NIIT UNIVERSITY, NEEMRANA
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AGENT TESLA MALWARE ANALYSIS REPORT

Under the supervision of

Prof Dr. Ashu Sharma

Submitted by

Sarath Kumar – MT20ACS531

Mahesh M – MT20ACS516

Jerald Philip - MT20ACS511

Anurag Chowdhury – MT20ACS496

Swetha Reddy Burgala – MT20ACS541

Dheeraj – MT20ACS506

Table of Contents

1. INTRODUCTION

Threat intelligence reports categorize malware with information stealing characteristics under the following three headings: i) Memory scraping malware; ii) Credentials dumping malware; and iii) banking trojans.

Primarily found in point-of-sale (PoS) terminals, memory scraping malware aims to steal sensitive data directly from PoS terminal memory, e.g., plaintext card details, through regular expression-based signatures and subsequently harvesting them for card cloning purposes or similar abuse. FighterPOS and GlitchPOS [48]) are two notorious examples of this type of malware.

Banking trojans are mass information stealing malware, typically also doubling as fully-fledged botnets, reacting to commands broadcast over command and control (C2) channels. Zeus was one of the earliest banking trojans to rise to notoriety, followed by variants such as Citadel and Gameover Zeus, as well as other separate families including Dridex, Ursnif, Trickbot and Qakbot, that are still infecting machines up until very recently. They tend to share advanced functionality, namely: client-side web page content injection (webinjects), key-logging, connect-back functionality (stealthy back-dooring), and obfuscated command and control (C2) channels

On the other hand, credentials dumping malware is the PC version of PoS malware, with web browsers presenting common targets. Actually, the target range is much wider, with any process that retains passwords, hashes or credentials of any form, e.g., session tickets, in memory presenting a potential target. Notable examples include CStealer and KPOT Stealer.

A stealer is a Trojan that gathers information from a system. The most common form of stealers is those that gather logon information, like usernames and passwords, and then send the information to another system either via email or over a network.

A powerful, easy-to-use password stealing program known as Agent Tesla has been infecting computers since 2014, but recently this malware strain has seen a surge in popularity — attracting more than 6,300 customers who pay subscription fees to license the software. Although Agent Tesla includes a multitude of features designed to help it remain undetected on host computers, the malware's apparent creator seems to have done little to hide his real-life identity.
The proprietors of Agent Tesla market their product at agenttesla-dot-com, selling access to the software in licenses paid for via bitcoin, for prices ranging from $15 to $69 depending on the desired features.

The malware communicates with the C2 infrastructure via HTTP requests and supports multiple commands to steal any kind of information from the infected systems.

The Agent Tesla Web site emphasizes that the software is strictly "for monitoring your personel [sic] computer." The site's "about" page states that Agent Tesla "is not a malware.

Please, don't use for computers which is not access permission." To backstop this disclaimer, the site warns that any users caught doing otherwise will have their software licenses revoked and subscriptions canceled.
At the same time, the Agent Tesla Web site and its 24/7 technical support channel (offered via Discord) is replete with instances of support personnel instructing users on ways to evade antivirus software detection, use software vulnerabilities to deploy the product, and secretly bundle the program inside of other file types, such as images, text, audio and even **Microsoft Office** files.

The earliest versions of Agent Tesla were made available for free via a Turkish-language **WordPress** site that oddly enough remains online (agenttesla.wordpress-dot-com), although its home page now instructs users to visit the current AgentTesla-dot-com domain. Not long after that WordPress site was erected, its author(s) began charging for the software, accepting payments via a variety of means, including PayPal, Bitcoin and even wire transfer to several bank accounts in Turkey.

2. AGENT TESLA MALWARE BASICS

The Agent Tesla family of remote access trojan (RAT) malware has been active for over seven years, yet it remains one of the most common threats to Windows users. A variety of attackers use the malware to steal user credentials and other information from victims through screenshots, keyboard logging, and clipboard capture
Because the malware's compiler hard-codes operator-specific variables at build time, Agent Tesla behavior can vary widely—and the malware continues to evolve. Recent changes increased the number of applications targeted for credential theft, including web browsers, email clients, virtual private network clients, and other software that store user names and passwords. The evolution of the tool also extends to its delivery package with one version that now targets Microsoft's Anit-Malware Software Interface (AMSI) in an attempt to defeat endpoint protection software.

Agent Tesla exploits the following vulnerabilities:

- Exploiting MS office vulnerability CVE-2017-11882
- Exploiting MS office vulnerability CVE-2017-8570
- Archives with double extension executable (ZIP, RAR etc.)

Operating System

Windows	MacOS	Linux	Android
✓	✗	✗	✗

Risk & Impact

Impact	**High**
Risk	**Medium**

Fig 1: Agent Telsa Malware OS Details with the risk and Impact

Currently, there are two prominent variants of Agent Tesla still found in-the-wild:

- Version 2 – First released version of the malware, with a focus on obfuscation and anti-analysis.
- Version 3 – Additional customization options, advances in obfuscation and further functionality.

Both variants have varying levels of obfuscation. In version 2, a single function decrypts all the strings and allows them to be executed. In version 3, each encrypted string has its own function, which makes reverse engineering these static strings more difficult.

Both versions of the malware can communicate over HTTP, SMTP, and FTP. Recent variants of Agent Tesla version 3 have been seen abusing the chat platform Telegram. This latter version also provides the option to use a Tor client to encrypt communications.

We have selected **Agent Tesla Malware Version 2** as part of our analysis.

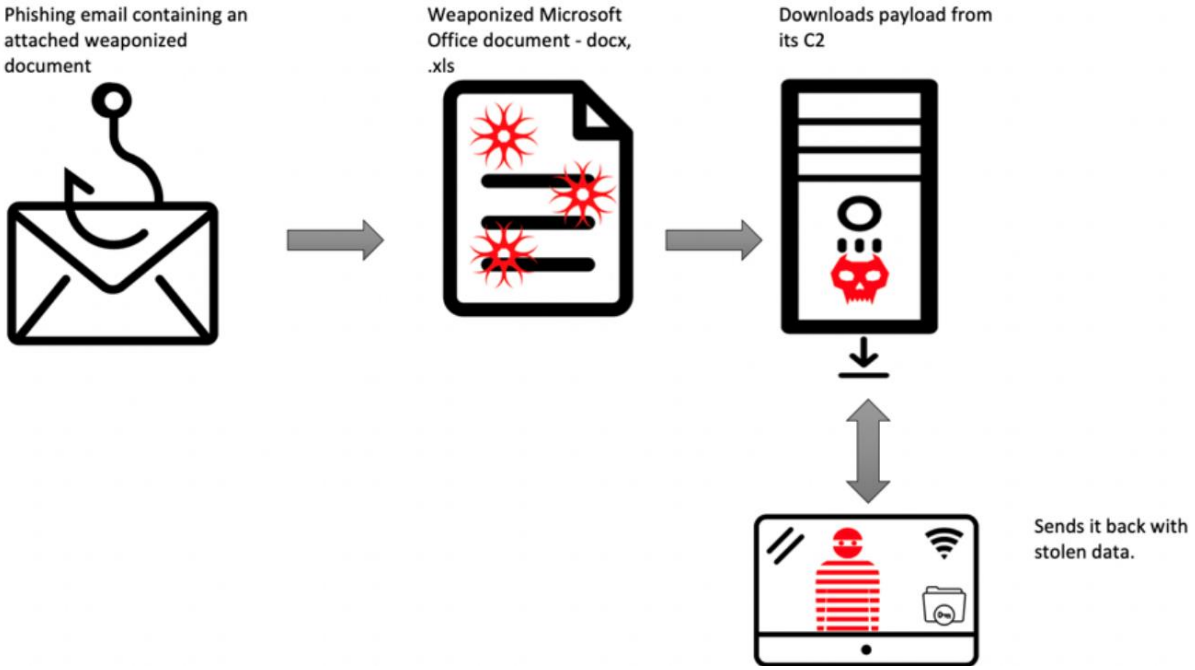


Fig 2: Basic Working of Agent Tesla

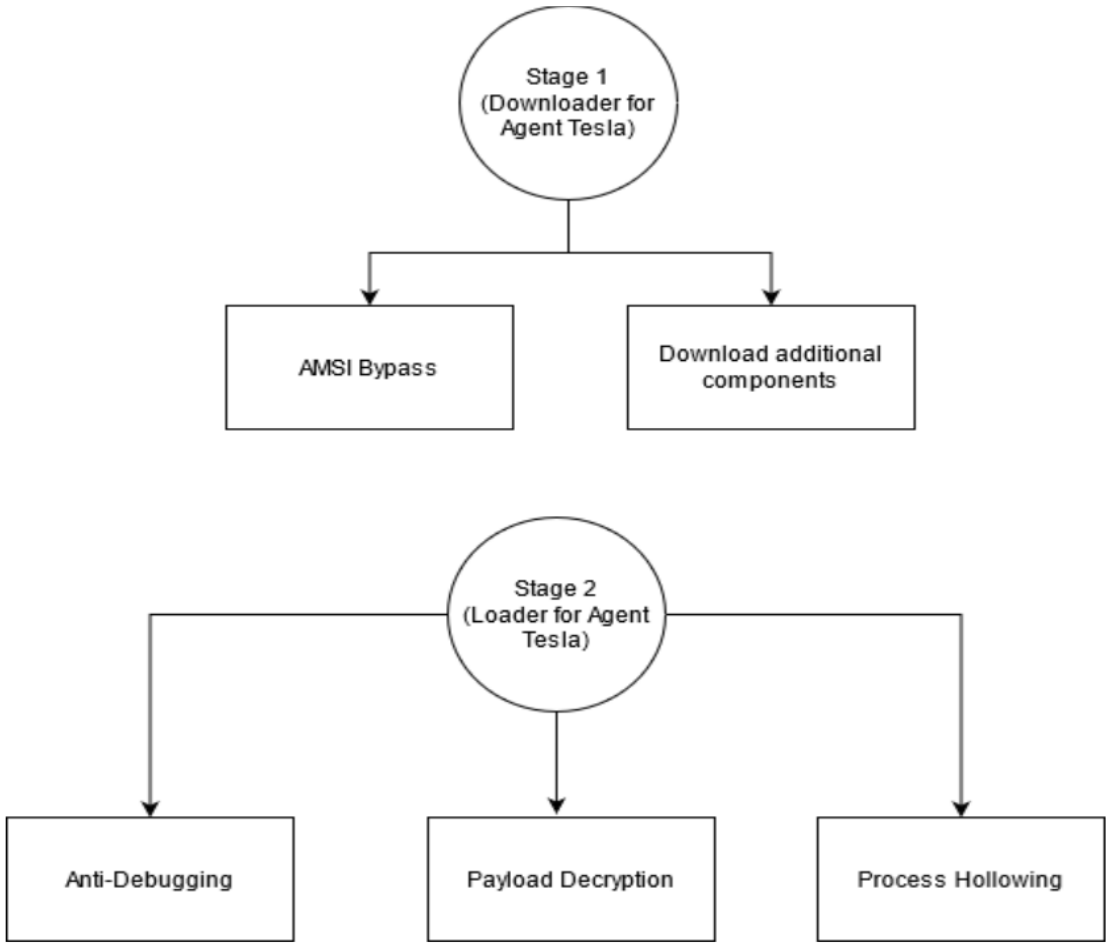


Fig 3: Stages of Agent Tesla Malware

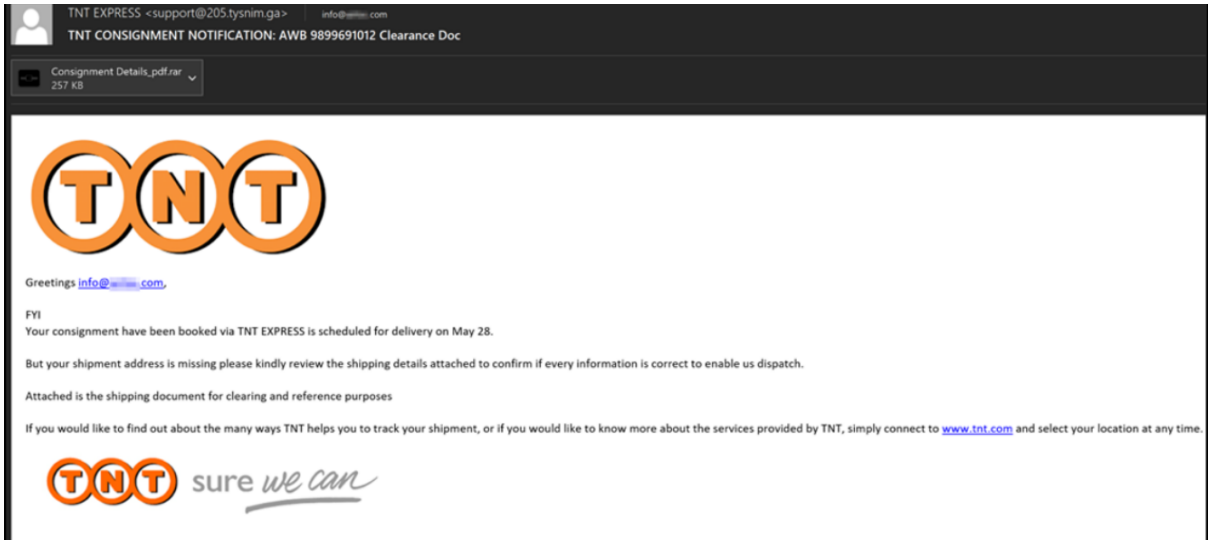


Fig 4: Agent Tesla Phishing email

We have got these malwares from the following online sources:

https://app.any.run/tasks/c3022529-4391-4a6a-8528-9b1c1f4de3c9/ - Stage 1 Malware

https://malshare.com/sample.php?action=detail&hash=fec8af4dbb834256ebaf7fbc4d722915 - Intermediate Downloader Malware

https://app.any.run/tasks/c249681e-3d96-4195-a8c7-36303968dd82/ - Stage 2 Malware

In the first stage, the malware is dropped in malicious spam emails as an attachment. This downloader part checks the presence of *AMSI* in the system and then tries to disable it. Then it attempts to download the second stage from websites such as *Pastebin* and Pastebin clone called *Hastebin*. It combines the various chunks downloaded to enable the Stage 2 part.

The second stage of the malware, tries to avoid sandbox analysis through debugging. Once the checks are passed successfully, the decrypted part creates a child process, and then injects itself to another process using the process hollowing technique. Then it uses an exfiltration carrier type that can be either HTTP, SMTP, FTP, or TELEGRAM. Then it proceeds with the info stealing parts such as browser credential gathering and copy of clipboard contents.

To analyze, we have used the following tools:

PEStudio - Static Analysis

DNSpy – Decompiler/Debugger

X32DGB – Debugger

Process Monitor – Dynamic Analysis

Process Explorer – Dynamic Analysis

Wireshark – Dynamic Analysis

Task Manager – Dynamic Analysis

XAMPP - Dynamic Analysis (Web Server)

Process Dumper (pd64) – Dynamic Analysis (Dump from memory)

Task Scheduler – Dynamic Analysis

3. AGENT TESLA MALWARE ANALYSIS

We have downloaded the malware from the resources mentioned above.

STATIC ANALYSIS OF 1st Stage

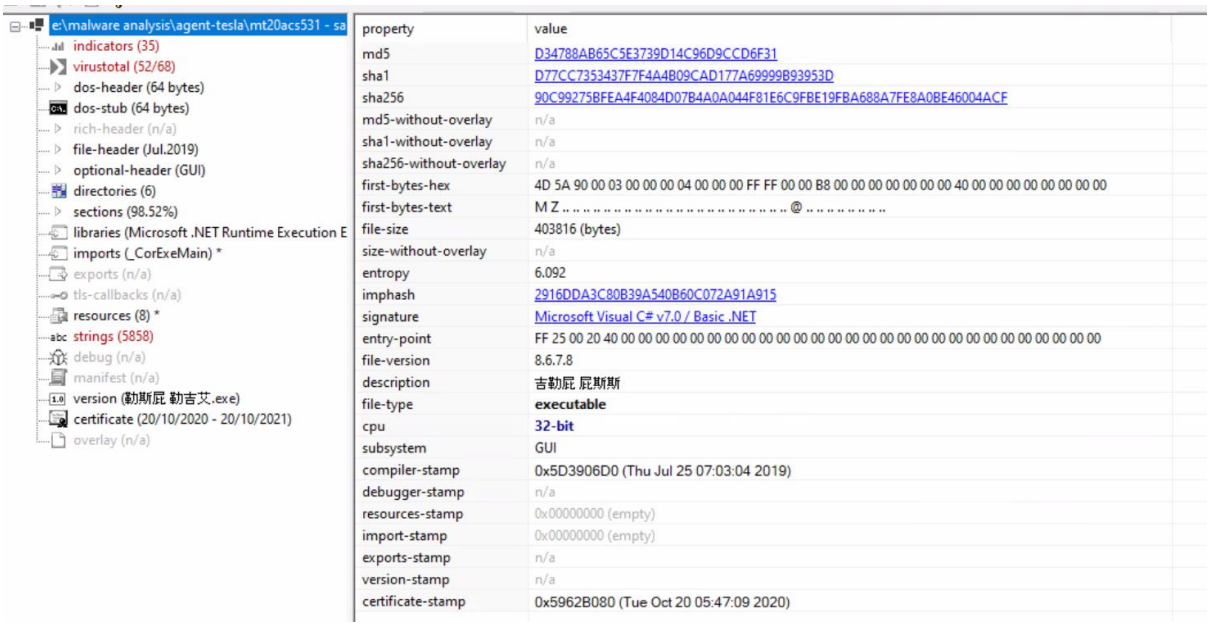


Fig 5: PEStudio – Static Analysis of 1st Stage Malware

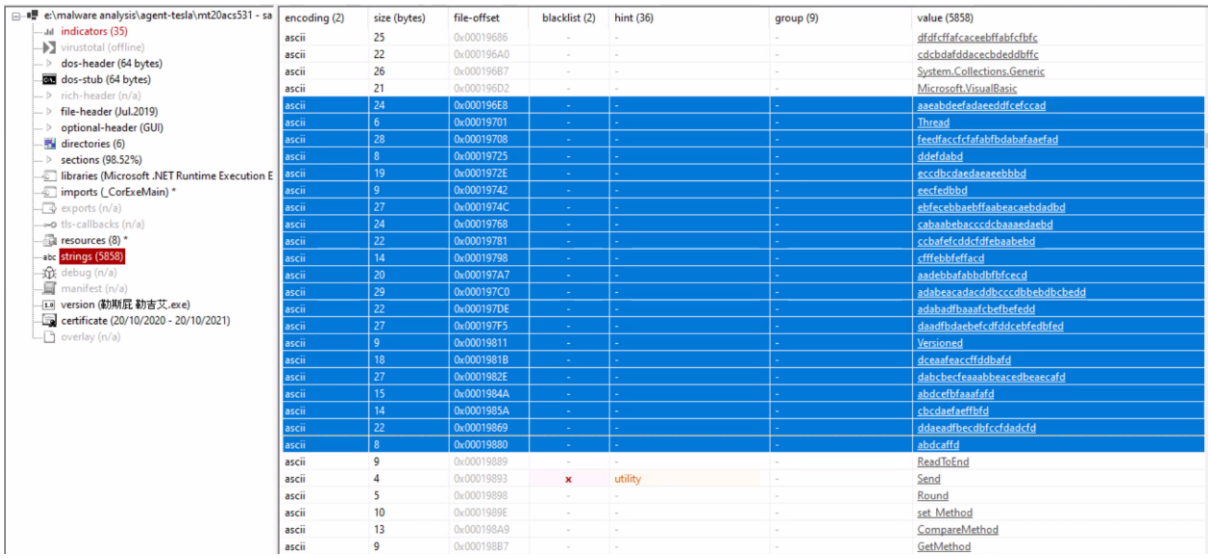


Fig 6: PEStudio – Static Analysis of 1st Stage Malware (Identified Obfuscated Strings)

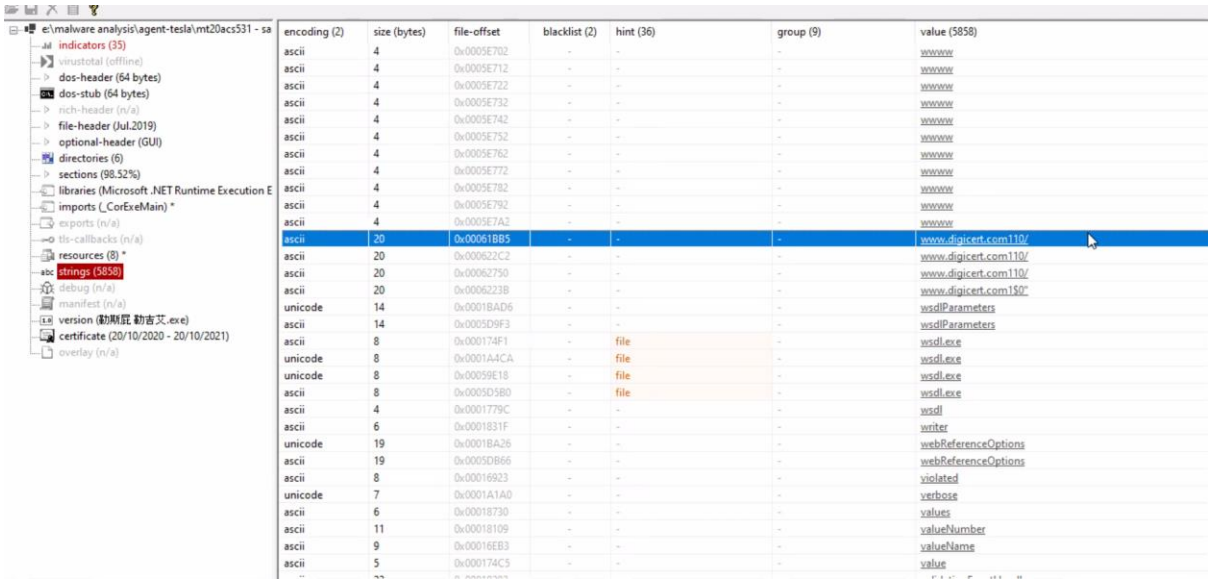


Fig 7: PEStudio – Static Analysis of 1st Stage Malware (Identified use of DigiCert)

From these, we have identified that it uses obfuscation and also using DigiCert i.e Digital Certificates

As we have understood from Fig 5, it is compiled using C# or .Net. So, we have used DNSpy which is a reverse engineering tool.

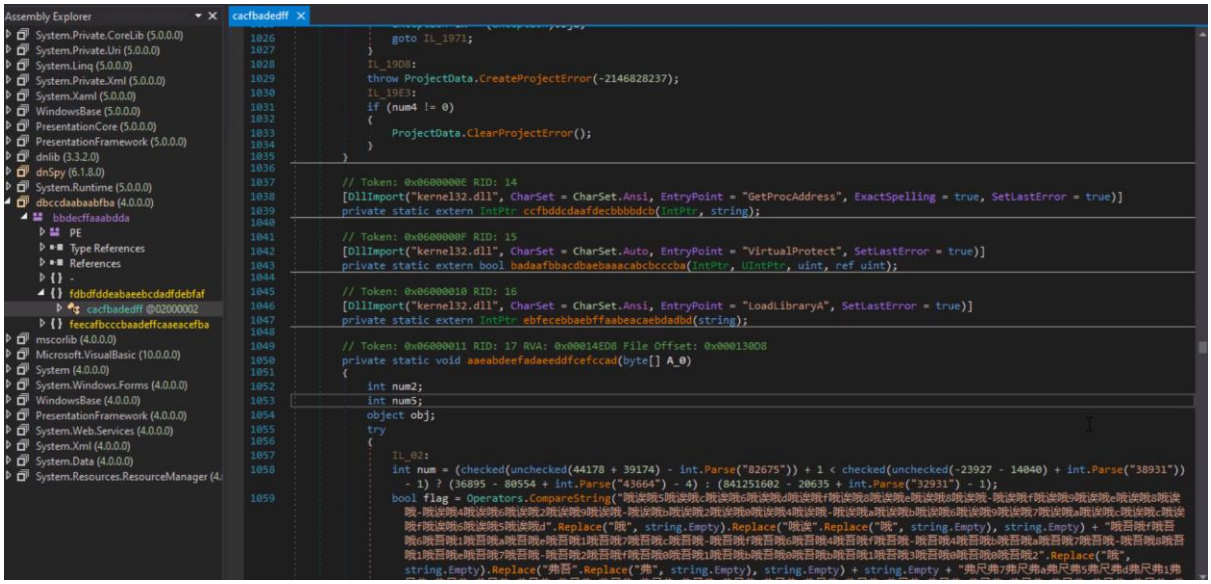


Fig 8:DNSpy – Static Analysis of 1st Stage Malware (use of LoadLibraryA and GetProcAddress)

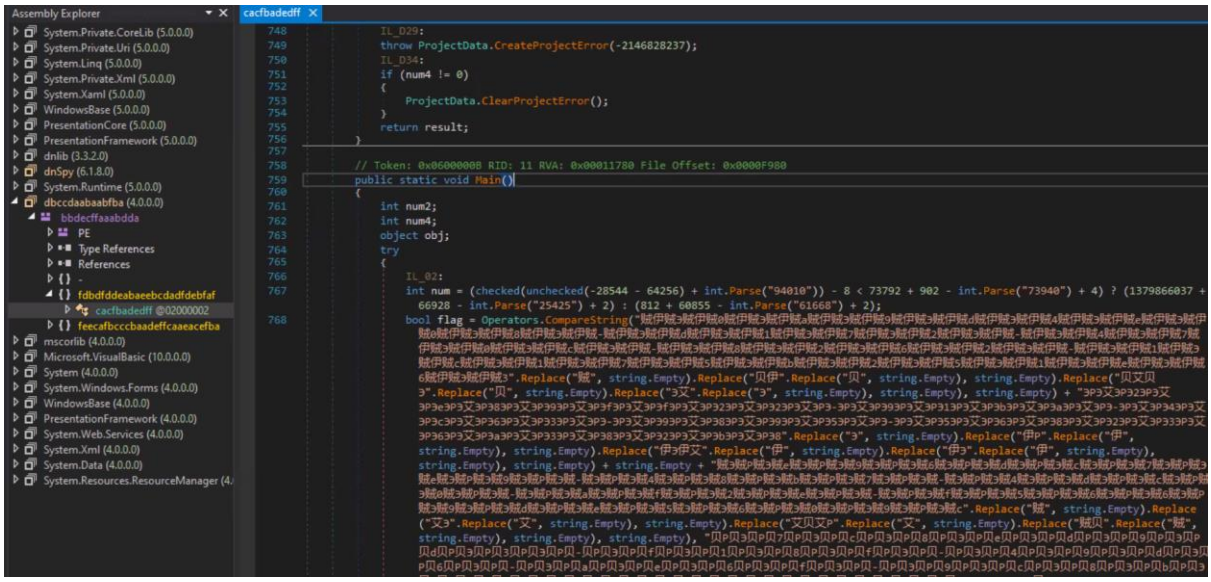


Fig 9:DNSpy – Static Analysis of 1st Stage Malware (String Obfuscation)

From this, we can say that Malware uses LoadLibraryA and GetProcAddress where LoadLibraryA are responsible for for loading a module specified as parameter into the address space of the calling process. In conjunction with that, GetProcAddress retrieves the address of an exported function or variable from the specified dynamic-link library (DLL). Here, it also performs String Replacement/Obfuscation.

DYNAMIC ANALYSIS OF 1st Stage

So, we perform Dynamic Analysis by execution. In this case, we have initially disabled the network interface and identified the following:

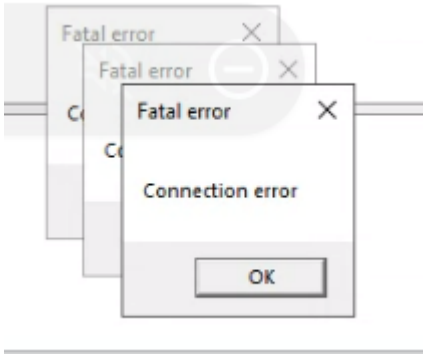


Fig 10: Fatal Error on executing the malware

From this, we have understood that if Internet or network interface is disabled, it results in Connection Error or Fatal Error and it retries continuously to connect to the network.

So, we have created a dummy XAMPP Server where we have added the pastebin and hastebin IP address to the localhost to have a fake network available.

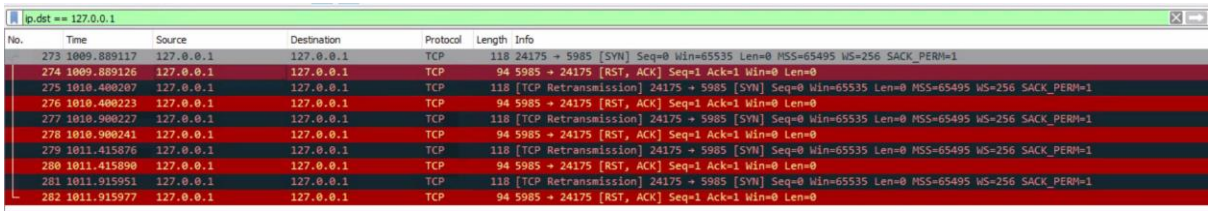


Fig 11: Wireshark: Malware trying to access hastebin and digicert at 127.0.0.1 as we have modified the host's file

Fig 12: Task Manager: Identified that the malware is running

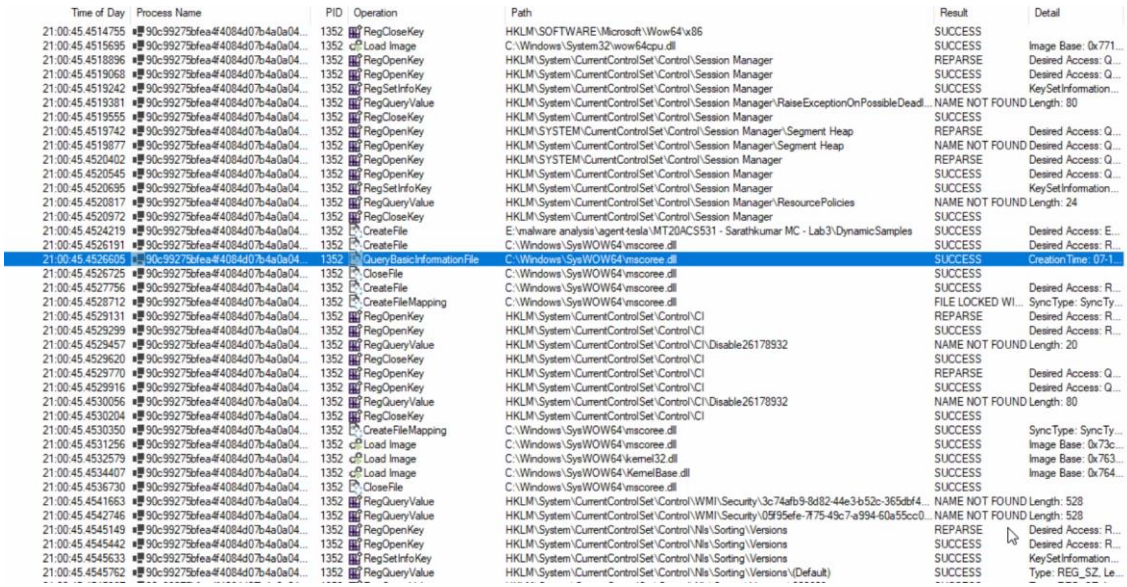


Fig 13: Process Monitor: Malware trying to access mscore.dll

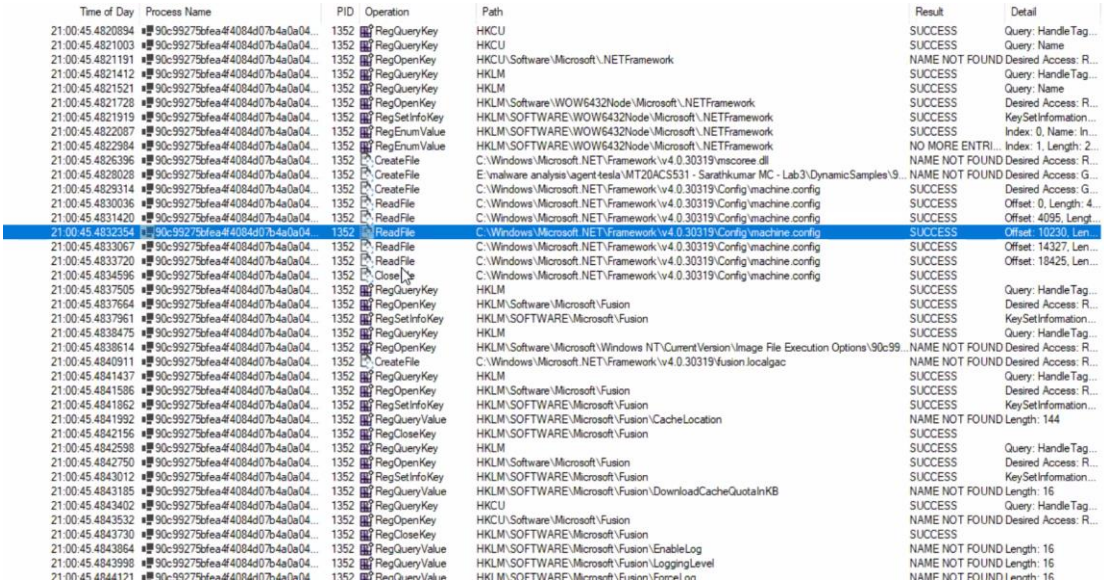


Fig 14: Process Monitor: Malware trying to access machine config and other HKLM registers

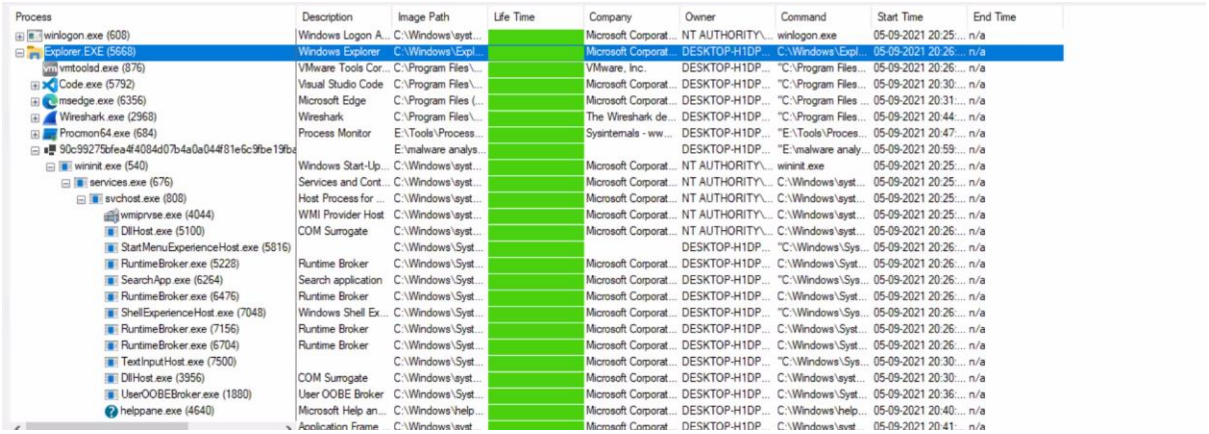


Fig 15: Process Monitor: Malware working under Explorer.exe and having multiple child processes running

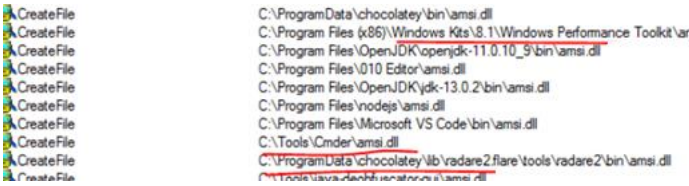


Fig 16: Process Monitor: Malware trying to disable AMSI.dll

From this dynamic analysis, we have identified that as soon as malware executes, it looks to connect with HasteBin/PastePin where it will try to download additional downloader files which is necessary for Stage 2 malware and it is trying to disable AMSI.dll

STATIC ANALYSIS OF Intermediate Downloader

Since, we have not connected to Internet, we have downloaded the intermediate downloader from other sources.

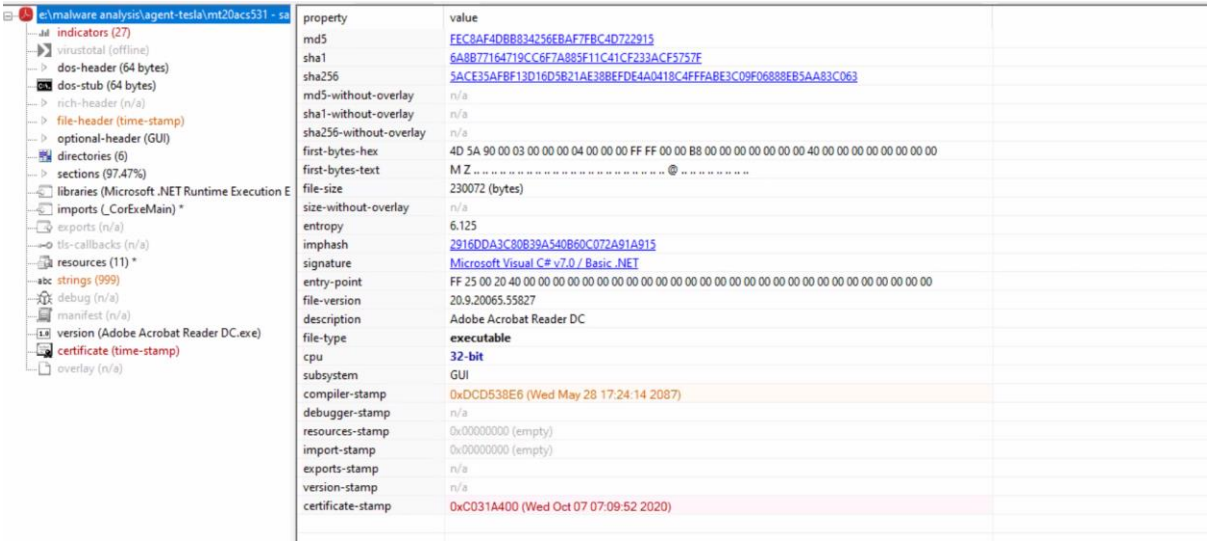


Fig 17: PEStudio: Intermediate Downloader

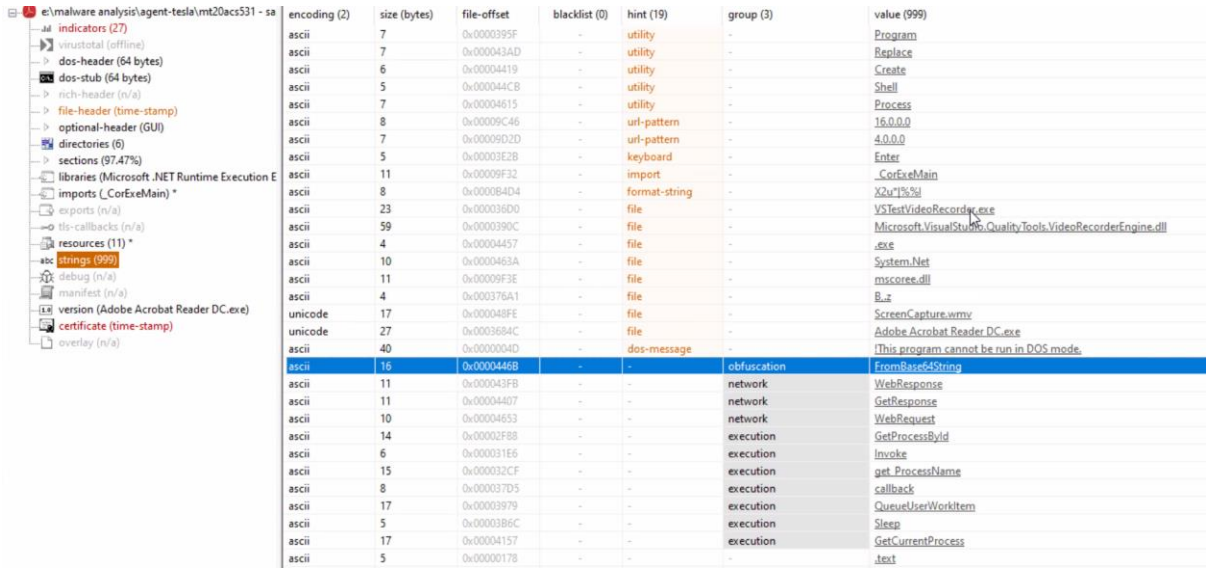


Fig 18: PEStudio: Intermediate Downloader Strings (Identified that it is using obfuscation)

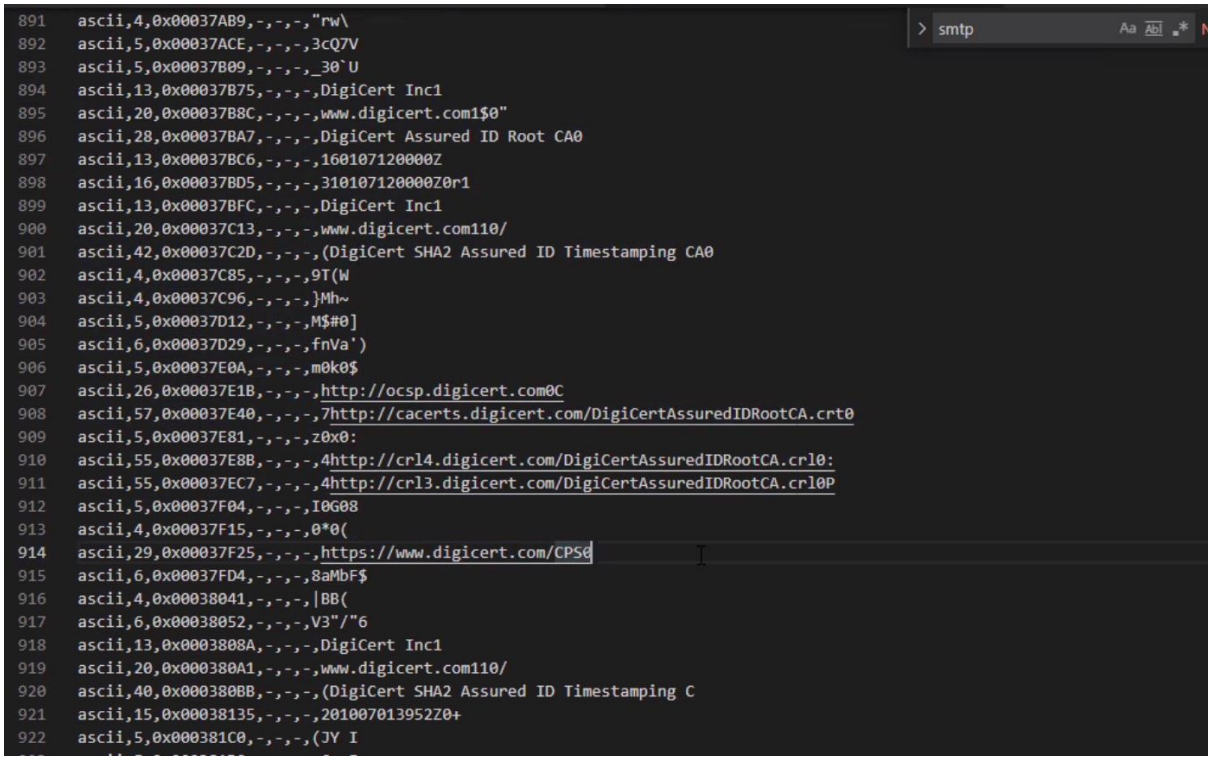


Fig 19: PEStudio: Intermediate Downloader Strings (Identified that it is also digitcert) – Copied to text editor

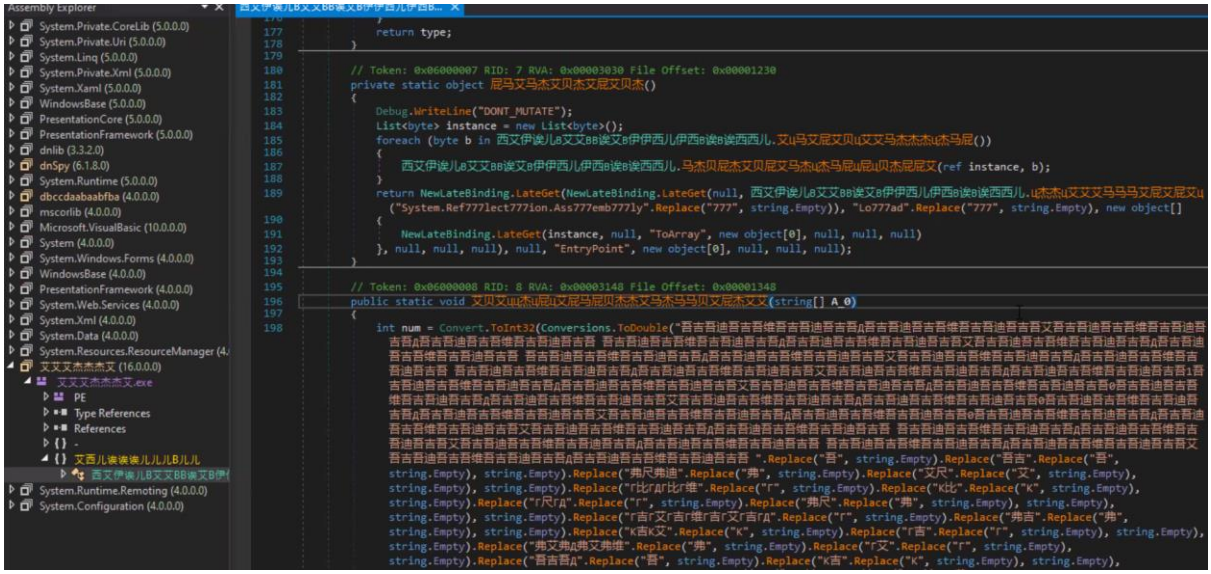


Fig 20: DNSpy: Intermediate Downloader De-compiler (uses String Obfuscation)

From this, we have identified, the intermediate downloader also uses String Obfuscation and having Digicert for digital certificates

DYNAMIC ANALYSIS OF Intermediate Downloader

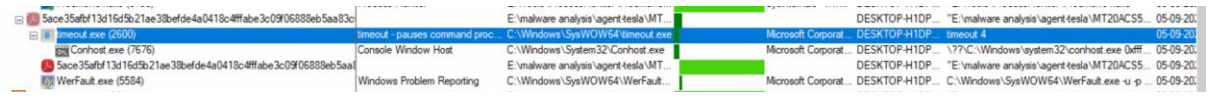


Fig 21: Process Monitor: Timeout.exe for timeout used for pausing command processing

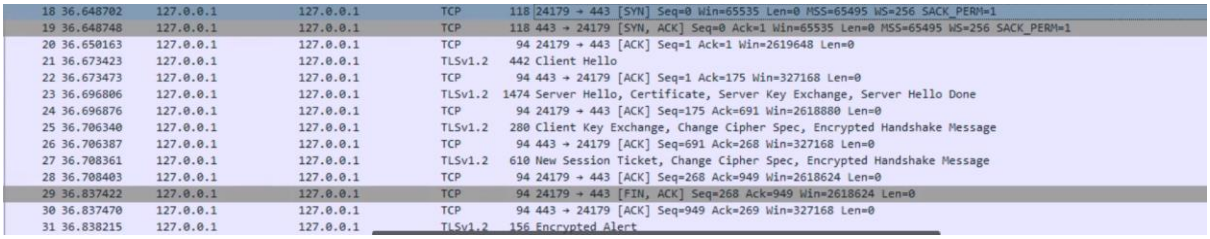


Fig 22: Wireshark: It is trying to access Internet for downloading other malwares (including Stage 2 malware and their dependencies)

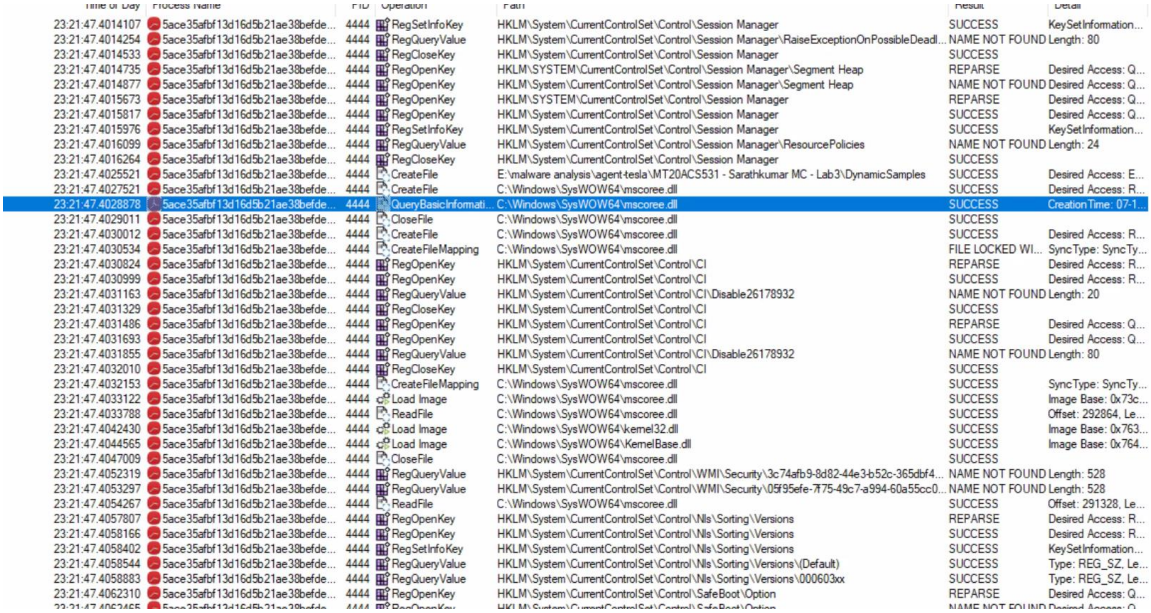


Fig 23: Process Monitor: It is trying to access mscorr.dll and Registry

From this, we have understood that it is trying to access Internet for more downloadable items including 2nd Stage Malware for further processing and tries to modify Registry accordingly

STATIC ANALYSIS OF 2nd Stage Malware

As we have not connected to Internet, we have downloaded the malware from other sources

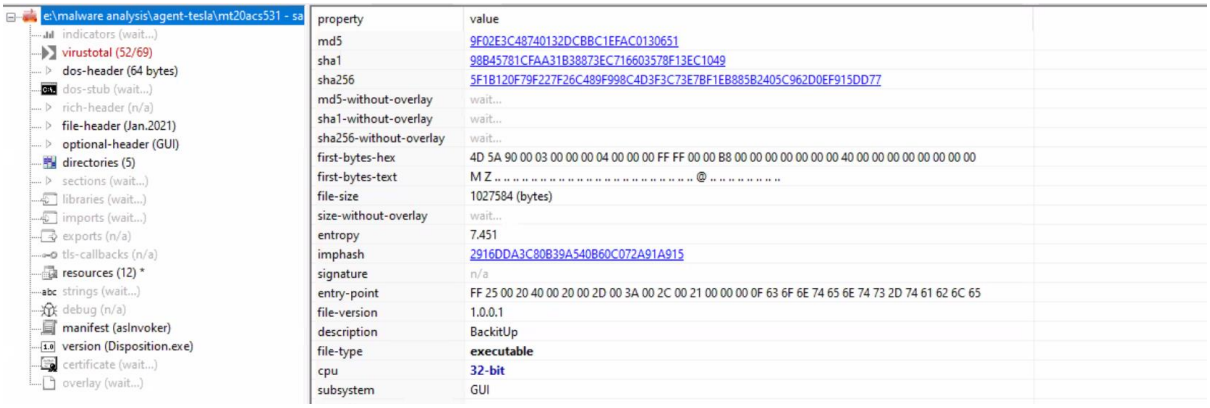


Fig 24: PEStudio: 2nd Stage Malware

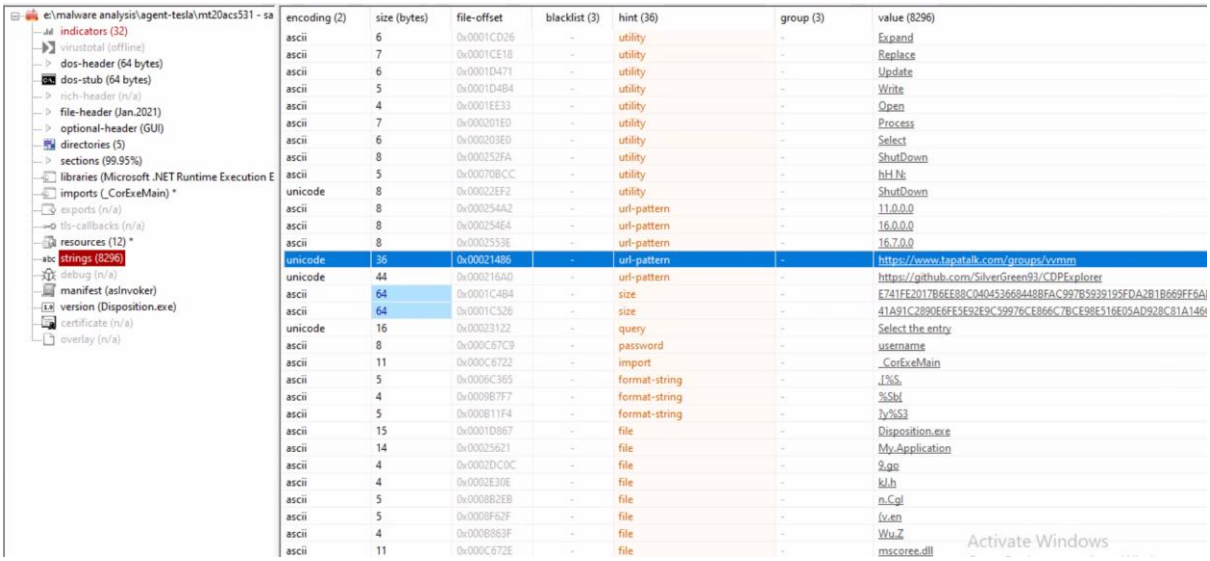


Fig 25: PEStudio: 2nd Stage Malware (we can see it is having URL Strings like tapatalk)

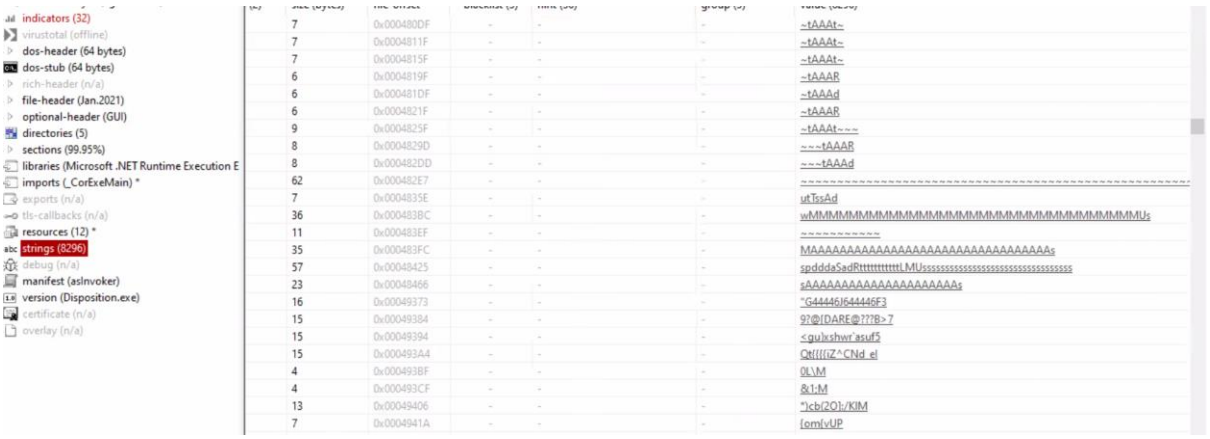


Fig 26: PEStudio: 2nd Stage Malware (we can see it is Obfuscated)

encoding (2)	size (bytes)	file-offset	blacklist (3)	hint (36)	group (3)	value (8296)
ascii	6	0x0001CD26	-	utility	-	Expand
ascii	7	0x0001CE18	-	utility	-	Replace
ascii	6	0x0001D471	-	utility	-	Update
ascii	5	0x0001D4B4	-	utility	-	Write
ascii	4	0x0001EE33	-	utility	-	Open
ascii	7	0x000201E0	-	utility	-	Process
ascii	6	0x000203E0	-	utility	-	Select
ascii	8	0x000252FA	-	utility	-	ShutDown
ascii	5	0x00070BCC	-	utility	-	hH N:
unicode	8	0x00022EF2	-	utility	-	ShutDown
ascii	8	0x000254A2	-	url-pattern	-	11.0.0.0
ascii	8	0x000254E4	-	url-pattern	-	16.0.0.0
ascii	8	0x0002553E	-	url-pattern	-	16.7.0.0

Fig 27: PEStudio: 2nd Stage Malware (Different Functionalities of malware)

ascii	35	0x0001C14A	-	-	-	get_CopyAssetInfoToolStripMenuItem1
ascii	35	0x0001C16E	-	-	-	set_CopyAssetInfoToolStripMenuItem1
ascii	7	0x0001C192	-	-	-	m_Form1
ascii	9	0x0001C19A	-	-	-	get_Form1
ascii	9	0x0001C1A4	-	-	-	set_Form1
ascii	21	0x0001C1AE	-	-	-	get_ContextMenuStrip1
ascii	21	0x0001C1C4	-	-	-	set_ContextMenuStrip1
ascii	10	0x0001C1DA	-	-	-	get_Timer1
ascii	10	0x0001C1E5	-	-	-	set_Timer1
ascii	15	0x0001C1F0	-	-	-	get_PictureBox1
ascii	15	0x0001C200	-	-	-	set_PictureBox1
ascii	13	0x0001C210	-	-	-	get_GroupBox1
ascii	13	0x0001C21E	-	-	-	set_GroupBox1
ascii	12	0x0001C22C	-	-	-	get_ListBox1
ascii	12	0x0001C239	-	-	-	set_ListBox1
ascii	10	0x0001C246	-	-	-	ReadUInt32
ascii	9	0x0001C251	-	-	-	ReadInt32
ascii	7	0x0001C25B	-	-	-	ToInt32
ascii	10	0x0001C266	-	-	-	get_Label2
ascii	10	0x0001C271	-	-	-	set_Label2
ascii	22	0x0001C27C	-	-	-	get_ToolStripMenuItem2
ascii	22	0x0001C293	-	-	-	set_ToolStripMenuItem2

Fig 28: PEStudio: 2nd Stage Malware (using PictureBox, GroupBox and ListBox)

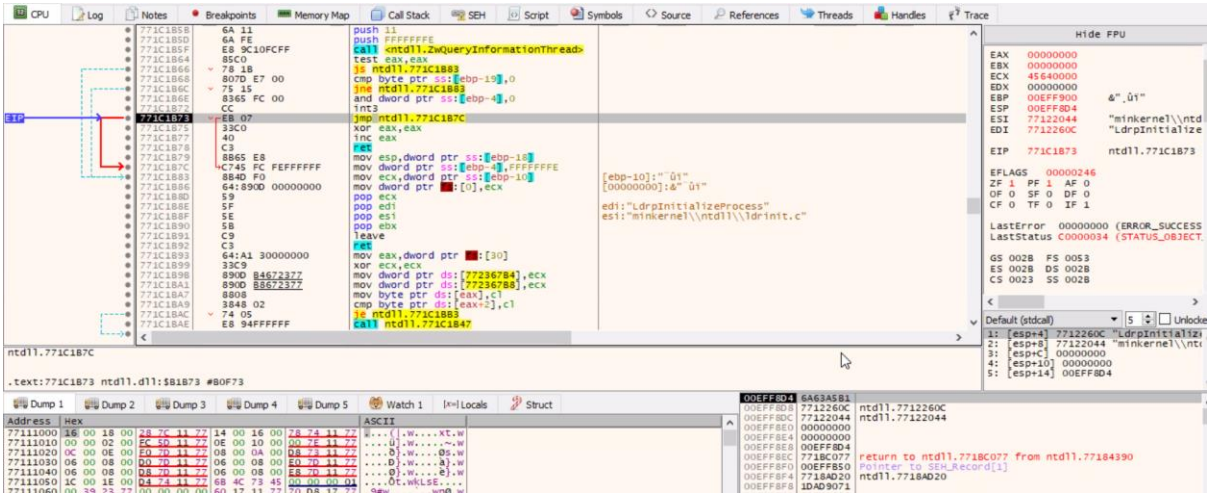


Fig 29: x32DGB: 2nd Stage Malware (To extract the malware from memory)

However, we have not been able to identify and we found 5 4D 5A files (possibly different executables with many legitimate and a single payload with malware)

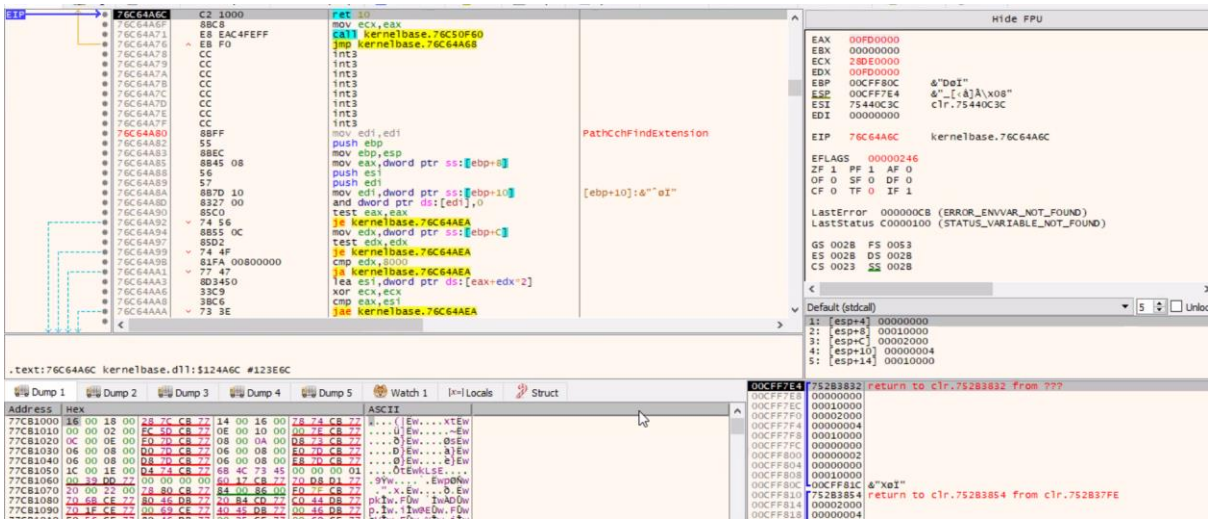


Fig 30: x32DGB: 2nd Stage Malware (To extract the malware from memory) – Identified the entry point and provided the breakpoint where it is required.

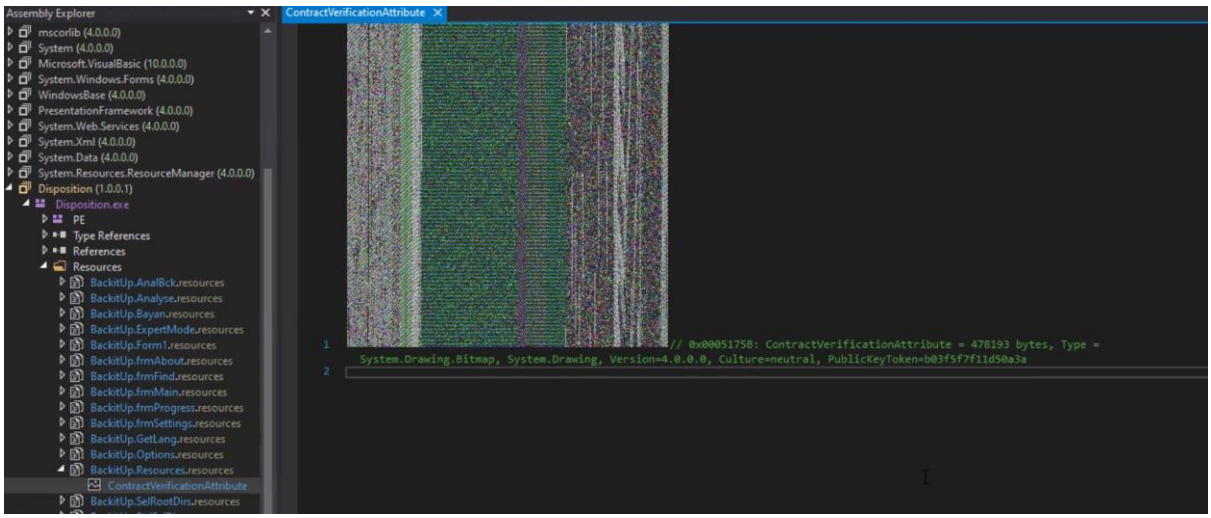


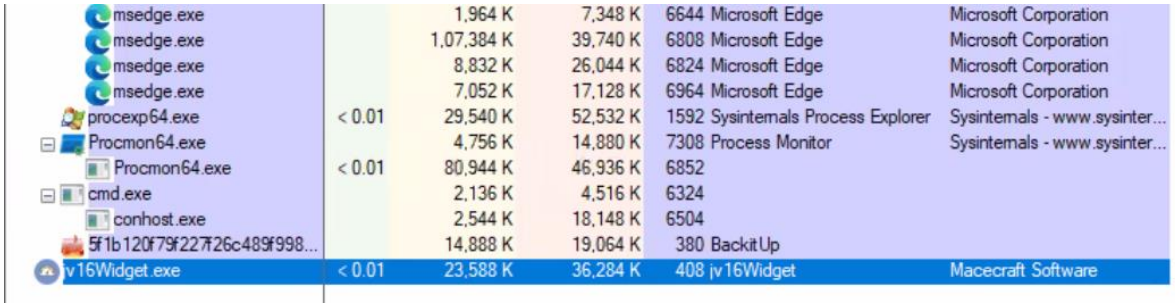
Fig 31: DNSpy: 2nd Stage Malware (Image Obfuscation is done)

Fig 32: DNSpy: 2nd Stage Malware (Keylogger)

```
275             {
276                 global::A.b.A += global::A.b.e;
277                 num = 10;
278             }
279             if (num == 17)
280             {
281                 global::A.b.A = string.Concat(array);
282                 num = 18;
283             }
284             if (num == 3)
285             {
286                 text = text.Replace(6EA5F15D-F238-4334-954E-F5D67B31D764.bN(), 6EA5F15D-F238-4334-954E-F5D67B31D764.bn());
287                 num = 4;
288             }
289             if (num == 2)
290             {
291                 text = global::A.B.Computer.Clipboard.GetText();
292                 num = 3;
293             }
294             if (num == 11)
```

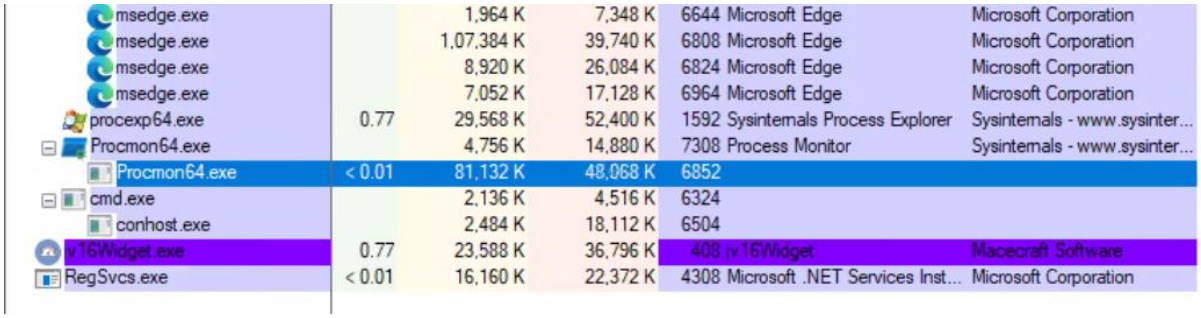
Fig 33: DNSpy: 2nd Stage Malware (Clipboard)

DYNAMIC ANALYSIS OF 2nd Stage Malware



msedge.exe		1,964 K	7,348 K	6644 Microsoft Edge	Microsoft Corporation
msedge.exe		1,07,384 K	39,740 K	6808 Microsoft Edge	Microsoft Corporation
msedge.exe		8,832 K	26,044 K	6824 Microsoft Edge	Microsoft Corporation
msedge.exe		7,052 K	17,128 K	6964 Microsoft Edge	Microsoft Corporation
procexp64.exe	< 0.01	29,540 K	52,532 K	1592 Sysinternals Process Explorer	Sysinternals - www.sysinter...
Procmon64.exe		4,756 K	14,880 K	7308 Process Monitor	Sysinternals - www.sysinter...
Procmon64.exe	< 0.01	80,944 K	46,936 K	6852	
cmd.exe		2,136 K	4,516 K	6324	
conhost.exe		2,544 K	18,148 K	6504	
5f1b120f79f227f26c489f998...		14,888 K	19,064 K	380 BackitUp	
jv16Widget.exe	< 0.01	23,588 K	36,284 K	408 jv16Widget	Macecraft Software

Fig 34: Process Monitor: 2nd Stage Malware (As soon as we execute)



msedge.exe		1,964 K	7,348 K	6644 Microsoft Edge	Microsoft Corporation
msedge.exe		1,07,384 K	39,740 K	6808 Microsoft Edge	Microsoft Corporation
msedge.exe		8,920 K	26,084 K	6824 Microsoft Edge	Microsoft Corporation
msedge.exe		7,052 K	17,128 K	6964 Microsoft Edge	Microsoft Corporation
procexp64.exe	0.77	29,568 K	52,400 K	1592 Sysinternals Process Explorer	Sysinternals - www.sysinter...
Procmon64.exe		4,756 K	14,880 K	7308 Process Monitor	Sysinternals - www.sysinter...
Procmon64.exe	< 0.01	81,132 K	48,068 K	6852	
cmd.exe		2,136 K	4,516 K	6324	
conhost.exe		2,484 K	18,112 K	6504	
jv16Widget.exe	0.77	23,588 K	36,796 K	408 jv16Widget	Macecraft Software
RegSvcs.exe	< 0.01	16,160 K	22,372 K	4308 Microsoft .NET Services Inst...	Microsoft Corporation

Fig 35: Process Monitor: 2nd Stage Malware (After sometime, RegSvcs.exe is executing)

After a while, we see that another process is created, namely RegSvc. This is a process hollowing technique, where Agent Tesla suspends the state of a legitimate process, then unmaps (hollows) the used memory location and loads the malicious code.

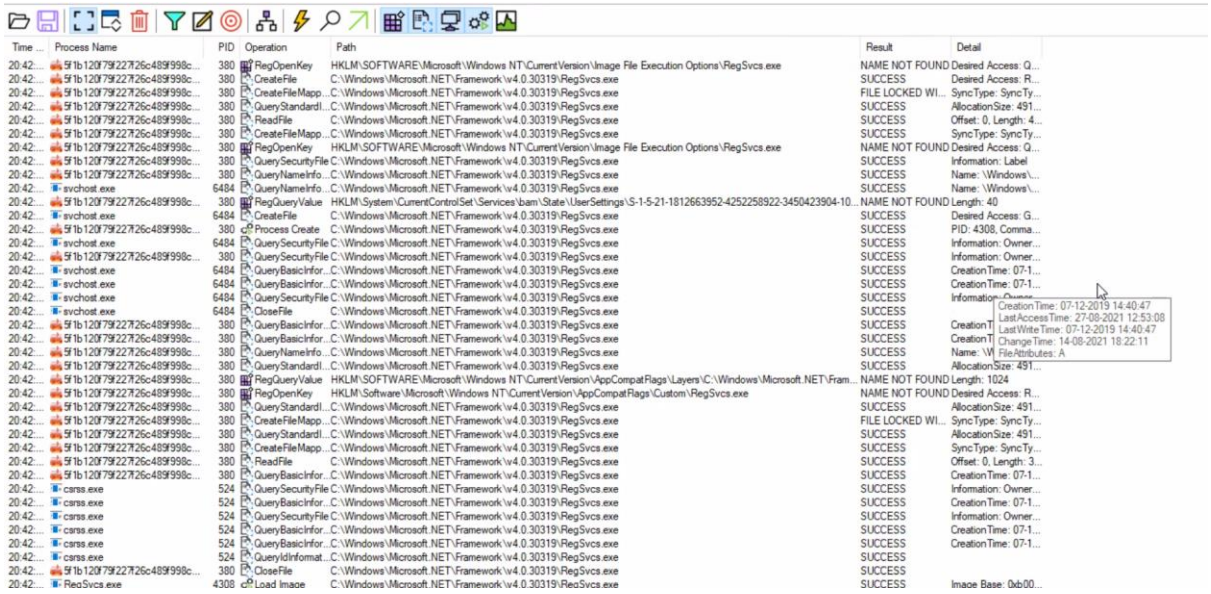


Fig 36: Process Monitor: 2nd Stage Malware (Modify/access Registry and uses RegSvcs.exe)

Here, RegSvcs.exe then begins searching the host for different kinds of information.

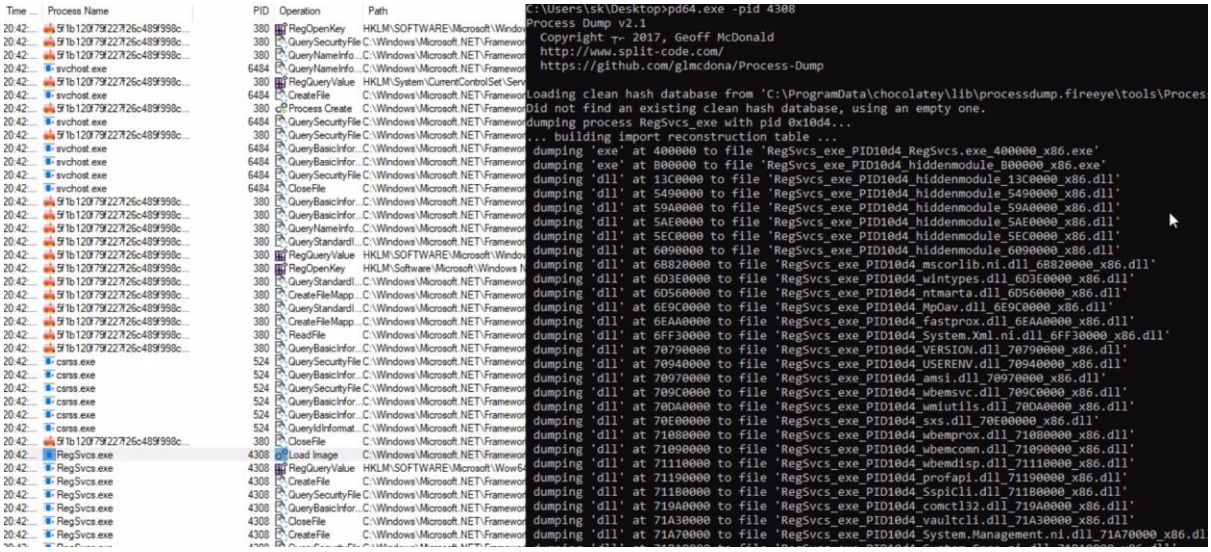


Fig 37: Process Monitor and Process Dump: 2nd Stage Malware (Dumping RegSvcs)

We use Process Dump to extract all the artifacts that exists in the memory location of RegSvcs exe

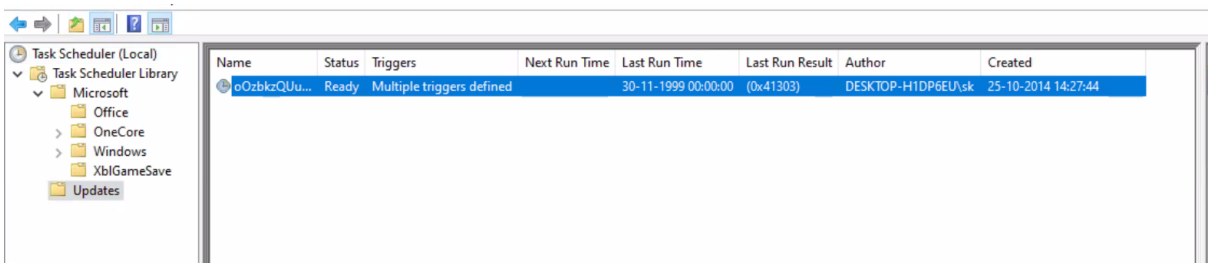


Fig 38: Process Monitor and Process Dump: 2nd Stage Malware (Dumping RegSvcs)

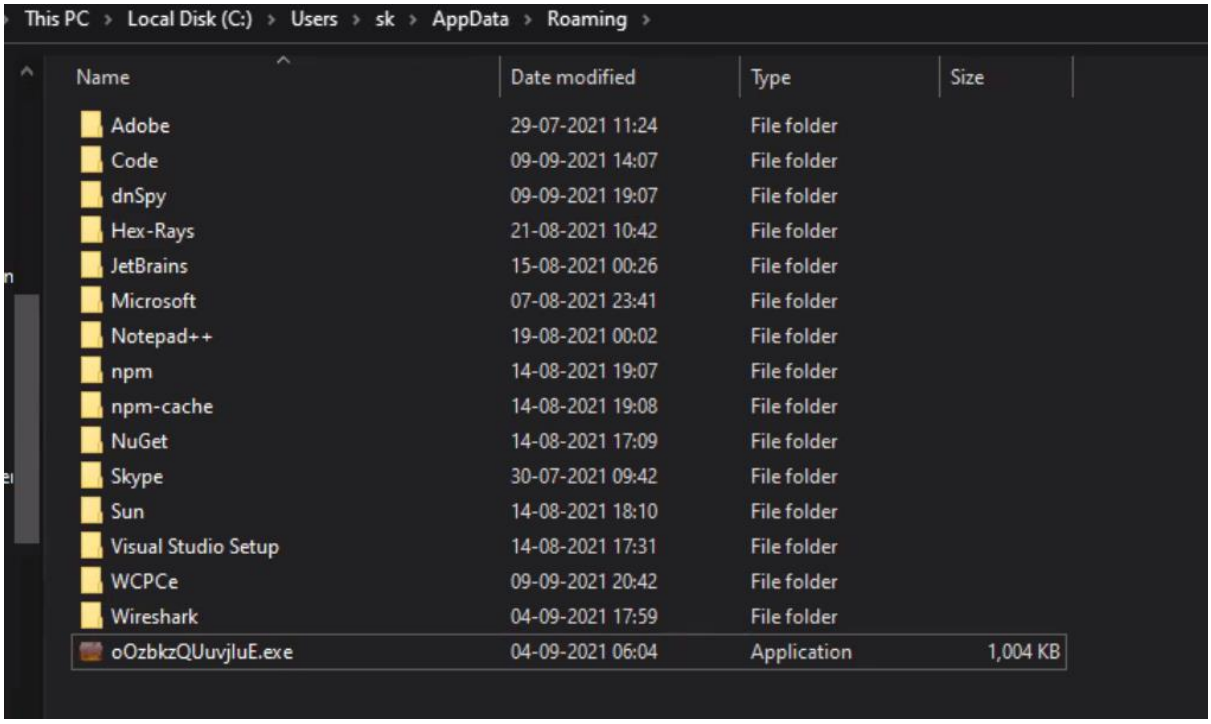


Fig 39: Malware creates an exe file in AppData folder

Here, from this, we can see that malware creates an exe file and adds themselves to registry for persistence.

The threat will search through the victim's machine for a pre-defined list of specific software and utilities. These lists tend to vary per sample, but they can be quite long. The goal of this functionality is to locate software to steal information from, by extracting saved credentials. This stolen information is stored for later exfiltration.

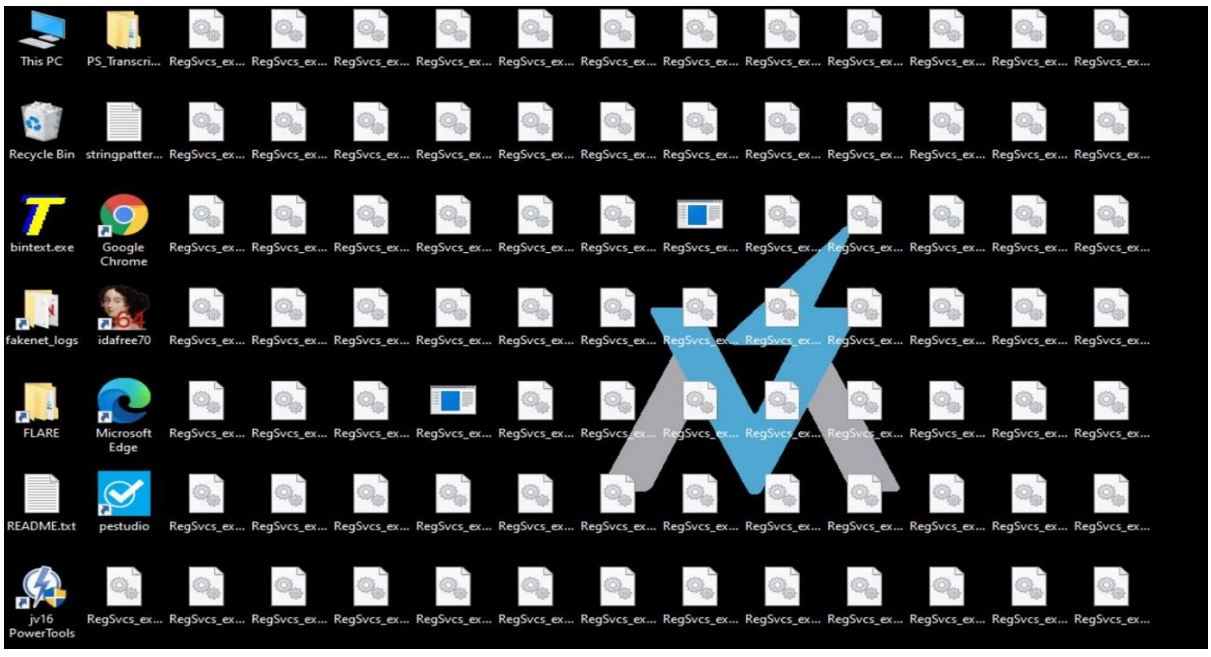


Fig 40: Malware activities after some time of execution where it copies the RegSvcs.exe multiple times

RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\CentBrowser\User Data
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\Yandex\YandexBrowser\User Data
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\BraveSoftware\Brave-Browser\User Data
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\Coowon\Coowon\User Data
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\Orbitum\User Data
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\Chromium\User Data
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\CocCoc\Browser\User Data
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Roaming\Opera Software\Opera Stable
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\Vivaldi\User Data
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\Amigo\User Data
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\Torch\User Data
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\360Chrome\Chrome\User Data
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\Kometa\User Data
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\Comodo\Dragon\User Data

Fig 41: Malware searching for user data in different browsers

RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Roaming\The Bat!
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Roaming\Thunderbird\profiles.ini
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Roaming\Thunderbird\profiles.ini
RegSvcs.exe	2540	RegOpenKey	HKCU\Software\IncrediMail\Identities
RegSvcs.exe	2540	RegOpenKey	HKCU\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
RegSvcs.exe	2540	RegOpenKey	HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
RegSvcs.exe	2540	RegOpenKey	HKCU\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Roaming\Claws-mail

Fig 42: Malware searching for email data

4. YARA RULES

Agent Tesla Malware Yara for all the files can be identified here at:

https://github.com/mcsarathkumar/AgentTeslaAnalysis/blob/master/AgentTesla_Static_and_Dynamic_Analysis.yara

```
FLARE 11-09-2021 09:39:29
PS E:\malware analysis\agent-tesla\MT20ACS531 - Sarathkumar MC - Lab3\dynamic analysis > yara .\AgentTesla_Static_and_DynamicAnalysis.yara .\samples\
AgentTeslaStaticDynamicRule .\samples\\5ace35afbf13d16d5b21ae38befde4a0418c4fffabe3c09f06888eb5aa83c063.exe
AgentTeslaStaticDynamicRule .\samples\\90c99275bfea4f4084d07b4a0a044f81e6c9fbe19fba688a7fe8a0be46004acf.exe
AgentTeslaStaticDynamicRule .\samples\\5f1b120f79f227f26c489f998c4d3f3c73e7bf1eb885b2405c962d0ef915dd77.exe
FLARE 11-09-2021 09:39:42
```

5. HOW TO OVERCOME IT?

A good AV can detect this malware.
Update the AV Database
Open the file only when it is received from a trusted party and make sure the all the software is updated regularly.

6. CONCLUSION

Agent Tesla collects credentials from files in VPN, FTP clients and download managers, also, it collects credentials from the system registry and sends them to a C&C server controlled by cyber criminals.
New Agent Tesla version is capable of starting every time the operating system starts, also, it can disable various operating system's features or prevent victims from using them. Additionally, Agent Tesla can restart a computer, take screenshots of victim's screen and send them to attacker's email address. Hence, proper care has to be taken for Phishing emails/documents shared via other platforms.

7. REFERENCES

https://www.riskiq.com/blog/external-threat-management/agent-tesla-trend-analysis
https://blogs.blackberry.com/en/2021/06/threat-thursday-agent-tesla-infostealer-malware
https://krebsonsecurity.com/2018/10/who-is-agent-tesla/
https://whatis.techtarget.com/definition/process-hollowing
https://georgemakrakisblog.azurewebsites.net/2021/06/03/agent-tesla-malware-analysis-report/
https://blogs.blackberry.com/en/2021/06/threat-thursday-agent-tesla-infostealer-malware
https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882