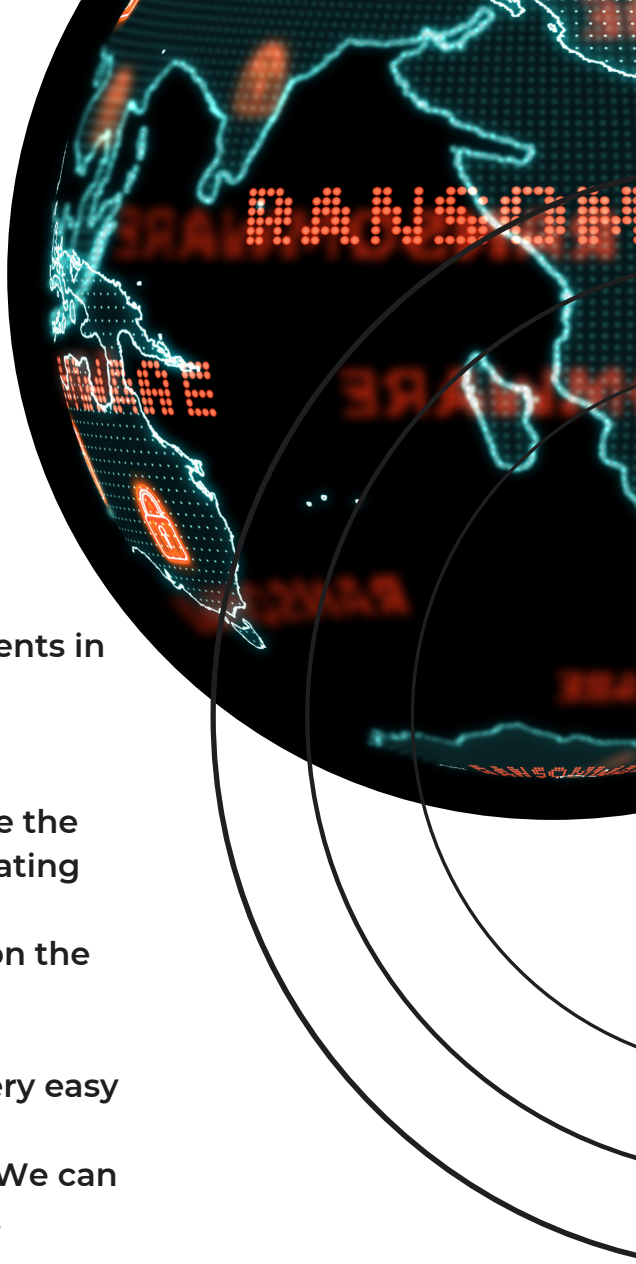
1. CFF Explorer
2. PEView
3. PEiD
4. BinText (I know it's not a File Editor but it can show you strings inside PE File)
5. DocFileViewerEX

4) Network Analysis Tools

Malware performs network activities for various activities such as hijacking data, receiving commands from command control servers and spreading within the network.

In order to monitor and analyze the network activities of the malicious software, the malware analyst must have a tool in her/his toolbox that can analyze network activities. Below are some network analysis tools you can use.

1. Wireshark
2. Fiddler



MALWARE ANALYST'S TOOLBOX

5) Others

Apart from the tools we have mentioned in our article, there are many tools that you can use in malware analysis and make your job easier.

You can view file, registry and process / thread events in the operating system with the procmon tool in Sysinternals.

With the autoruns tool in Sysinternals, you can see the processes that will start automatically in the operating system. Malware often registers itself to start automatically in order to ensure its permanence on the system.

Each of the Sysinternals tools will make our job very easy in malware analysis. For this reason, we strongly recommend adding Sysinternals to your toolbox. We can do many operations with the tools in Sysinternals.

With the Volatility tool, you can perform your forensics analysis on memory.

You can use tools such as Process Hacker, Process Explorer to see and monitor the processes running on the operating system.

Do not forget to take snapshots after installing these tools on the virtual operating system that we have created for malware analysis. After analysis, we will return to snapshot again and return to the time when all tools were installed.

WHİCH APPROACH SHOULD YOU CHOOSE WHEN ANALYZİNG MALWARE?

If you work in the defensive field, analyzing malware becomes part of your job.

In this article, we will discuss with which approaches you can analyze malware and the advantages / disadvantages of these approaches to each other.

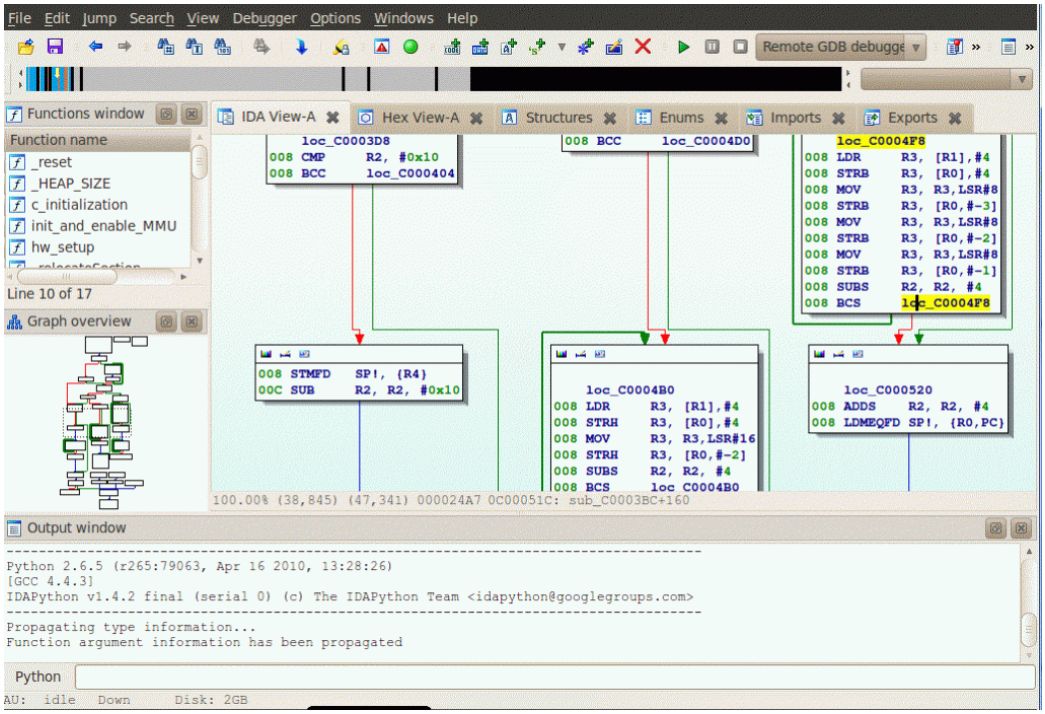
There are 2 different approaches to analyzing malware.

1. Static Analysis
2. Dynamic Analysis

What is Static Analysis?

It is the approach of analyzing malicious software by reverse engineering methods without running them.

Generally, by decompile / disassemble the malware, each step that the malware will execute is analyzed, hence the behavior / capacity of the malware can be analyzed.



LetsDefend

WHİCH APPROACH SHOULD YOU CHOOSE WHEN ANALYZİNG MALWARE?

Your device will not be infected as you do not run malicious software in static analysis. (However, we do not recommend performing static analysis on your host device, it will be more proper to do your analysis in a virtual operating system.)

The information examined during the static analysis is as follows.

1. P.E. (Portable Executable) Headers
2. Imported DLL's
3. Exported DLL's
4. Strings in binary
5. CPU Instructions

You can obtain malware sample from blue team training platform LetsDefend

What is Dynamic Analysis?

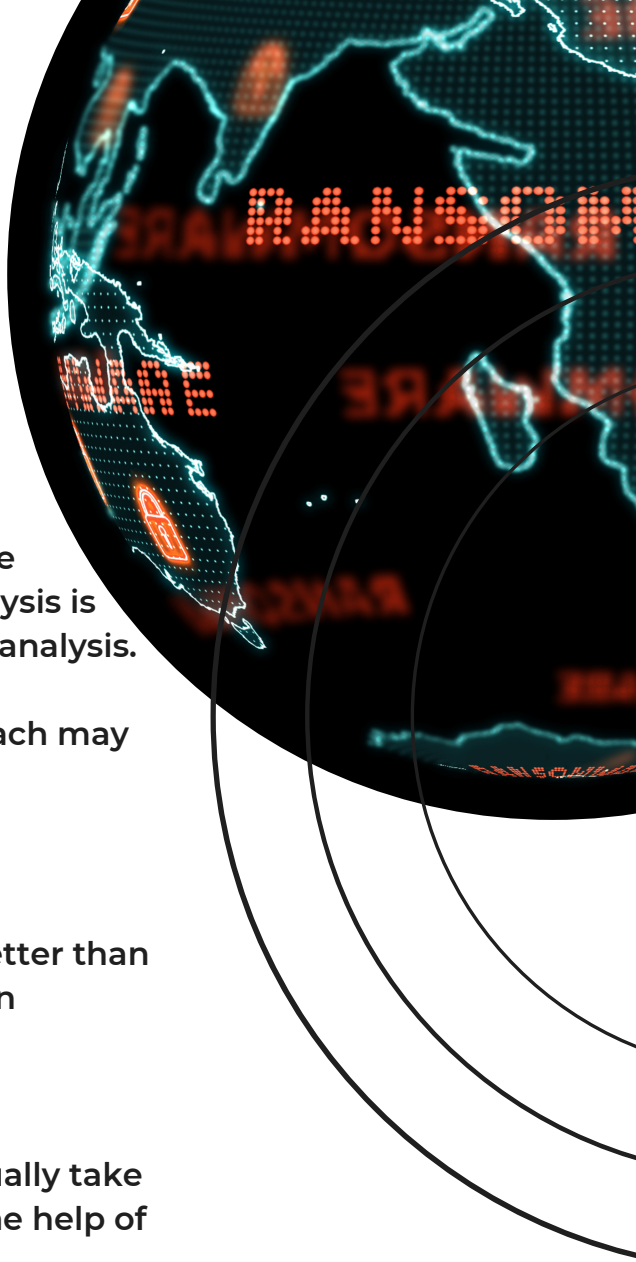
It is the approach that examines the behavior of malicious software on the system by running it.

In dynamic analysis, applications that can examine registry, file, network and process events are installed in the system, and their behavior is examined by running malicious software.

While doing dynamic analysis, you should carefully examine the following events.

1. Network Connections
2. File Events
3. Process Events
4. Registry Events

WHİCH APPROACH SHOULD YOU CHOOSE WHEN ANALYZİNG MALWARE?



Static Analysis vs Dynamic Analysis

Which approach to use when analyzing malware depends on the current circumstances. In cases where you want to get fast results, you can choose dynamic analysis, but we cannot say that the analysis is complete without doing both static and dynamic analysis.

It should also be noted that using only one approach may not be sufficient to analyze malware. Using both approaches together will lead you to victory!

As a result, we cannot say that one approach is better than another. Each has an advantage over each other in different conditions.

If you work as a Level 1-2 SOC analyst, you can usually take action by quickly obtaining the address c2 with the help of dynamic analysis.

DYNAMIC ANALYSIS EXAMPLE USING ANYRUN #1

You can take advantage of sandbox services/products to quickly analyze malware.

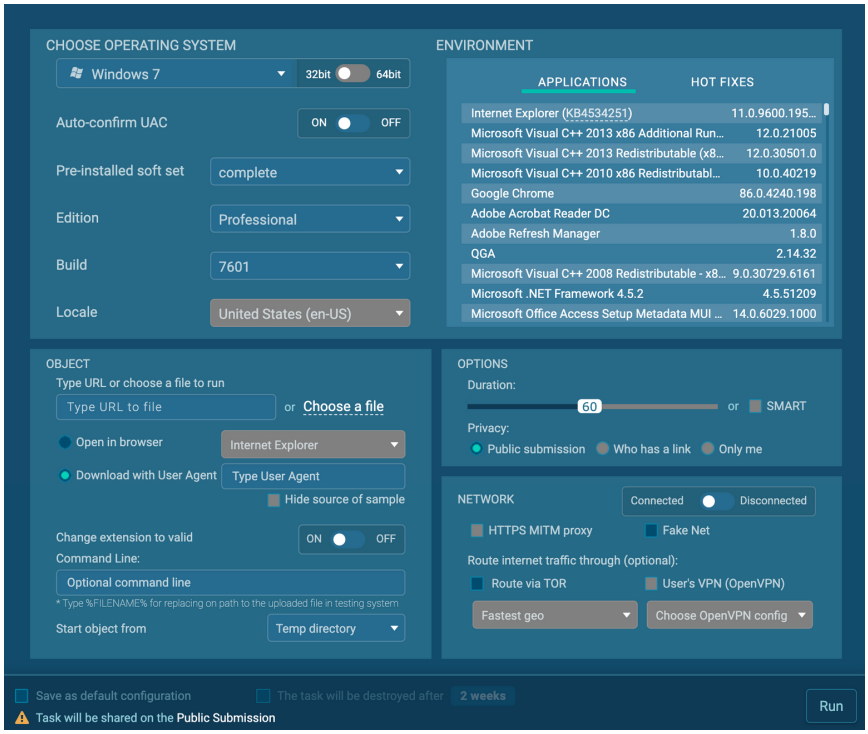
AnyRun is an interactive sandbox that you can use when you want to analyze malware quickly.

AnyRun has options for paid or free use. If you want to take advantage of it for free, all your analysis is visible to others, therefore we do not recommend that you upload files that may contain personal data to AnyRun. In addition, the free plan has restrictions such as usage time.

How can we use AnyRun for our malware analysis, what kind of outputs we can get, let's examine it together.

Let's download the malware with hash 80b51e872031a2befeb9a0a13e6fc480 to analyze via AbuseCH.

We have to click on the "+" (New Task) button on the left menu to upload the malware we downloaded.



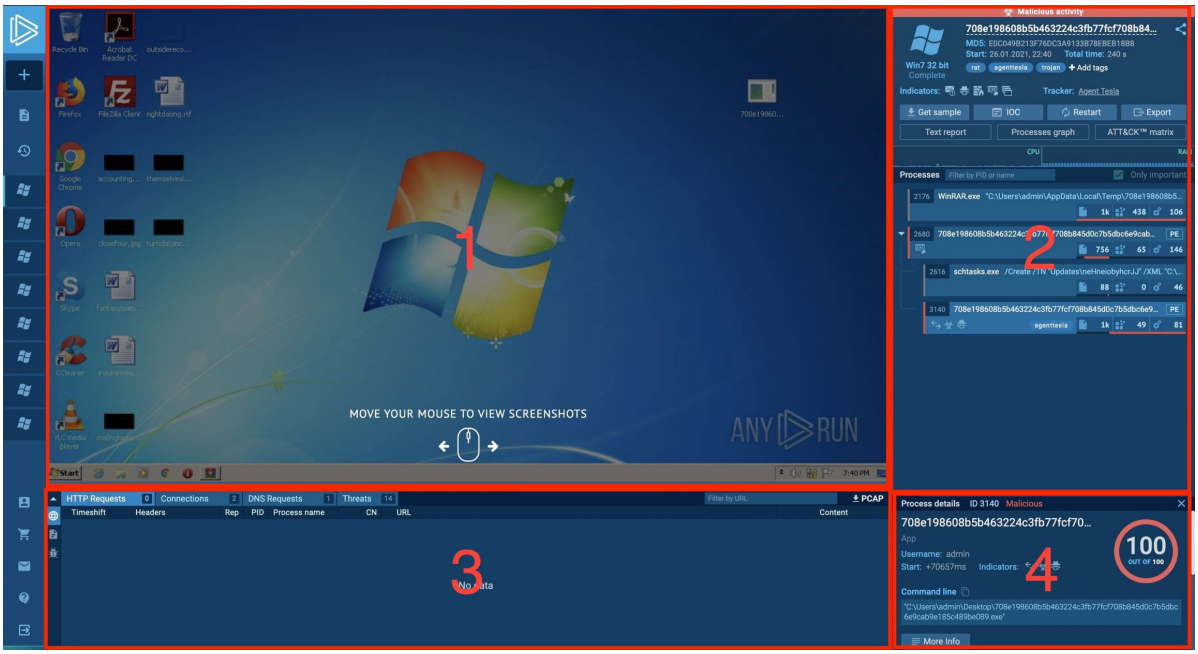
LetsDefend

DYNAMIC ANALYSIS EXAMPLE USING ANYRUN #1

Let's upload the file we want to analyze on the screen that opens with the help of the "Choose a file" button. After the file is uploaded, we can determine the parameters such as which operating system we want to run the malware and 32/64 bit of operating system to use. After determining these, we open our sandbox with the help of the "Run" button at the bottom right of the screen that opens.

When our machine is turned on, we run the malicious software we uploaded to see it's activities.

Some malware stays dormant for a certain period of time before performing its malicious activities, making analysis difficult. Let's allow time for the malware to perform its activities, during this time, let's examine the AnyRun interface together.



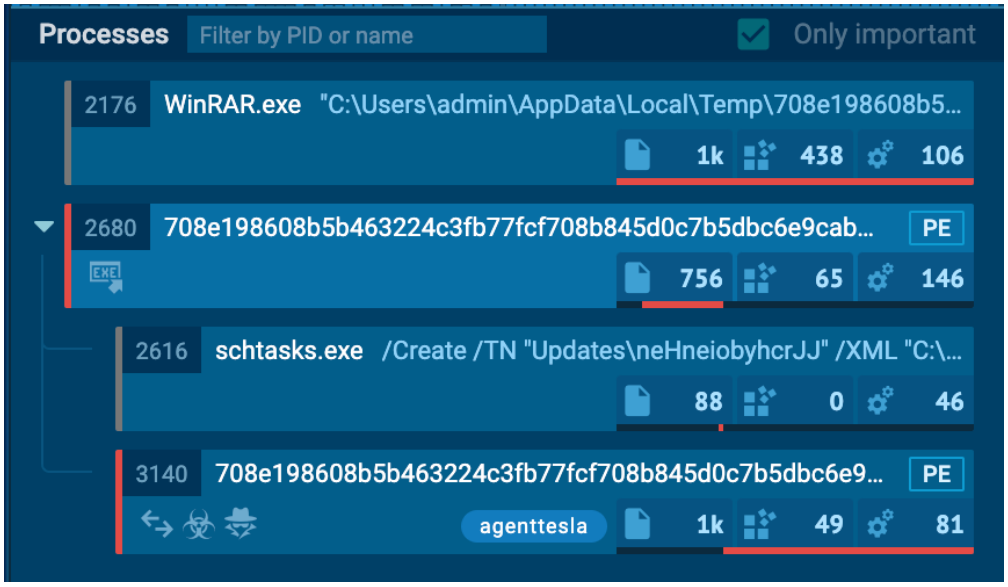
LetsDefend

DYNAMIC ANALYSIS EXAMPLE USING ANYRUN #1

1. From this area, you can use the operating system interactively.
2. Here is a list of processes in this section. From here, you can easily see which childprocesses the malware you run has.
3. In this area there is network and files events.
4. This section contains details of the process.

Let's examine these outputs.

First, let's examine the process events of the malware in the section marked "2" in the image above.



LetsDefend

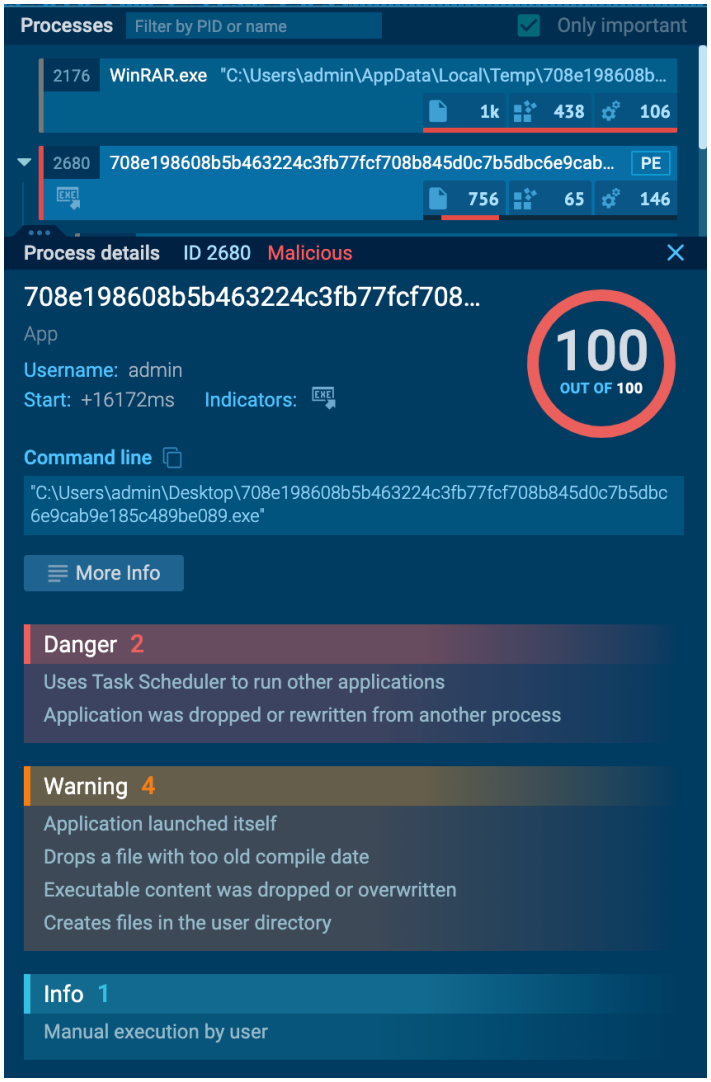
DYNAMIC ANALYSIS EXAMPLE USING ANYRUN #1

The malware we run manually seems to have created 2 child processes. One of them is schtasks.exe, which is run to ensure persistence on the system by creating a schedule task and the other is the process specified as "AgentTesla" malware by AnyRun.

When we click on Processes, information about this process is displayed in panel number 4. Let's examine the details of all processes respectively.

Since the process named "WinRAR.exe" is created when we extract the malware from the archive file to run it, we will not examine this process.

When we click on the process with ID 2680, information about this process is listed on panel number 4.



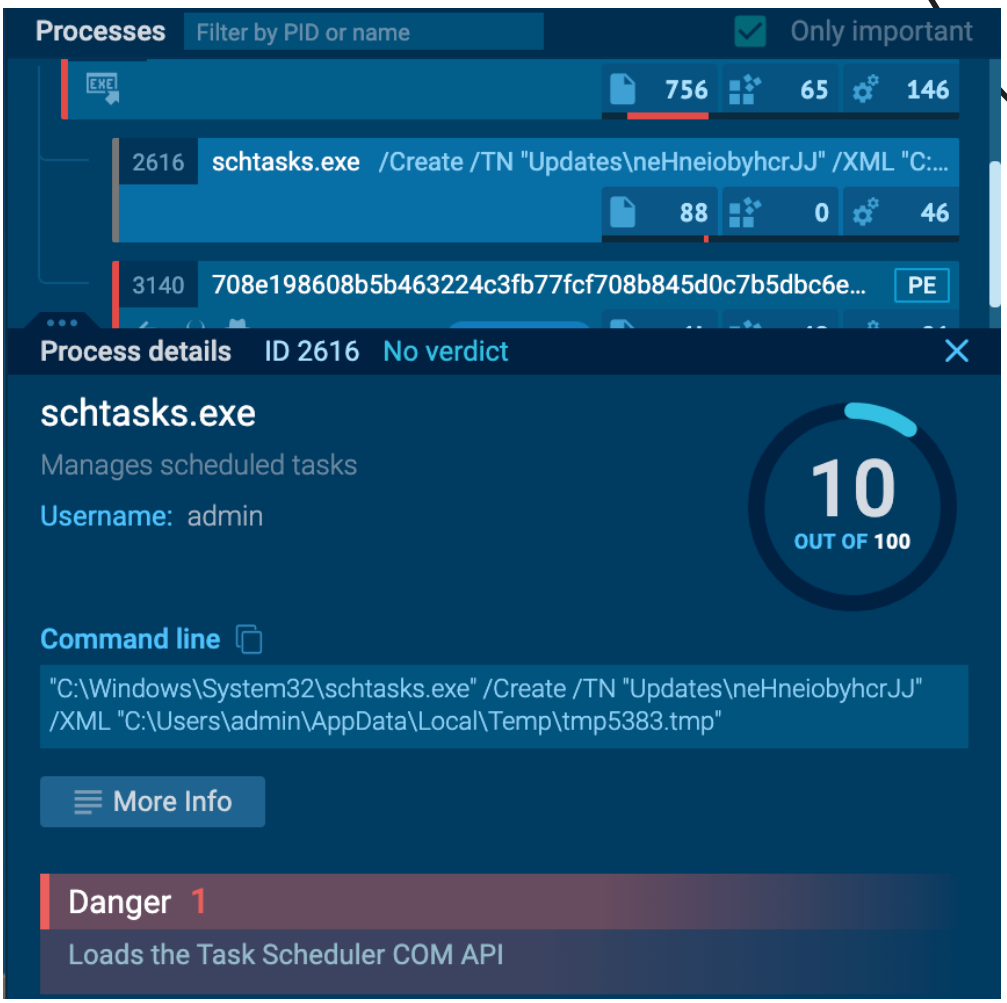
LetsDefend

DYNAMIC ANALYSIS EXAMPLE USING ANYRUN #1

With the "More Info" button on this panel, a page with detailed information about the process is opened. When we want to reach detailed information, we can use this section.

When the process information with 2680 ID is examined, the malware:

- Uses Task Scheduler,
- Writes a program to the file system which compile time is too old,
- Writes many files to the user directory

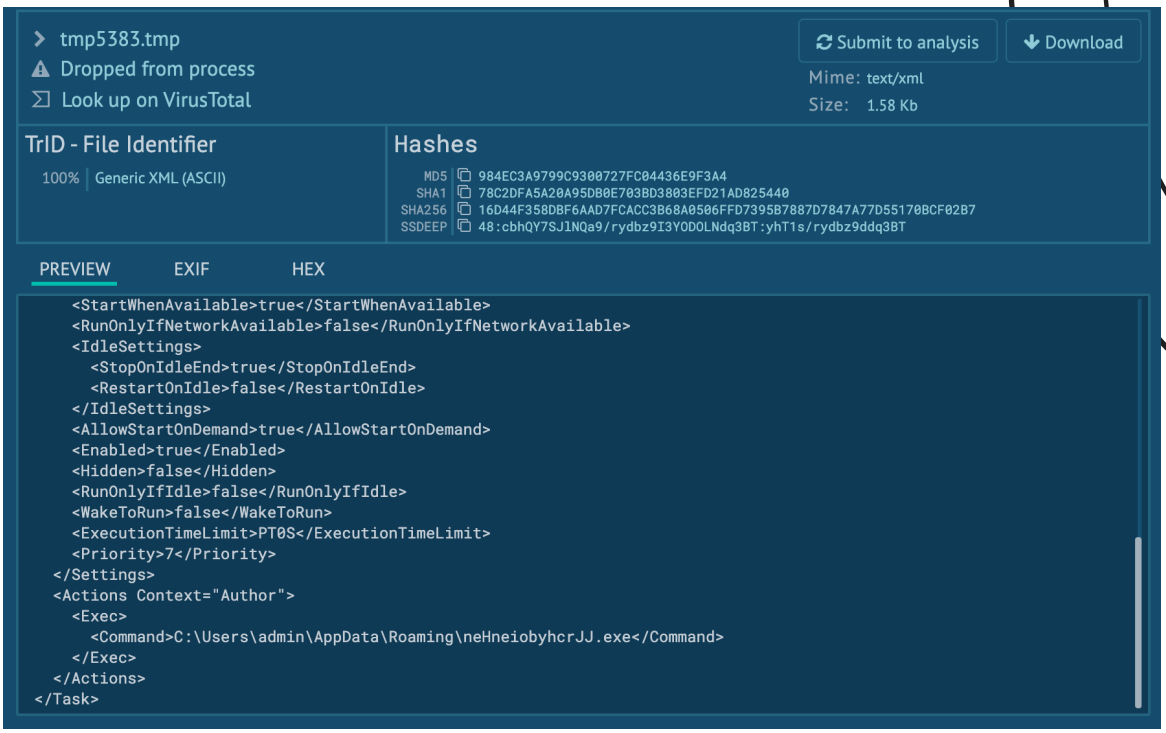


LetsDefend

DYNAMIC ANALYSIS EXAMPLE USING ANYRUN #1

When we examine the process with ID 2616, we see that it is schtasks.exe belonging to Task Scheduler.

When we examine the "Command Line" parameters, we see that it creates a schedule task named "Updates\neHneiobyhcrJJ". The configurations for this schedule task are in the file "tmp5383.tmp".

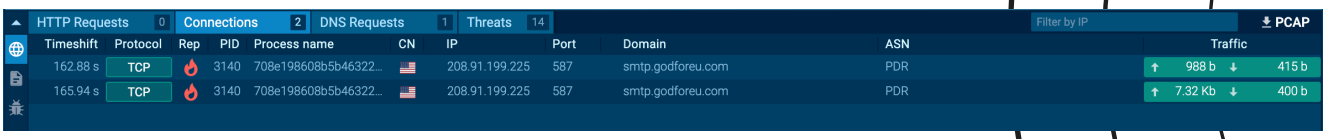


When we examine the schedule task configuration file named tmp5383.tmp, we see that the program named "neHneiobyhcrJJ.exe" will run.

DYNAMIC ANALYSIS EXAMPLE USING ANYRUN #1

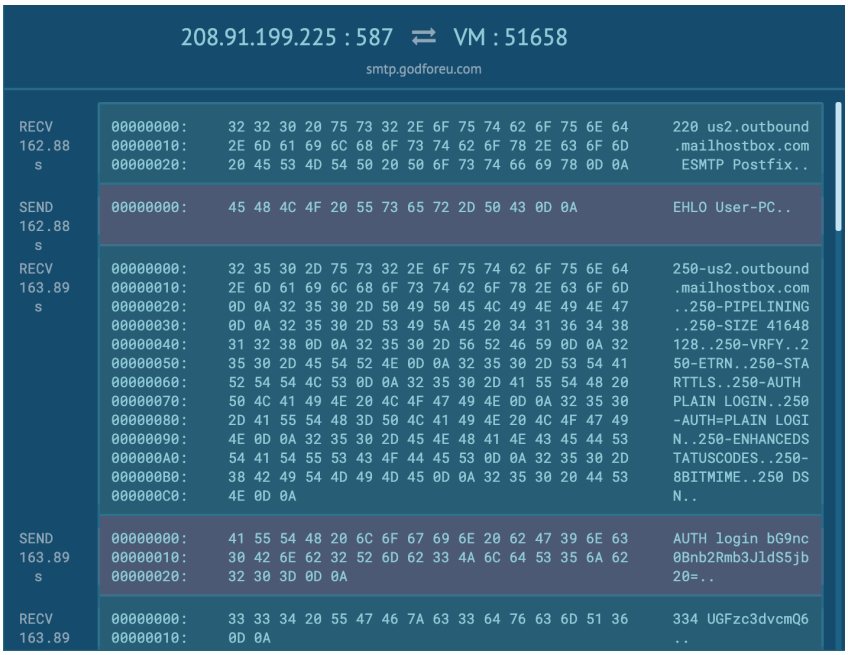
When we examine the process with ID 3140:

- This malware is recognized by AnyRun as AgentTesla,
- Steals credentials,
- Creating files in the user directory



When we examine the network connections made from panel number 3, we see that malware connects to smtp.godforeu.com.

With the help of the button on the right of the panel, we can examine the incoming/outgoing data.



When the network activities of the malware are examined, we find that malware exfiltrates data with the SMTP protocol.

If you want to examine, you can reach the analysis made here.

LetsDefend

29 ADDRESSES TO ANALYZE MALWARE FASTER

We constantly spend time analyzing malware. We have listed 29 addresses that can be useful for blue team members to use time more effectively:

- Anlyz
- Any.run
- Comodo Valkyrie
- Cuckoo
- Hybrid Analysis
- Intezer Analyze
- SecondWrite Malware Deepview
- Jevereg
- IObit Cloud
- BinaryGuard
- BitBlaze
- SandDroid
- Joe Sandbox
- AMAaaS
- IRIS-H
- Gatewatcher Intelligence
- Hatching Triage
- InQuest Labs
- Manalyzer
- SandBlast Analysis
- SNDBOX
- firmware
- opswat
- virusade
- virustotal
- malware config
- malware hunter team
- virscan
- jotti