Executive Summary

This report presents the findings from both static and dynamic analysis performed on the malware sample labeled ‘Malware 2.exe’. The analysis was conducted as part of the deliverables for the OpenAvenues micro-internship in Malware Analysis. The primary objectives of this analysis were to identify the malware’s functionality, assess its impact, and determine the appropriate remediation steps to mitigate any associated threats.

Case Details

Date	**29/08/2024.**
Analyst	**Eurydice Tracy Makena**

Sample information

File name	Malware 2
File size	8192 bytes
File type	executable
MD5	4280AAC55C1D3C327A6C00F0F0085677
SHA1	E006036FF66277BDA3E811B260A6441AEC64DC73
SHA256	84b7967aad00e982842045e7b9744af0a457d46bba70456e5f99e7eb9cd783c7
Packer / compiler info	Compiler: Microsoft Visual C/C++(6.0) [msvcrt] Linker: Microsoft Linker(6.0*)[EXE32]
Compile time	Thu May 14 19:12:41 2009

Standing Information Requirements

What functionality does the malware provide?

Upon execution the malware exhibits the behaviour below on the system:

- **Self-Deletion**

Immediately after running the executable file, the file spawns a process to delete the malware file using ‘cmd.exe’. This might be a tactic to make it difficult to perform further analysis and to make detection and eradication of the malware more challenging.

- **Spawning of new processes**

The malware spawns new processes upon execution. This may suggest that the malware carries out its malicious activities through child processes probably to evade security tools that may be monitoring the parent process.

- **Registry Modification**

The malware uses spawned processes to modify the registry. This is by modifying entries under the key '**HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap'.** This registry key is used to manage the security zones settings in Internet Explorer and other applications that rely on Internet Explorer's settings, such as Microsoft Edge.

What indicators of compromise are associated with this malware?

- **Network -Related**

Upon execution the malware attempts to send TCP connection to the IP address 60.248.52.95 on port 443. However, there was not much further traffic that stood out beyond that.

- **Processes**

The malware spawns multiple processes upon execution. These include cmd.exe and Conhost.exe. Additionally, one of the processes is responsible for self-deleting the malware upon execution.

- **Registry Modification**

The malware modifies the registry key HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap. The key controls Internet Explorer's security zone settings for different websites and network locations. By modifying this key, malware can potentially lower security settings for malicious websites, making it easier to download and execute additional malicious content. The following entries were added to the key; ProxyBypass, IntranetName, UNCAsIntranet and AutoDetect.

- **File creation**

A prefetch file associated with the malware sample was found created on the system. The file for this was **C:\Windows\prefetch\MALWARE 2.EXE-460B2161.pf.** This can be an Indicator of Compromise since it shows that the malware was executed in the system.

Does the malware maintain persistence on the victim system? If so, how?

I believe the malware maintains persistence on the system by modifying the registry key above. This may be to manipulate the security settings to ensure that it remains active even after a user is logged out or if the computer is rebooted.

Which application, service or other vulnerability does this malware exploit?

a. Is it related to an existing CVE?
    i. If yes, list all related CVE numbers
    ii. If not, could it be an unknown 0-day vulnerability?

The malware does not appear to exploit a known CVE, but instead generally modifies a registry key, which may point to attempting to bypass security settings. The ZoneMap key controls

Internet Explorer's security zone settings for different websites and network locations and may be modified to lower security settings for malicious sites, elevate privileges status for attacker-controlled domains and bypass security restrictions. Overall, this could potentially allow:

- Drive-by downloads from untrusted sources.
- Disabling security features like Protected Mode.
- Redirection of traffic to malicious sites.
- Persistence of malware across browser sessions.

Does Endpoint Protection protect against this attack?
Endpoint detection and response solutions should be able to detect the presence of this malware in a system and delete it from the system. Ensuring the solutions are updated regularly ensures their effectiveness since new threats are discovered regularly.

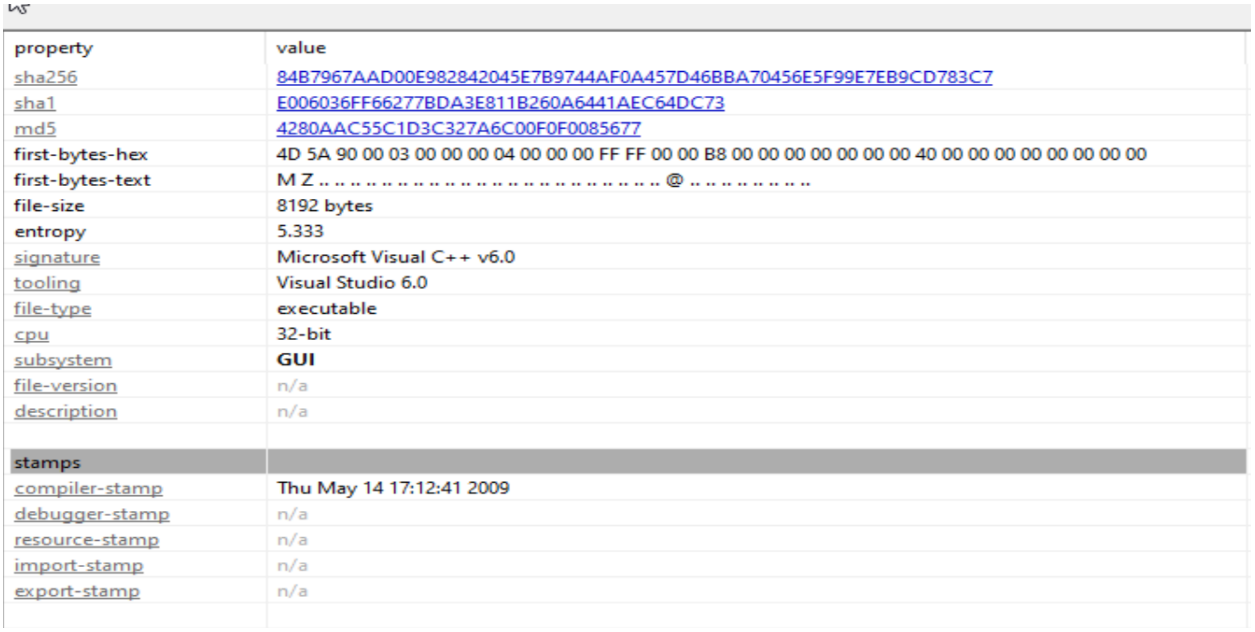
What remediation options are available to effectively remove the malware and return the system to a secure state?

- The first step is to isolate the affected machine to ensure that the malware does not spread to other machines on the same network.
- Terminate the processes that were started up from the malware's execution including the child processes.
- While the malware deletes itself upon execution, check for any other copies of the malware and permanently delete those too.
- Perform a cleanup of the registry to remove any keys or entries that were created by the process.
- Run a full system scan using an up-to-date antivirus solution to detect any remaining malware components or identify any related malware activity.
- Apply any missing patches or updates to the operating system and other system applications to ensure that any existing vulnerabilities have been patched.
- If any data was lost, restore system state from backup that was taken before the attack.
- Continuously monitor the system for any signs of malware activity.

Attachments

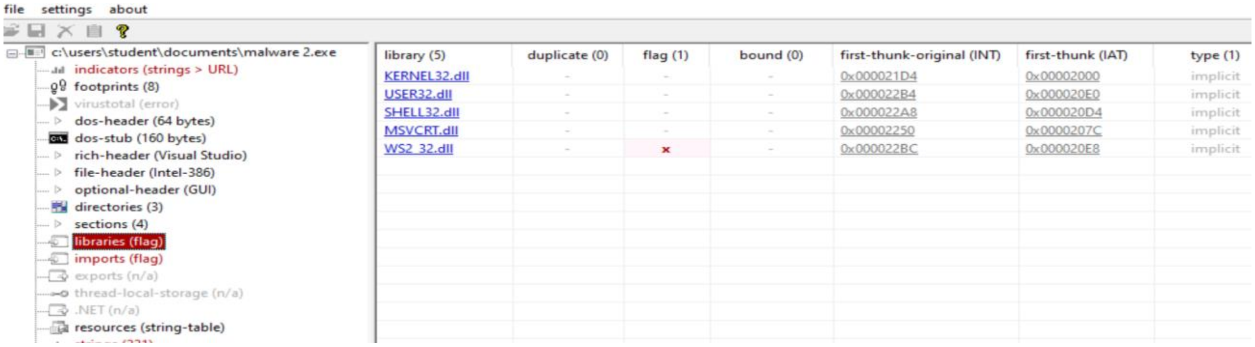
Procmon log – The log file containing the activity captured when the malware was executed.

Static Information on the malware



property	value
sha256	84B7967AAD00E982842045E7B9744AF0A457D46BBA70456E5F99E7EB9CD783C7
sha1	E006036FF66277BDA3E811B260A6441AEC64DC73
md5	4280AAC55C1D3C327A6C00F0F0085677
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	8192 bytes
entropy	5.333
signature	Microsoft Visual C++ v6.0
tooling	Visual Studio 6.0
file-type	executable
cpu	32-bit
subsystem	**GUI**
file-version	n/a
description	n/a
stamps	
compiler-stamp	Thu May 14 17:12:41 2009
debugger-stamp	n/a
resource-stamp	n/a
import-stamp	n/a
export-stamp	n/a

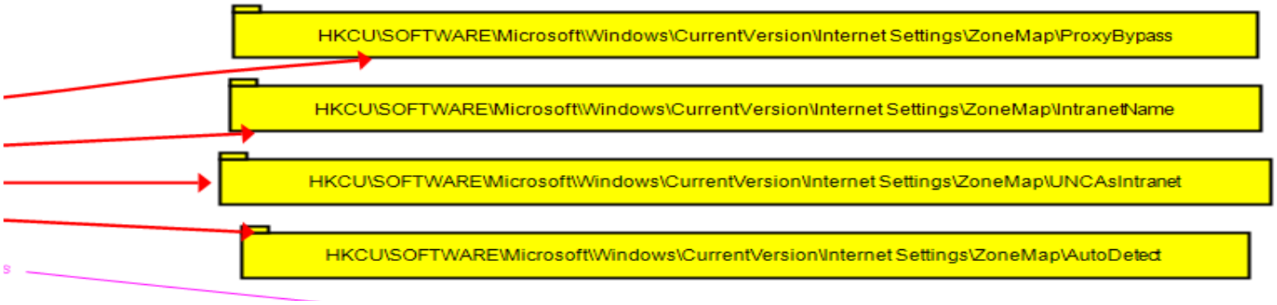
Libraries



c:\users\student\documents\malware 2.exe
- indicators (strings > URL)
- footprints (8)
- virustotal (error)
- dos-header (64 bytes)
- dos-stub (160 bytes)
- rich-header (Visual Studio)
- file-header (Intel-386)
- optional-header (GUI)
- directories (3)
- sections (4)
- libraries (flag)
- imports (flag)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (string-table)

library (5)	duplicate (0)	flag (1)	bound (0)	first-thunk-original (INT)	first-thunk (IAT)	type (1)
KERNEL32.dll	-	-	-	0x000021D4	0x00002000	implicit
USER32.dll	-	-	-	0x000022B4	0x000020E0	implicit
SHELL32.dll	-	-	-	0x000022A8	0x000020D4	implicit
MSVCRT.dll	-	-	-	0x00002250	0x0000207C	implicit
WS2_32.dll	-	x	-	0x000022BC	0x000020E8	implicit

Registry Keys Created



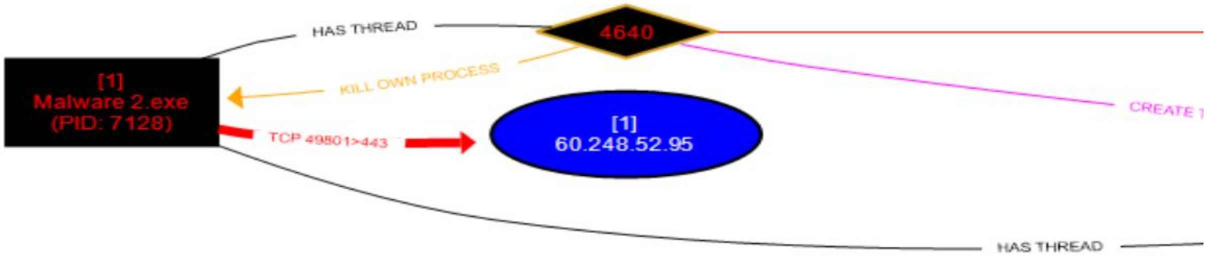
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

Self-Deletion Process


HAS THREAD
4640
KILL OWN PROCESS
[1]
Malware 2.exe
(PID: 7128)
CREATE T
TCP 49801>443
[1]
60.248.52.95
HAS THREAD