Assignment 2

Applied Reverse Engineering Analysis

Name: Marco CAVANI

Student Number: **10570027**

Email: [**mcavani@our.ecu.edu.au**](mailto:mcavani@our.ecu.edu.au)

Malware 1- Hash:

3db0e385eb53a32d61a5a35908a99317868b571e4cf7079db67fd68604da662c

Malware 2 Hash:

5e61c19f634091264c187eb51acc8ac346914919e4f6a8b1e7a7087d0fcf8bf6

Lecture: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tutor: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Findings

## Executive Summary

Identification of malware samples was performed using VirusTotal, Hybrid-Analysis, Triage sandboxes, along with other malware tools such as Radare 2(R2), Ultimate Packer for eXecutable (UPX), Detect Is Easy (DIE) and terminal apps such as Kali and Windows 10 virtual machines. The analysis was conducted following safety guidelines as per lecture.  In saying that, the first sample was labelled  as Dowloader.MSIL.DowloadSponsor.AP, which is seen to infect computers from malicious websites. The second one has been labelled as a Trojan generic, which can be disruptive for the computer infected as it contains packed malicious software and privilege escalation methods. During the analysis, the two samples were unpacked and analysed. In the first part you can find a comprehensive analysis of the detection rate and the security vendors review, whereas in the second part a deeper analysis is provided. Further, the last part includes YARA rules for both samples as well as the cleaning processes.

# Malware Identification

## VirusTotal - Static Analysis – Sample 1

sample 1 was identified using the VirusTotal website. An initial static analysis conducted using the sandbox outlined the malicious nature of it. According to VirusTotal, the malware is a Windows 32 based Executable file 1.14 MB, created in July 2015. VirusTotal indicates that 47 out of 71 security vendors, including Google, Microsoft, McAfee, and Malwarebytes have flagged the file as malicious.

|  |  |
| --- | --- |
| SHA256 | 3db0e385eb53a32d61a5a35908a99317868b571e4cf7079db67fd68604da662c |
| Creation Date | 2015-07-22 13:51:55 UTC |
| File Type | Win 32 EXE |
| File Size | 1.14 Megabytes |
| Classification | malicious |

Table 1

### VirusTotal - Security Vendor Report – Sample 1

|  |  |
| --- | --- |
| **Vendor** | **Signature** |
| Acronis (Static ML) | Suspicious |
| ClamAV | Win.Dropper.DarkKomet-9164386-0 |
| CrowdStrike Falcon | Win/grayware\_confidence\_100% (W) |
| Cynet | Malicious (score: 100) |
| DrWeb | Adware.Downware.10929 |
| Emsisoft | Application.AdLoad (A) |
| Fortinet | AutoIt/Dloader.SM!tr |
| Google | Detected |
| Ikarus | PUA.DownloadSponsor |
| K7AntiVirus | Unwanted-Program ( 004eb1091 ) |
| Caspersky | Not-a-virus:Downloader.MSIL.DownloadSponsor |
| MaxSecure | Downloader.MSIL.DownloadSponsor.gen |
| MacAfee-DW-Secure | BehavesLike.Win32.DLSponsor.th |
| Nano-Antivirus | Trojan.Win32.Agent.edqrfj |
| Panda | PUP/DownloadAssistant |
| Rising | PUF.DownloadSponsor!1.BE33 (CLASSIC) |
| ESET-NOD32 | A Variant Of Win32/DownloadSponsor.C Po |
| GData | Win32.Trojan.Agent.907XE1 |
| Gridinsoft (no cloud) | PUP.Downloader.dd!c |
| Jiangmin | Downloader.DownloadSponsor.am |
| K7GW | Unwanted-Program ( 004eb1091 ) |
| Malwarebytes | PUP.Optional.ChipDe |
| McAfee | DLSponsor |
| Microsoft | PUADlManager:Win32/DownloadSponsor |
| Palo Alto Networks | Generic.ml |
| QuickHeal | PUA.Chipdigita1.Gen |
| Sangfor Engine Zero | PUA.Win32.Sign.a |
| SUPERAntiSpyware | PUP.DownloadSponsor/Variant |
| TEHTRIS | Generic.Malware |
| Trapmine | Malicious.high.ml.score |
| TrendMicro | PUA.MSIL.DownloadSponsor.SMDR |
| VBA-32 | Downloader.MSIL.DownloadSponsor |
| ViRobot | Adware.Downloadsponsor.1198368.DTK |
| Yadex | PUA.Downloader!CI3y1nhnBOw |

Table 2

[Www.virustotal.com.https://www.virustotal.com/gui/file/3db0e385eb53a32d61a5a35908a99317868b571e4cf7079db67](http://Www.virustotal.com.https://www.virustotal.com/gui/file/3db0e385eb53a32d61a5a35908a99317868b571e4cf7079db67)

## VirusTotal - Static Analysis – Sample 2

VirusTotal sandbox detection rate shows that 57 out of 72 security vendors, including Avast, AVG, Google, Sophos, and Microsoft have flagged the file as malicious, in which many have defined it as Trojan. The malware sample is a Windows 32-bit executable program created in 2012.

|  |  |
| --- | --- |
| SHA256 | 5e61c19f634091264c187eb51acc8ac346914919e4f6a8b1e7a7087d0fcf8bf6 |
| Creation Date | 2012-07-13 13:09:56 UTC |
| File Type | Win 32 EXE |
| File Size | 1.83 Megabytes |
| Classification | Malicious/Trojan |

Table 3

#### VirusTotal - Security Vendor Report – Sample 2

|  |  |
| --- | --- |
| Vendor | Signature |
| Ad-Aware | Trojan.Generic.22209847 |
| Alibaba | Trojan:Win32/Generic.698a3760 |
| Antiy-AVL | Trojan[Backdoor]/Win32.BlackHole |
| Avast | Win32:Malware-gen |
| BitDefender | Trojan.Generic.22209847 |
| Bkav Pro | W32.AIDetect.malware1 |
| Comodo | Worm.Win32.Dropper.RA@1qraug |
| Cybereason | Malicious.ce63cf |
| Cynet | Malicious (score: 100) |
| Elastic | Malicious (high Confidence) |
| eScan | Trojan.Generic.22209847 |
| Fortinet | Riskware/Application |
| Google | Detected |
| Ikarus | Trojan.Rootkit.Gen2 |
| K7AntiVirus | Trojan ( 005246d51 ) |
| Kingsoft | Win32.Hack.Heidong.cw.(kcloud) |
| Malwarebytes | PUP.Optional.ChinAd |
| MaxSecure | Dropper.Dinwod.frindll |
| McAfee-GW-Edition | BehavesLike.Win32.Flyagent.th |
| NANO-Antivirus | Trojan.Win32.BlackHole.bomwes |
| Panda | Generic Malware |
| Sangfor Engine Zero | Trojan.Win32.Bitrep.B |
| SentinelOne (Static ML) | Static AI - Malicious PE |
| Symantec | ML.Attribute.HighConfidence |
| Trapmine | Malicious.moderate.ml.score |
| TrendMicro | TROJ\_FRS.0NA103K319 |
| VIPRE | Trojan.Generic.22209847 |
| Yandex | Trojan.GenAsa!h4mMSIEsIEA |
| AhnLab-V3 | Trojan/Win.Malware-gen.C4686009 |
| ALYac | rojan.Generic.22209847 |
| Arcabit | Trojan.Generic.D152E537 |
| AVG | Win32:Malware-gen |
| BitDefenderTheta | Gen:NN.ZexaF.34698.1v0@amK7S9bb |
| ClamAV | Win.Trojan.Flystudio-9943951-0 |
| CrowdStrike Falcon | Win/malicious\_confidence\_100% (W) |
| Cylance | Unsafe |
| Cyren | W32/Trojan.GRW.gen!Eldorado |
| Emsisoft | Application.Generic (A) |
| ESET-NOD32 | A Variant Of Win32/Packed.FlyStudio.AA |
| GData | A Variant Of Win32/Packed.FlyStudio.AA |
| Gridinsoft (no cloud) | Trojan.Win32.Agent.dg |
| Jiangmin | Backdoor/Blackhole.mwo |
| K7GW | Trojan ( 005246d51 ) |
| Lionic | Trojan.Multi.Generic.mpTZ |
| MAX | Malware (ai Score=99) |
| McAfee | GenericRXAA-AA!11F76B1CE63C |
| Microsoft | Trojan:Win32/CryptInject |
| Palo Alto Networks | Generic.ml |
| Rising | Trojan.Bitrep!8.F596 (CLOUD) |
| Sophos | Malicious |
| SecureAge | Generic PUA NK (PUA) |
| Trellix (FireEye) | Generic.mg.11f76b1ce63cf905 |
| TrendMicro-HouseCall | TROJ\_FRS.0NA103K319 |
| ViRobot | Trojan.Win32.Z.Blackhole.1916928.C |
| Zillya | Backdoor.BlackHole.Win32.22443 |

Table 4

[Www.virustotal.com.https://www.virustotal.com/gui/file/5e61c19f634091264c187eb51acc8ac346914919e4f6a8b1e7a7087d0fcf8bf6](http://Www.virustotal.com.https://www.virustotal.com/gui/file/5e61c19f634091264c187eb51acc8ac346914919e4f6a8b1e7a7087d0fcf8bf6)

## Obfuscation

Obfuscation is used in malware development to obfuscate programs in which the malicious code is compressed and cannot be analysed. However, using the Detect It Easy (DIE) malware analysis tool, it is possible to reveal packed files within the sample by looking at the entropy percentage rate. The  rate refers to a statistical variation in the sample executable. A higher rate indicates a high possibility of obfuscation. The two malware samples were analysed.

### Sample 1 – obfuscation – Analysis

Sample one entropy percentage is at 98%, that indicates the file is packed (see figure 1).

Graphical user interface

Description automatically generated

Figure 1

The screenshot below (figure 2), shows that sample one has being unpacked using Ultimate Packer for eXecutable (UPX) by running UPX command on Kali Linux Terminal App.

Text

Description automatically generated

Figure 2

After that, entropy percentage has dropped by 17% .

Graphical user interface, chart

Description automatically generated

Figure 3

### Sample 2 – obfuscation – Analysis

Sample 2 was analysed similarly to sample one. As it can be seen from the image below, the entropy percentage rate of the second sample was at 95% and it was packed. According to a Hybrid analysis report, a file had obfuscated details: "SkinH\_EL.dll" has a section named "UPX0" & "SkinH\_EL.dll" has a section named "UPX1".

Graphical user interface, application

Description automatically generated

Figure 4

Sample 2 was unpacked using UPX by running UPX command on Kali Linux Terminal App.

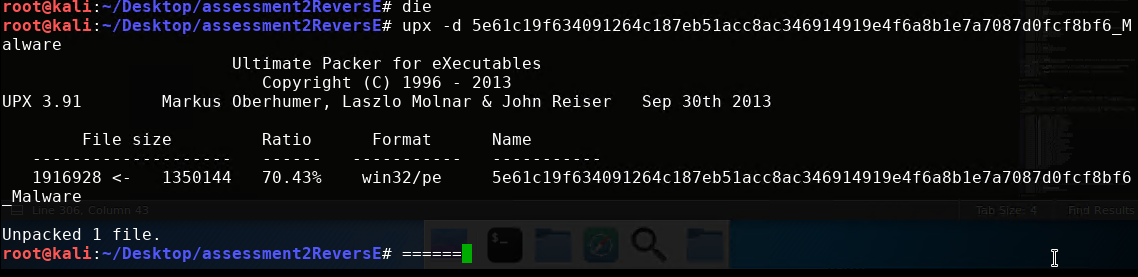


Figure 5

After That, the rate dropped by 12%. (See figure 6)

Graphical user interface

Description automatically generated

Figure 6

## Targeted Architecture

### Targeted Architecture - Sample 1

|  |  |
| --- | --- |
| Category | Contents |
| Library | Autolt(-)[-] |
| compiler | Microsoft Visual C/C++(2012)[-] |
| Linker | Microsoft linker (11.0)[EXE32] |

### Targeted Architecture - Sample 2

|  |  |
| --- | --- |
| Category | Contents |
| Library | N/A |
| compiler | Microsoft Visual C/C++(6.0)[] |
| Linker | Microsoft linker (6.0)[EXE32] |

## Malware Behaviour

### Strings - Analysis – Sample 1

Strings can contain information about the malware structure and might be analysed to understand the malware functionalities. Using Linux Terminal App, it is possible to get all strings within the malware sample by running strings -a -n 8 + filename >> file.txt it is possible to obtain strings within the file, including strings which are minimum 9 characters long, in order to exclude ASCII strings. As a result, a text file was created, and strings analysed. The table below shows the findings of the analysis.

|  |  |
| --- | --- |
| **String** | **Description** |
| Dmr\_72.exe | Trojan/Backdoor |
| advapi32. dll | It queries privileges and try to set them |
| kernel32.dll | Find process address, load libraries, exec (run new processes), write file creates files, manipulate resources |
| System.Reflection | Contains types that retrieve information about assemblies, modules, members, parameters, and other entities in managed code by examining their metadata. |
|  |  |
| CreateEncryptor | Creates a symmetric encryptor object. |
| CreateDecryptor | Creates a symmetric decryptor object. |
| CryptoStreamMode | Specifies the mode of a cryptographic stream. |
| get\_DLList  set\_DLList | It may communicate with a server |

Table 5

The malware might contain modules for retrieving information in managed code by examining its metadata. Also, it might be able to create Encryption and decryption objects as well as connect to a server through get and set calls.

#### Signature – Sample 1

|  |
| --- |
| Executes dropped EXE ⋅ 1 IoCs |
| Loads dropped DLL ⋅ 4 IoCs |
| AutoIT Executable ⋅ 2 IoCs |
| UPX packed file ⋅ 2 IoCs |
| Detects executables packed with UPX/modified UPX open source packer. [upx](https://tria.ge/s?q=tags:upx) |
| AutoIT scripts compiled to PE executables. |
| Enumerates physical storage devices ⋅ 1 TTPs  Attempts to interact with connected storage/optical drive(s). Likely ransomware behaviour. |
| Suspicious use of AdjustPrivilegeToken ⋅ 1 IoCs |
| Suspicious use of FindShellTrayWindow ⋅ 3 IoCs |
| Suspicious use of SendNotifyMessage ⋅ 3 IoCs |
| Suspicious use of SetWindowsHookEx ⋅ 2 IoCs |
| Suspicious use of WriteProcessMemory ⋅ 4 IoCs |

Table 6

https://tria.ge/221010-k4fdhabcg4/behavioral1#report

#### Processes – Sample 1

The process section outlines the location where the malware sits within Windows systems. Further, the malware installs itself inside a Temp subfolder inside AppData/local in the admin folder of the User directory. Inside the C-drive at: C:\Users\Admin\AppData\Local\Temp\3db0e385eb53a32d61a5a35908a99317868b571e4cf704da662c\_malware.exe. A Triage dynamic analysis report, have had identified malicious executable component been installed at the following location: C:\Users\Admin\AppData\Local\Temp\DMR\ called Dmr\_72.exe (*Dmr\_72.Exe Windows Process - What Is It?*, n.d.) which was then identified on the binary level using R2..



The Dmr\_72.exe, is an executable file considered to be a trojan malware component that can remotely execute programs and run commands, sand data using the network and replicate its-self in the system. This Trojan create the following folders: %User Temp%\DMR %User Profile%\CHIP Secured Installer\1.0.7.6 %User Profile%\Chip Digital GmbH\CHIP Secured Installer %User Profile%\Application Data\Chip. The (*Dmr\_72.Exe Windows Process - What Is It?*, n.d.). A report from Hybrid analysis outlined the following processes:

* Drops executable file immediately after starts
* Application was dropped or rewritten from another process dmr\_72.exe
* Checks supported languages
* Checks Windows language
* Executable content was dropped or overwritten
* Reads the computer name dmr\_72.exe
* Reads Environment values

The sample was labelled  as Dowloader.MSIL.DowloadSponsor.AP, which is seen to infect computers from malicious websites. Moreover, according with MITRE ATT&CK®, The malware can be used to attempt to get information about the Operating System and hardware, including version, patches, hotfixes, service packs, and architecture.

<https://www.hybrid-analysis.com/sample/3db0e385eb53a32d61a5a35908a99317868b571e4cf7079db67fd68604da662c/63438b34d7f6624c7044c980>

### Strings - Analysis – Sample 2

Strings can contain information about the malware structure and might be analysed to understand the malware functionalities. Using Linux Terminal App with radare2 installed, it is possible to get all strings within the malware sample by running r2 + sample name, then aaaa and f  >> file.txt. As a result, a text file was created, and strings analysed. The table below shows the most relevant findings of the analysis.

|  |  |  |
| --- | --- | --- |
| **String** | **Description** | **Source** |
| KinH\_EL.dll | Trojan/backdoor  Imports:  KERNEL32.dll  COMCTL32.dll  USER32.dll  GDI32.dll  MSIMG32.dll | https://www.virustotal.com/gui/file/573cf4e4dfa8fe51fc8b80b79cd626cb861260d26b6e4f627841e11b4dce2f48/details |
| RASAPI32.dll | rasapi32.dll is the Remote Access API (RAS), used by Windows applications to control modem connections. | rasapi32*.dll - What is rasapi32.dll?* (n.d.). Www.processlibrary.com. Retrieved October 11, 2022, from https://www.processlibrary.com/en/directory/files/rasapi32/24102/ |

Table 7

Two suspicious strings were identified using Radare2 while querying the sample. The first one, “KinH\_EL.dll” was reported as a malicious component by three security vendors in a VirusTotal sandbox report. The other one “RASAPI32.dll” is the Remote Access API (RAS), used by Windows applications to control modem connections.

### Signature - Sample 2

|  |
| --- |
| ACProtect 1.3x - 1.4x DLL software ⋅ 1 IoCs  Detects file using ACProtect software. |
| PX packed file ⋅ 2 IoCs  Detects executables packed with UPX/modified UPX open source packer. |
| Loads dropped DLL ⋅ |
| Suspicious use of SetWindowsHookEx ⋅ 3 IoCs |

Table 8

<https://tria.ge/221010-qxg7eacbfr/behavioral1>

#### Processes – Sample 2

According to Any Run, the malware executes itself in the Temp subfolder inside AppData/local in the admin folder of the User directory. Inside the C-drive at: C:\Users\Admin\AppData\Local\Temp\5e61c19f634091264c187eb51acc8ac346914919e4f6a8b1e7a7087d0fcf8bf6\_malware.exedb0e385eb53a32d61a5a35908a99317868b571e4cf704da662c\_malware.exe, then it loads dropped or rewritten executable and drops executable file immediately after starts. Whereas Hybrid-Analysis sandbox has labelled it as a Trojan Generic.

## Rule and Cleaning Process - Sample

### YARA Rule – Sample - 1

rule wordyMod

{

strings:

$stringOne “%TEMP%\DMR\dmr\_72.exe”

$stringTwo “(DigiCert SHA2 Assured ID Code Signing CA”

$stringthree “Unable to get a list of running processes.”

$stringfour “(DigiCert SHA2 Assured ID Code Signing CA”

condition:

all of them

}

#### Rule wordyMod

This is the name assigned to the role.

#### Strings

$stringOne “%TEMP%\DMR\dmr\_72.exe”

$stringTwo “(DigiCert SHA2 Assured ID Code Signing CA”

$stringthree “Unable to get a list of running processes.”

$stringfour “(DigiCert SHA2 Assured ID Code Signing CA”

These strings can be linked to the malware sample and are unique.

#### Condition

The condition is the parameter in which the role will be trigged. The rule is set to all and will be trigged if all four conditions are met.

### YARA Rule – Sample - 1

rule AtticMod

{

strings:

$stringOne “CN\_Honker\_WordpressScanner”

$stringTwo “Sample from CN Honker Pentest Toolset - file WordpressScanner.exe”

$stringthree “(&07-034/)7 ”

$stringfour “%2\protocol\StdFileEditing\verb\0”

condition:

all of them

}

#### Rule AtticMod

This is the name assigned to the role

#### Strings

$stringOne “CN\_Honker\_WordpressScanner”

$stringTwo “Sample from CN Honker Pentest Toolset - file WordpressScanner.exe”

$stringthree “(&07-034/)7 ”

$stringfour “%2\protocol\StdFileEditing\verb\0”

These strings can be linked to the malware sample and are unique.

#### Condition

The condition is the parameter in which the role will be trigged. The rule is set to all and will be trigged if all four conditions are made.

## Cleaning Process

The Sample have been tested and analysed in a virtual environment to prevent the spread of the payload on the actual machine. In saying that sample where deleted and the virtual machines were reset to the safety.

# Presentation link

<https://ecu.ap.panopto.com/Panopto/Pages/Viewer.aspx?id=fe4f528f-af55-4711-a137-af2c0059e818>

# Reference

[1] dmr\_72.exe Windows process - What is it? (n.d.). Www.file.net. https://www.file.net/process/dmr\_72.exe.html

[2] Free Automated Malware Analysis Service - powered by Falcon Sandbox. (2019). Hybrid-Analysis.com. https://www.hybrid-analysis.com/

[3] Interactive Online Malware Analysis Sandbox - ANY.RUN. (n.d.). App.any.run. https://app.any.run/

[4] PUA.Win32.DownloadSponsor.AP - Threat Encyclopedia - Trend Micro AU. (n.d.). Www.trendmicro.com. <https://www.trendmicro.com/vinfo/au/threat-encyclopedia/malware/pua.win32.downloadsponsor.ap>

[5] rasapi32*.dll - What is rasapi32.dll?* (n.d.). Www.processlibrary.com. Retrieved October 11, 2022, from https://www.processlibrary.com/en/directory/files/rasapi32/24102/

[6] Sandbox for High-Volume Automated Malware Analysis. (n.d.). Tria.ge. Retrieved October 11, 2022, from https://tria.ge

[7]VirusTotal. (2000). Virustotal.com. https://www.virustotal.com/