



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



NIIT UNIVERSITY, NEEMRANA
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Table of Contents

1. INTRODUCTION.....	3
2. AGENT TESLA MALWARE BASICS	4
3. AGENT TESLA MALWARE ANALYSIS.....	8
4. YARA RULES.....	22
5. HOW TO OVERCOME IT?.....	22
6. CONCLUSION.....	22
7. REFERENCES.....	23



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 (webinjests), keylogging, 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.



NIIT UNIVERSITY, NEEMRANA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

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 Tesla 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.

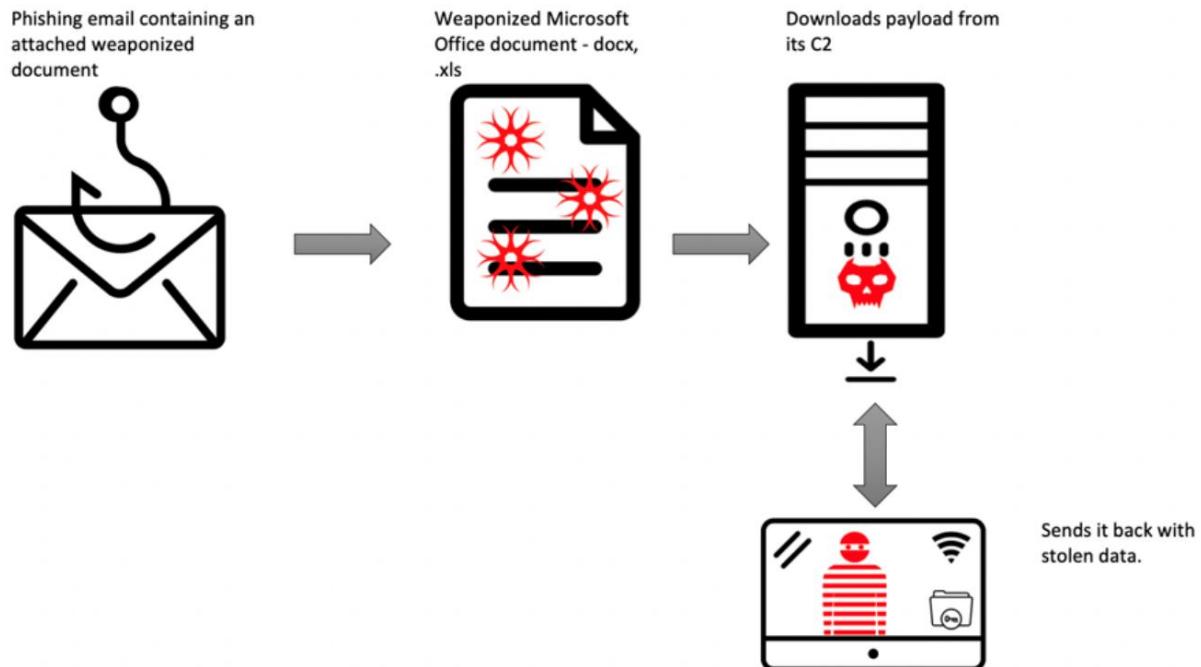


Fig 2: Basic Working of Agent Tesla

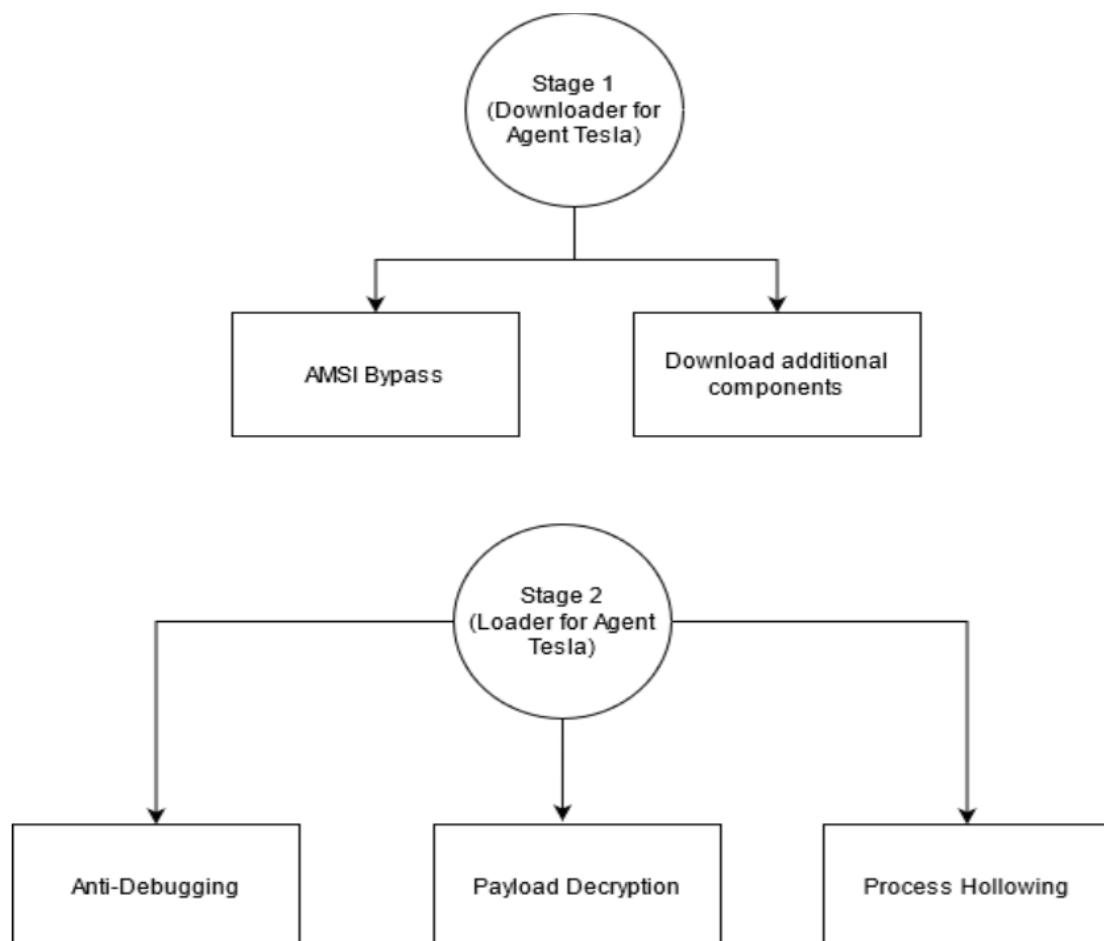


Fig 3: Stages of Agent Tesla Malware

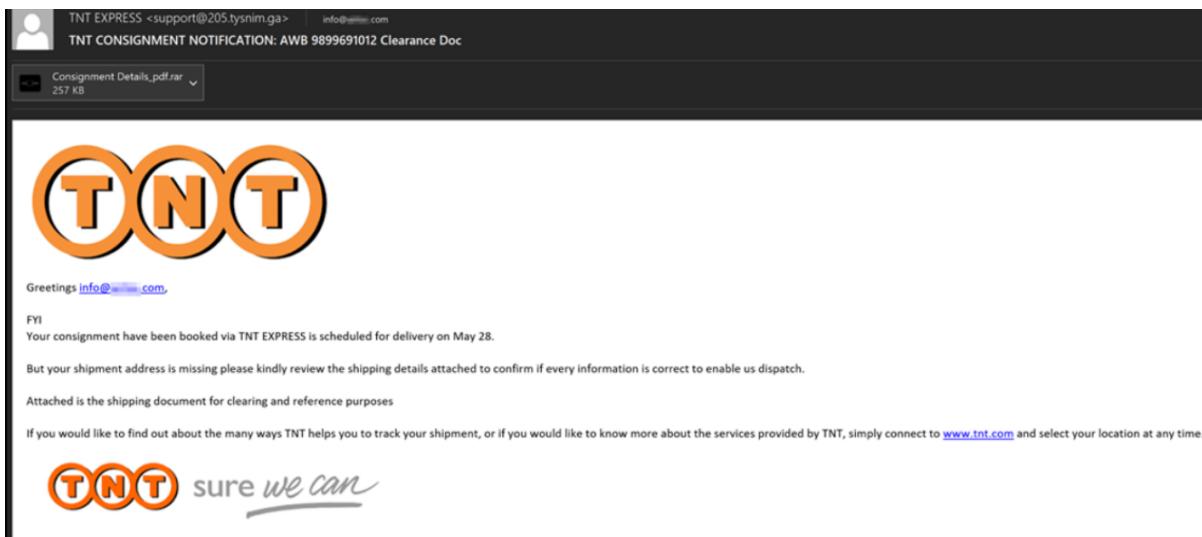


Fig 4: Agent Tesla Phishing email

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)

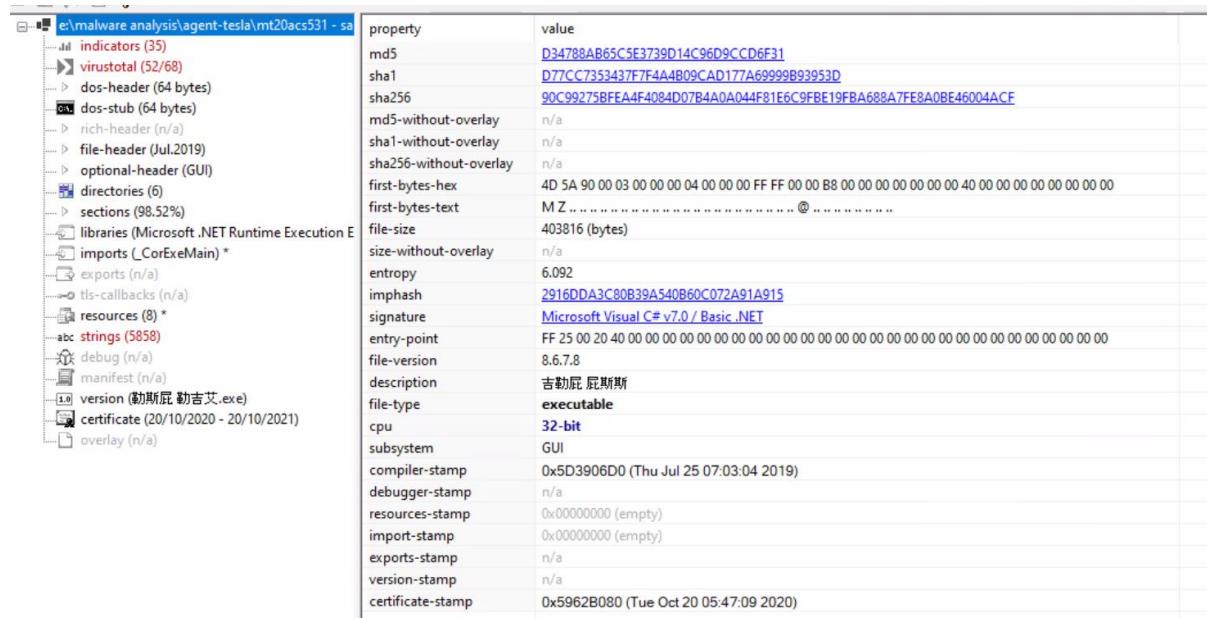
Process Dumper (pd64) – Dynamic Analysis (Dump from memory)

Task Scheduler – Dynamic Analysis

3. AGENT TESLA MALWARE ANALYSIS

We have downloaded the malware from the resources mentioned above.

STATIC ANALYSIS OF 1st Stage



property	value
md5	D34788AB65C5E3739D14C96D9CCD6F31
sha1	D77CC7353437F7F4A4B09CAD177A69999B93953D
sha256	90C99275BFEA4F4084D07B4A0A044F81E6C9FBE19FBA688A7FE8A0BE46004ACF
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 90 00 03 00 00 04 00 00 FF FF 00 00 B8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00
first-bytes-text	M Z ... @
file-size	403816 (bytes)
size-without-overlay	n/a
entropy	6.092
imphash	2916DDA3C80B39A540B60C072A91A915
signature	Microsoft Visual C# v7.0 / Basic .NET
entry-point	FF 25 00 20 40 00
file-version	8.6.7.8
description	吉勒屁 尿斯斯
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	0x5D3906D0 (Thu Jul 25 07:03:04 2019)
debugger-stamp	n/a
resources-stamp	0x00000000 (empty)
import-stamp	0x00000000 (empty)
exports-stamp	n/a
version-stamp	n/a
certificate-stamp	0x5962B080 (Tue Oct 20 05:47:09 2020)

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

encoding (2)	size (bytes)	file-offset	blacklist (2)	hint (36)	group (9)	value (5858)
ascii	25	0x00019686	-	-	-	df1fcffacacebfabfcfc
ascii	22	0x00019640	-	-	-	cddcbdafdacecbdddbffc
ascii	26	0x00019687	-	-	-	System.Collections.Generic
ascii	21	0x000196D2	-	-	-	Microsoft.VisualBasic
ascii	24	0x000196E8	-	-	-	aeeabdeefadneeddfccfcad
ascii	6	0x00019701	-	-	-	Thread
ascii	28	0x00019708	-	-	-	feedfaccfcfafahfbabafaefad
ascii	8	0x00019725	-	-	-	dfeefad
ascii	19	0x0001972E	-	-	-	ecccbcdaedaaeaeabbcd
ascii	9	0x00019742	-	-	-	ecfcfdhbcd
ascii	27	0x0001974C	-	-	-	ekfcebaebdffaabeaceaebadbd
ascii	24	0x00019768	-	-	-	cababebcccdbaaaeabbd
ascii	22	0x00019781	-	-	-	ccbafeccdcfiebaabed
ascii	14	0x00019798	-	-	-	cffebbbfeffacd
ascii	20	0x000197A7	-	-	-	addebbafabbdffbfcecd
ascii	29	0x000197C0	-	-	-	asabbeacadacddcccdhbbebdbbedd
ascii	22	0x000197D6	-	-	-	ababdadbsaafchbfefedd
ascii	27	0x000197F5	-	-	-	daadfbdaefcfddcfefbfed
ascii	9	0x00019811	-	-	-	Versioned
ascii	18	0x0001981B	-	-	-	dcgaaefaccffdbbfad
ascii	27	0x0001982E	-	-	-	dbcbefexaabbeacedbeacafcd
ascii	15	0x0001984A	-	-	-	abdcfffaaaafdf
ascii	14	0x0001985A	-	-	-	ckcdaefaffbd
ascii	22	0x00019869	-	-	-	daedadfbcdlfcfcfadcfdf
ascii	8	0x00019880	-	-	-	ahdcffdf
ascii	9	0x00019889	-	-	-	ReadToEnd
ascii	4	0x00019893	x	utility	-	Send
ascii	5	0x00019898	-	-	-	Round
ascii	10	0x0001989E	-	-	-	set Method
ascii	13	0x000198A9	-	-	-	CompareMethod
ascii	9	0x000198B7	-	-	-	GetMethod

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

encoding (2)	size (bytes)	file-offset	blacklist (2)	hint (36)	group (9)	value (5858)
ascii	4	0x0005E702	-	-	-	wwwwww
ascii	4	0x0005E712	-	-	-	wwwwww
ascii	4	0x0005E722	-	-	-	wwwwww
ascii	4	0x0005E732	-	-	-	wwwwww
ascii	4	0x0005E742	-	-	-	wwwwww
ascii	4	0x0005E752	-	-	-	wwwwww
ascii	4	0x0005E762	-	-	-	wwwwww
ascii	4	0x0005E772	-	-	-	wwwwww
ascii	4	0x0005E782	-	-	-	wwwwww
ascii	4	0x0005E792	-	-	-	wwwwww
ascii	4	0x0005E7A2	-	-	-	wwwwww
ascii	20	0x00061B85	-	-	-	www.digicert.com110/
ascii	20	0x00062C22	-	-	-	www.digicert.com110/
ascii	20	0x00062750	-	-	-	www.digicert.com110/
ascii	20	0x0006223B	-	-	-	www.digicert.com150/
unicode	14	0x0001BAD6	-	-	-	wsdlParameters
ascii	14	0x0005D9F3	-	-	-	wsdlParameters
ascii	8	0x000174F1	file	-	-	wsdlExe
unicode	8	0x0001A14CA	file	-	-	wsdlExe
unicode	8	0x00059E18	file	-	-	wsdlExe
ascii	8	0x0005D3B0	file	-	-	wsdlExe
ascii	4	0x0001779C	-	-	-	wsdl
ascii	6	0x0001831F	-	-	-	writer
unicode	19	0x0001BA26	-	-	-	webReferenceOptions
ascii	19	0x0005D866	-	-	-	webReferenceOptions
ascii	8	0x00016923	-	-	-	violated
unicode	7	0x0001A1A0	-	-	-	verbose
ascii	6	0x00018730	-	-	-	values
ascii	11	0x00018109	-	-	-	valueNumber
ascii	9	0x00016EB3	-	-	-	valueName
ascii	5	0x000174C5	-	-	-	value

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.

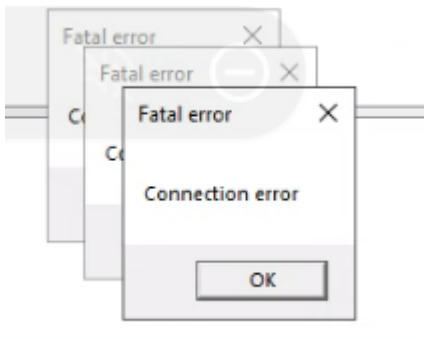


Fig 10: Fatal Error on executing the malware

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.

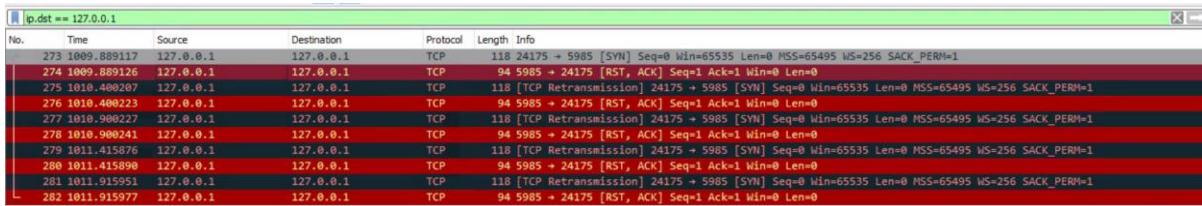


Fig 11: Wireshark: Malware trying to access hastebin and digicert at 127.0.0.1 as we have modified the host's file

No.	Time	Source	Destination	Protocol	Length	Info	sk	00	2,108 K	Enabled
273	1009.889117	127.0.0.1	127.0.0.1	TCP	118	24175 + 5985 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1				
274	1009.889126	127.0.0.1	127.0.0.1	TCP	94	5985 + 24175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0				
275	1018.400287	127.0.0.1	127.0.0.1	TCP	118	[TCP Retransmission] 24175 + 5985 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1				
276	1018.400223	127.0.0.1	127.0.0.1	TCP	94	5985 + 24175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0				
277	1018.900227	127.0.0.1	127.0.0.1	TCP	118	[TCP Retransmission] 24175 + 5985 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1				
278	1018.900241	127.0.0.1	127.0.0.1	TCP	94	5985 + 24175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0				
279	1011.415876	127.0.0.1	127.0.0.1	TCP	118	[TCP Retransmission] 24175 + 5985 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1				
280	1011.415894	127.0.0.1	127.0.0.1	TCP	94	5985 + 24175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0				
281	1011.915951	127.0.0.1	127.0.0.1	TCP	118	[TCP Retransmission] 24175 + 5985 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1				
282	1011.915977	127.0.0.1	127.0.0.1	TCP	94	5985 + 24175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0				

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

Time of Day	Process Name	PID	Operation	Path	Result	Detail
21:00:45.451755	90c99275bfe4f4084d07b4a0e04	1352	RegCloseKey	HKEY_LOCAL_MACHINE\Software\Microsoft\Wow64v86	SUCCESS	
21:00:45.451569	90c99275bfe4f4084d07b4a0e04	1352	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x771...
21:00:45.451893	90c99275bfe4f4084d07b4a0e04	1352	RegOpenKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
21:00:45.451908	90c99275bfe4f4084d07b4a0e04	1352	RegOpenKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
21:00:45.451924	90c99275bfe4f4084d07b4a0e04	1352	RegSetInfoKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformation...
21:00:45.451931	90c99275bfe4f4084d07b4a0e04	1352	RegQueryValue	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadl...	NAME NOT FOUND	Length: 80
21:00:45.451955	90c99275bfe4f4084d07b4a0e04	1352	RegOpenKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Session Manager	SUCCESS	
21:00:45.451974	90c99275bfe4f4084d07b4a0e04	1352	RegOpenKey	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Segment\Heap	REPARSE	Desired Access: Q...
21:00:45.451977	90c99275bfe4f4084d07b4a0e04	1352	RegOpenKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Session Manager\Segment\Heap	NAME NOT FOUND	Desired Access: Q...
21:00:45.452042	90c99275bfe4f4084d07b4a0e04	1352	RegOpenKey	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
21:00:45.452054	90c99275bfe4f4084d07b4a0e04	1352	RegOpenKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
21:00:45.452059	90c99275bfe4f4084d07b4a0e04	1352	RegSetInfoKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformation...
21:00:45.452081	90c99275bfe4f4084d07b4a0e04	1352	RegQueryValue	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
21:00:45.452097	90c99275bfe4f4084d07b4a0e04	1352	RegCloseKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Session Manager	SUCCESS	
21:00:45.4524219	90c99275bfe4f4084d07b4a0e04	1352	CreateFile	E:\malware\analysis\agent\code\MT20AC5531 - Sarath Kumar MC - Lab3\Dynamic Samples\cmd.exe	Desired Access: E...	
21:00:45.4526191	90c99275bfe4f4084d07b4a0e04	1352	CreateFile	C:\Windows\SysWOW64\mscoree.dll	SUCCESS	Desired Access: R...
21:00:45.4526605	90c99275bfe4f4084d07b4a0e04	1352	QueryBasicInformationFile	C:\Windows\SysWOW64\mscoree.dll	SUCCESS	Creation Time: 07/1...
21:00:45.4526725	90c99275bfe4f4084d07b4a0e04	1352	CloseFile	C:\Windows\SysWOW64\mscoree.dll	SUCCESS	
21:00:45.4527795	90c99275bfe4f4084d07b4a0e04	1352	CreateFile	C:\Windows\SysWOW64\mscoree.dll	SUCCESS	Desired Access: R...
21:00:45.4528712	90c99275bfe4f4084d07b4a0e04	1352	CreateFileMapping	C:\Windows\SysWOW64\mscoree.dll	FILE LOCKED WI...	SyncType: SyncTy...
21:00:45.452913	90c99275bfe4f4084d07b4a0e04	1352	RegOpenKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Cl	REPARSE	Desired Access: R...
21:00:45.452929	90c99275bfe4f4084d07b4a0e04	1352	RegOpenKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Cl	SUCCESS	Desired Access: R...
21:00:45.4529457	90c99275bfe4f4084d07b4a0e04	1352	RegQueryValue	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Cl\Disable26178932	NAME NOT FOUND	Length: 20
21:00:45.4529625	90c99275bfe4f4084d07b4a0e04	1352	RegCloseKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Cl	SUCCESS	
21:00:45.4529770	90c99275bfe4f4084d07b4a0e04	1352	RegOpenKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Cl	REPARSE	Desired Access: Q...
21:00:45.4529916	90c99275bfe4f4084d07b4a0e04	1352	RegOpenKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Cl	SUCCESS	Desired Access: Q...
21:00:45.4530056	90c99275bfe4f4084d07b4a0e04	1352	RegQueryValue	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Cl\Disable26178932	NAME NOT FOUND	Length: 80
21:00:45.453020	90c99275bfe4f4084d07b4a0e04	1352	RegCloseKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Cl	SUCCESS	
21:00:45.453039	90c99275bfe4f4084d07b4a0e04	1352	CreateFileMapping	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Cl	SUCCESS	SyncType: SyncTy...
21:00:45.453125	90c99275bfe4f4084d07b4a0e04	1352	Load Image	C:\Windows\SysWOW64\mscoree.dll	SUCCESS	Image Base: 0x73c...
21:00:45.4532579	90c99275bfe4f4084d07b4a0e04	1352	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x763...
21:00:45.4534407	90c99275bfe4f4084d07b4a0e04	1352	Load Image	C:\Windows\SysWOW64\kernelbase.dll	SUCCESS	Image Base: 0x764...
21:00:45.4536739	90c99275bfe4f4084d07b4a0e04	1352	CloseFile	C:\Windows\SysWOW64\mscoree.dll	SUCCESS	
21:00:45.4541652	90c99275bfe4f4084d07b4a0e04	1352	RegQueryValue	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\WMI\Security\3c74af9-8d244e3b52c-365dbf4...	NAME NOT FOUND	Length: 528
21:00:45.4542746	90c99275bfe4f4084d07b4a0e04	1352	RegQueryValue	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\WMI\Security\0f95feef-7f49c7a-994-50a55c0...	NAME NOT FOUND	Length: 528
21:00:45.4545149	90c99275bfe4f4084d07b4a0e04	1352	RegOpenKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Nls\Sorting\Versions	REPARSE	Desired Access: R...
21:00:45.4545444	90c99275bfe4f4084d07b4a0e04	1352	RegOpenKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	Desired Access: R...
21:00:45.4545623	90c99275bfe4f4084d07b4a0e04	1352	RegSetInfoKey	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	KeySetInformation...
21:00:45.4545761	90c99275bfe4f4084d07b4a0e04	1352	RegQueryValue	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Nls\Sorting\Versions\{Default}	SUCCESS	Type: REG_SZ, Le...

STATIC ANALYSIS OF Intermediate Downloader

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

property	value
md5	FEC8AF4DBB834256EBAF7FBC4D722915
sha1	5AB77164719CC6F7A885F11CA1CE233ACE5757E
sha256	5ACE35AFBF13D16D5B21AE38BEFDE4A0418C4FFFA8E3C09F06888EB5AA83C063
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 90 00 03 00 00 04 00 00 FF FF 00 B8 00 00 00 00 00 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z
file-size	230072 (bytes)
size-without-overlay	n/a
entropy	6.125
imphash	2916DDA3C80B39A540B60C072A91A915
signature	Microsoft Visual C# v7.0 / Basic .NET
entry-point	FF 25 00 20 40 00
file-version	20.9.20065.55827
description	Adobe Acrobat Reader DC
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	0x4CD538E6 (Wed May 28 17:24:14 2007)
debugger-stamp	n/a
resources-stamp	0x00000000 (empty)
import-stamp	0x00000000 (empty)
exports-stamp	n/a
version-stamp	n/a
certificate-stamp	0xC031A400 (Wed Oct 07 07:09:52 2020)

Fig 17: PEStudio: Intermediate Downloader

encoding (2)	size (bytes)	file-offset	blacklist (0)	hint (19)	group (3)	value (999)
ascii	7	0x0000395F	-	utility	-	Program
ascii	7	0x000043AD	-	utility	-	Replace
ascii	6	0x00004419	-	utility	-	Create
ascii	5	0x000044CB	-	utility	-	Shell
ascii	7	0x00004615	-	utility	-	Process
ascii	8	0x00009C46	-	url-pattern	-	16.0.0
ascii	7	0x00009D2D	-	url-pattern	-	4.0.0
ascii	5	0x00003E2B	-	keyboard	-	Enter
ascii	11	0x00009F32	-	import	-	CorExeMain
ascii	8	0x000084D4	-	format-string	-	X2u"%"
ascii	23	0x000036D0	-	file	-	VSTestVideoRecorder.exe
ascii	59	0x0000390C	-	file	-	Microsoft.VisualStudio.QualityTools.VideoRecorderEngine.dll
ascii	4	0x00004457	-	file	-	.exe
ascii	10	0x0000463A	-	file	-	System.Net
ascii	11	0x00009F3E	-	file	-	mscoree.dll
ascii	4	0x0000376A	-	file	-	B_z
unicode	17	0x000048FE	-	file	-	ScreenCapture.wmv
unicode	27	0x00003684C	-	file	-	Adobe Acrobat Reader DC.exe
ascii	40	0x0000004D	-	dos-message	-	This program cannot be run in DOS mode.
ascii	16	0x0000446B	-	-	obfuscation	FromBase64String
ascii	11	0x000043FB	-	-	-	WebResponse
ascii	11	0x00004407	-	-	-	GetResponse
ascii	10	0x00004653	-	-	-	WebRequest
ascii	14	0x00002F88	-	-	execution	GetProcessByld
ascii	6	0x000031E6	-	-	execution	Invoke
ascii	15	0x000032CF	-	-	execution	get_ProcName
ascii	8	0x000037D5	-	-	execution	callback
ascii	17	0x00003979	-	-	execution	QueueUserWorkItem
ascii	5	0x0000386C	-	-	execution	Sleep
ascii	17	0x00004157	-	-	execution	GetCurrentProcess
ascii	5	0x00000178	-	-	-	text

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

DYNAMIC ANALYSIS OF Intermediate Downloader

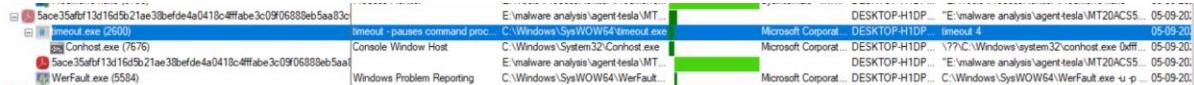


Fig 21: Process Monitor: Timeout.exe for timeout used for pausing command processing

18 36..648780	127.0.0.1	127.0.0.1	TCP	118 [24179 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1	DESKTOP-H1DP... "E:\malware analysis\agent\testa\MT20AC55.. 05-09-20:
19 36..648748	127.0.0.1	127.0.0.1	TCP	118 443 → 24179 [SYN, ACK] Seq=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1	Microsoft Corporat... DESKTOP-H1DP... timeout 4 05-09-20
20 36..650163	127.0.0.1	127.0.0.1	TCP	94 24179 → 443 [ACK] Seq=1 Ack=1 Win=2619648 Len=0	Microsoft Corporat... DESKTOP-H1DP... \??C:\Windows\system32\conhost.exe 0fff.. 05-09-20:
21 36..673423	127.0.0.1	127.0.0.1	TLSv1.2	442 Client Hello	Microsoft Corporat... DESKTOP-H1DP... \??C:\Windows\system32\conhost.exe 0fff.. 05-09-20:
22 36..673473	127.0.0.1	127.0.0.1	TCP	94 443 → 24179 [ACK] Seq=1 Ack=175 Win=327168 Len=0	E:\malware analysis\agent\testa\MT20AC55.. 05-09-20:
23 36..696866	127.0.0.1	127.0.0.1	TLSv1.2	1474 Server Hello, Certificate, Server Key Exchange, Server Hello Done	C:\Windows\SysWOW64\WerFault.exe p.. 05-09-20:
24 36..696876	127.0.0.1	127.0.0.1	TCP	94 24179 → 443 [ACK] Seq=175 Ack=691 Win=2618880 Len=0	Microsoft Corporat... DESKTOP-H1DP... E:\malware analysis\agent\testa\MT20AC55.. 05-09-20:
25 36..706346	127.0.0.1	127.0.0.1	TLSv1.2	288 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	Microsoft Corporat... DESKTOP-H1DP... E:\malware analysis\agent\testa\MT20AC55.. 05-09-20:
26 36..706387	127.0.0.1	127.0.0.1	TCP	94 443 → 24179 [ACK] Seq=691 Ack=268 Win=327168 Len=0	Microsoft Corporat... DESKTOP-H1DP... E:\malware analysis\agent\testa\MT20AC55.. 05-09-20:
27 36..708361	127.0.0.1	127.0.0.1	TLSv1.2	618 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message	Microsoft Corporat... DESKTOP-H1DP... E:\malware analysis\agent\testa\MT20AC55.. 05-09-20:
28 36..708403	127.0.0.1	127.0.0.1	TCP	94 24179 → 443 [ACK] Seq=268 Ack=949 Win=2618624 Len=0	Microsoft Corporat... DESKTOP-H1DP... E:\malware analysis\agent\testa\MT20AC55.. 05-09-20:
29 36..837422	127.0.0.1	127.0.0.1	TCP	94 24179 → 443 [FIN, ACK] Seq=268 Ack=949 Win=2618624 Len=0	Microsoft Corporat... DESKTOP-H1DP... E:\malware analysis\agent\testa\MT20AC55.. 05-09-20:
30 36..837470	127.0.0.1	127.0.0.1	TCP	94 443 → 24179 [ACK] Seq=949 Ack=269 Win=327168 Len=0	Microsoft Corporat... DESKTOP-H1DP... E:\malware analysis\agent\testa\MT20AC55.. 05-09-20:
31 36..838215	127.0.0.1	127.0.0.1	TLSv1.2	156 Encrypted Alert	Microsoft Corporat... DESKTOP-H1DP... E:\malware analysis\agent\testa\MT20AC55.. 05-09-20:

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

TIME / DAY	PROCESS NAME	FID	OPERATOR	DATA	RESULT	DETAIL
23:21:47.4014107	5ace35afb13d16d5b21ae38bfe...	4444	? RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformation...
23:21:47.4014254	5ace35afb13d16d5b21ae38bfe...	4444	? RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadl...	NAME NOT FOUND Length: 80	
23:21:47.4014533	5ace35afb13d16d5b21ae38bfe...	4444	? RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
23:21:47.4014735	5ace35afb13d16d5b21ae38bfe...	4444	? RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Q...
23:21:47.4014877	5ace35afb13d16d5b21ae38bfe...	4444	? RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND Desired Access: Q...	
23:21:47.4015673	5ace35afb13d16d5b21ae38bfe...	4444	? RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
23:21:47.4015817	5ace35afb13d16d5b21ae38bfe...	4444	? RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
23:21:47.4015976	5ace35afb13d16d5b21ae38bfe...	4444	? RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformation...
23:21:47.4016099	5ace35afb13d16d5b21ae38bfe...	4444	? RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND Length: 24	
23:21:47.4016264	5ace35afb13d16d5b21ae38bfe...	4444	? RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
23:21:47.4025521	5ace35afb13d16d5b21ae38bfe...	4444	? CreateFile	E:\malware analysis\agent\testa\MT20AC5531 - Sarathkumar MC - Lab 3\DynamicSamples	SUCCESS	Desired Access: E...
23:21:47.4027521	5ace35afb13d16d5b21ae38bfe...	4444	? CreateFile	C:\Windows\SysWOW64\mscorre.dll	SUCCESS	Desired Access: R...
23:21:47.4028878	5ace35afb13d16d5b21ae38bfe...	4444	? QueryBasicInformation	C:\Windows\SysWOW64\mscorre.dll	SUCCESS	CreationTime: 07-1...
23:21:47.4029011	5ace35afb13d16d5b21ae38bfe...	4444	? CloseFile	C:\Windows\SysWOW64\mscorre.dll	SUCCESS	
23:21:47.4030012	5ace35afb13d16d5b21ae38bfe...	4444	? CreateFile	C:\Windows\SysWOW64\mscorre.dll	SUCCESS	Desired Access: R...
23:21:47.4030534	5ace35afb13d16d5b21ae38bfe...	4444	? CreateFileMapping	C:\Windows\SysWOW64\mscorre.dll	FILE LOCKED WI...	SyncType: SyncTy...
23:21:47.4030824	5ace35afb13d16d5b21ae38bfe...	4444	? RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	REPARSE	Desired Access: R...
23:21:47.4030991	5ace35afb13d16d5b21ae38bfe...	4444	? RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	Desired Access: R...
23:21:47.4031163	5ace35afb13d16d5b21ae38bfe...	4444	? RegQueryValue	HKLM\System\CurrentControlSet\Control\CI\Disable26178932	NAME NOT FOUND Length: 20	
23:21:47.403129	5ace35afb13d16d5b21ae38bfe...	4444	? RegCloseKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	
23:21:47.4031496	5ace35afb13d16d5b21ae38bfe...	4444	? RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	REPARSE	Desired Access: Q...
23:21:47.4031693	5ace35afb13d16d5b21ae38bfe...	4444	? RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	Desired Access: Q...
23:21:47.4031855	5ace35afb13d16d5b21ae38bfe...	4444	? RegQueryValue	HKLM\System\CurrentControlSet\Control\CI\Disable26178932	NAME NOT FOUND Length: 80	
23:21:47.4032010	5ace35afb13d16d5b21ae38bfe...	4444	? RegCloseKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	
23:21:47.4032153	5ace35afb13d16d5b21ae38bfe...	4444	? CreateFileMapping	C:\Windows\SysWOW64\mscorre.dll	SUCCESS	SyncType: SyncTy...
23:21:47.4033122	5ace35afb13d16d5b21ae38bfe...	4444	? LoadImage	C:\Windows\SysWOW64\mscorre.dll	SUCCESS	Image Base: 0x73...
23:21:47.4033788	5ace35afb13d16d5b21ae38bfe...	4444	? ReadFile	C:\Windows\SysWOW64\mscorre.dll	SUCCESS	Offset: 292864, Le...
23:21:47.4042430	5ace35afb13d16d5b21ae38bfe...	4444	? LoadImage	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x763...
23:21:47.4044562	5ace35afb13d16d5b21ae38bfe...	4444	? LoadImage	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x764...
23:21:47.4047008	5ace35afb13d16d5b21ae38bfe...	4444	? CloseFile	C:\Windows\SysWOW64\mscorre.dll	SUCCESS	
23:21:47.4052319	5ace35afb13d16d5b21ae38bfe...	4444	? RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\3c74af9-8d82-44e3-b52c-365dbf40...	NAME NOT FOUND Length: 528	
23:21:47.4053287	5ace35afb13d16d5b21ae38bfe...	4444	? RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\0f95fe-7f75-49c7-a994-60a5cc0...	NAME NOT FOUND Length: 528	
23:21:47.4054267	5ace35afb13d16d5b21ae38bfe...	4444	? ReadFile	C:\Windows\SysWOW64\mscorre.dll	SUCCESS	Offset: 291238, Le...
23:21:47.4057807	5ace35afb13d16d5b21ae38bfe...	4444	? RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	REPARSE	Desired Access: R...
23:21:47.4058166	5ace35afb13d16d5b21ae38bfe...	4444	? RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	Desired Access: R...
23:21:47.4058402	5ace35afb13d16d5b21ae38bfe...	4444	? RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	KeySetInformation...
23:21:47.4058544	5ace35afb13d16d5b21ae38bfe...	4444	? RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\Default	SUCCESS	Type: REG_SZ, Le...
23:21:47.4058883	5ace35afb13d16d5b21ae38bfe...	4444	? RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\0006030x	SUCCESS	Type: REG_SZ, Le...
23:21:47.4062310	5ace35afb13d16d5b21ae38bfe...	4444	? RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Q...
23:21:47.4062442	5ace35afb13d16d5b21ae38bfe...	4444	? ReadFile	C:\Windows\SysWOW64\mscorre.dll	SUCCESS	Name: KMMF_EPMKIMI_Pending_Access /

Fig 23: Process Monitor: It is trying to access mscorre.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

c:\malware analysis\agent-tesla\mt20acs531 - sa		property	value
indicators (wait...)		md5	9f02e3c48740132dcbbc1efac0130651
virustotal (52/69)		sha1	99845781cfaa31b38873ec716603578f13ec1049
dos-header (64 bytes)		sha256	5f1b120f79f227f26c489f998c4d3f3c73e7bf1eb885b2405c962d0ef915dd77
dos-stub (wait...)		md5-without-overlay	wait...
rich-header (n/a)		sha1-without-overlay	wait...
optional-header (GUI)		sha256-without-overlay	wait...
file-header (Jan.2021)		first-bytes-hex	4D 5A 90 00 03 00 00 04 00 00 FF FF 00 00 B8 00 00 00 00 00 40 00 00 00 00 00 00 00
directories (5)		first-bytes-text	M Z@.....
sections (wait...)		file-size	1027584 (bytes)
libraries (wait...)		size-without-overlay	wait...
imports (wait...)		entropy	7.451
exports (n/a)		imphash	2916DDA3C80B39A540B60C072A91A915
tls-callbacks (n/a)		signature	n/a
resources (12) *		entry-point	FF 25 00 20 40 00 20 00 2D 00 3A 00 2C 00 21 00 00 00 63 6F 6E 74 65 6E 74 73 2D 74 61 62 6C 65
abc strings (wait...)		file-version	1.0.0.1
debug (n/a)		description	BackUp
manifest (asInvoker)		file-type	executable
version (Disposition.exe)		cpu	32-bit
certificate (wait...)		subsystem	GUI

Fig 24: PEStudio: 2nd Stage Malware

e:\malware analysis\agent-tesla\mt20acs531 - sa		encoding (2)	size (bytes)	file-offset	blacklist (3)	hint (36)	group (3)	value (8296)
indicators (32)		ascii	6	0x0001CD26	-	utility	-	Expand
virustotal (offline)		ascii	7	0x0001CE18	-	utility	-	Replace
dos-header (64 bytes)		ascii	6	0x0001D471	-	utility	-	Update
dos-stub (64 bytes)		ascii	5	0x0001D4B4	-	utility	-	Write
rich-header (n/a)		ascii	4	0x0001E33	-	utility	-	Open
file-header (Jan.2021)		ascii	7	0x000201E0	-	utility	-	Select
optional-header (GUI)		ascii	6	0x000203E0	-	utility	-	Process
directories (5)		ascii	8	0x000252FA	-	utility	-	Select
sections (99.95%)		ascii	5	0x00070BCC	-	utility	-	Shutdown
libraries (Microsoft .NET Runtime Execution E		unicode	8	0x00022E92	-	utility	-	hH N:
imports (.CorExeMain)*		unicode	8	0x00025AA2	-	url-pattern	-	Shutdown
exports (n/a)		ascii	8	0x000254E4	-	url-pattern	-	11.0.0.0
tls-callbacks (n/a)		ascii	8	0x0002553E	-	url-pattern	-	16.0.0
resources (12) *		unicode	36	0x00021486	-	url-pattern	-	16.7.0
abc strings (8296)		unicode	44	0x00021640	-	uri-pattern	-	https://www.tapatalk.com/groups/vvmm
debug (n/a)		ascii	64	0x0001C484	-	size	-	https://github.com/SilverGreer93/CDPExplorer
manifest (asInvoker)		ascii	64	0x0001C526	-	size	-	E741FE2017B6EE88C04053668448FBAC997B5939195FDA2B1B669FF6A
version (Disposition.exe)		unicode	16	0x00023122	-	query	-	41A91C2890E6FE5E92E9C59976CE866C7BCE98E516E05AD328C81A146
certificate (n/a)		ascii	8	0x000C67C9	-	password	-	Select the entry
overlay (n/a)		ascii	11	0x000C6722	-	import	-	CorExeMain
		ascii	5	0x0006C3B5	-	format-string	-	%S
		ascii	4	0x000967F7	-	format-string	-	%Sb
		ascii	5	0x000B11F4	-	format-string	-	%VS3
		ascii	15	0x0001D867	-	file	-	Disposition.exe
		ascii	14	0x00025621	-	file	-	My.Application
		ascii	4	0x0002020C0C	-	file	-	9.go
		ascii	4	0x0002E30E	-	file	-	kljh
		ascii	5	0x0008E2E8	-	file	-	n.Cgl
		ascii	5	0x0008F62F	-	file	-	lv.en
		ascii	4	0x000863F	-	file	-	Wu.Z
		ascii	11	0x000C672E	-	file	-	mscoreee.dll

Activate Windows

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

		encoding (2)	size (bytes)	file-offset	blacklist (3)	hint (36)	group (3)	value (8296)
indicators (32)		7	0x000480DF	-	-	-	-	-taAAAt-
virustotal (offline)		7	0x0004811F	-	-	-	-	-taAAAt-
dos-header (64 bytes)		7	0x0004818	-	-	-	-	-taAAAt-
dos-stub (64 bytes)		6	0x0004819F	-	-	-	-	-taAAAR
rich-header (n/a)		6	0x000481DF	-	-	-	-	-taAAAd
file-header (Jan.2021)		6	0x0004821F	-	-	-	-	-taAAAR
optional-header (GUI)		9	0x0004825F	-	-	-	-	-taAAAt--
directories (5)		8	0x0004829D	-	-	-	-	-taAAAR
sections (99.95%)		8	0x000482DD	-	-	-	-	-taAAAd
libraries (Microsoft .NET Runtime Execution E		62	0x000482E7	-	-	-	-	utTsAd
imports (.CorExeMain)*		62	0x000482E7	-	-	-	-	wMoo
exports (n/a)		7	0x0004835E	-	-	-	-	
tls-callbacks (n/a)		36	0x000483BC	-	-	-	-	MAAAAAAAAAAAAAAAAAAAAAAAA
resources (12) *		11	0x000483EF	-	-	-	-	spididasSdRtttttttMUssssssssssssssssssssssss
abc strings (8296)		35	0x000483FC	-	-	-	-	sAAAAAA.....AAAAA.....AAAAA.....AAAAA.....
debug (n/a)		57	0x00048425	-	-	-	-	"G44446j44446F3
manifest (asInvoker)		23	0x00048466	-	-	-	-	97@DARE@??TB-7
version (Disposition.exe)		16	0x00049373	-	-	-	-	cgukslwrsusf5
certificate (n/a)		15	0x00049384	-	-	-	-	Ct((Z^Cnd_e
overlay (n/a)		15	0x00049394	-	-	-	-	0LM
		15	0x000493A4	-	-	-	-	81M
		4	0x000493BF	-	-	-	-	"cb(20)/KIM
		4	0x000493CF	-	-	-	-	(emvUP
		13	0x00049406	-	-	-	-	
		7	0x0004941A	-	-	-	-	

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 (3296)
ascii	6	0x0001CD26	-	utility	-	<u>Expand</u>
ascii	7	0x0001CE18	-	utility	-	<u>Replace</u>
ascii	6	0x0001D471	-	utility	-	<u>Update</u>
ascii	5	0x0001D4B4	-	utility	-	<u>Write</u>
ascii	4	0x0001E33	-	utility	-	<u>Open</u>
ascii	7	0x000201E0	-	utility	-	<u>Process</u>
ascii	6	0x000203E0	-	utility	-	<u>Select</u>
ascii	8	0x000252FA	-	utility	-	<u>Shutdown</u>
ascii	5	0x00070BC	-	utility	-	<u>hHN:</u>
unicode	8	0x00022EF2	-	utility	-	<u>Shutdown</u>
ascii	8	0x000254A2	-	url-pattern	-	<u>11.0.0.0</u>
ascii	8	0x000254E4	-	url-pattern	-	<u>16.0.0.0</u>
ascii	8	0x0002553E	-	url-pattern	-	<u>16.7.0.0</u>

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)

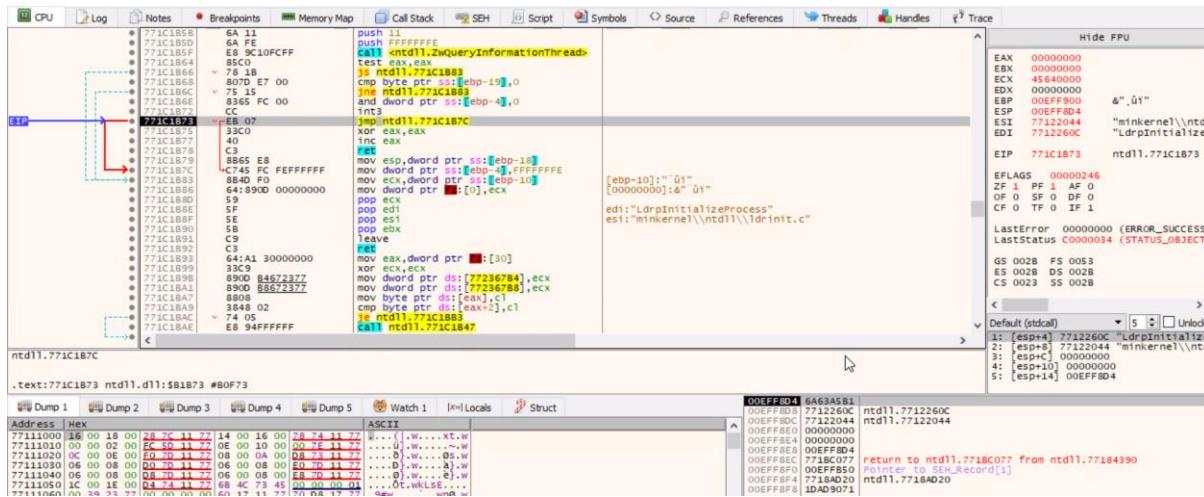


Fig 29: x32DDBG: 2nd Stage Malware (To extract the malware from memory)

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)

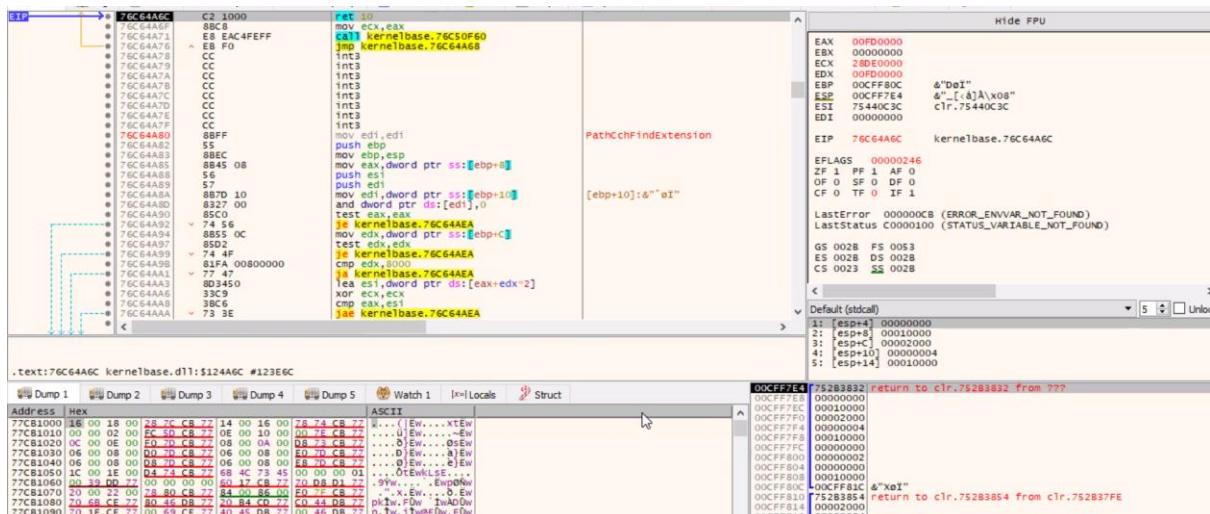


Fig 30: x32DDBG: 2nd Stage Malware (To extract the malware from memory) – Identified the entry point and provided the breakpoint where it is required.

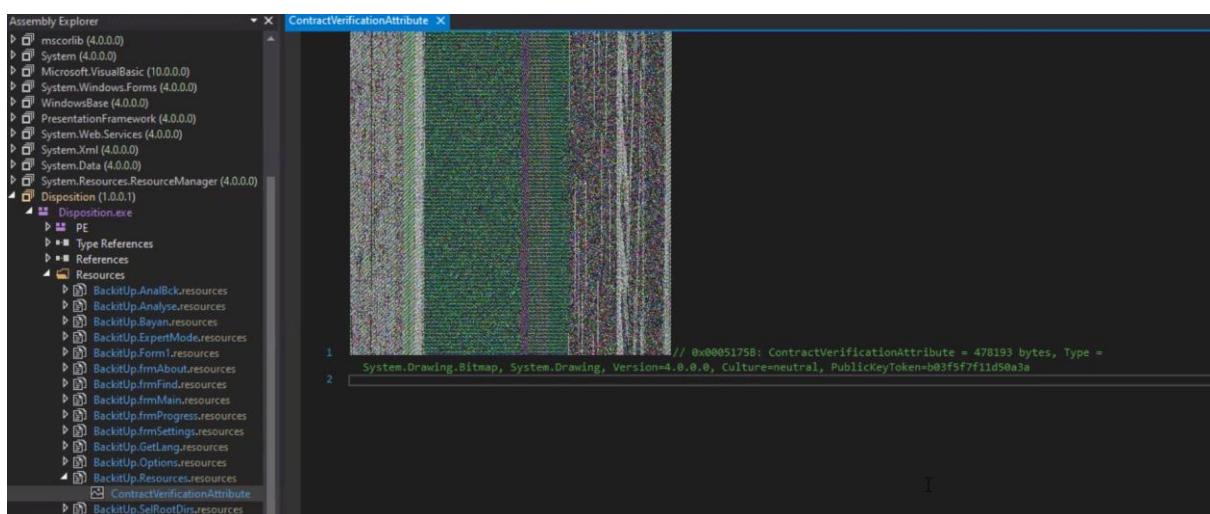


Fig 31: DNSpy: 2nd Stage Malware (Image Obfuscation is done)

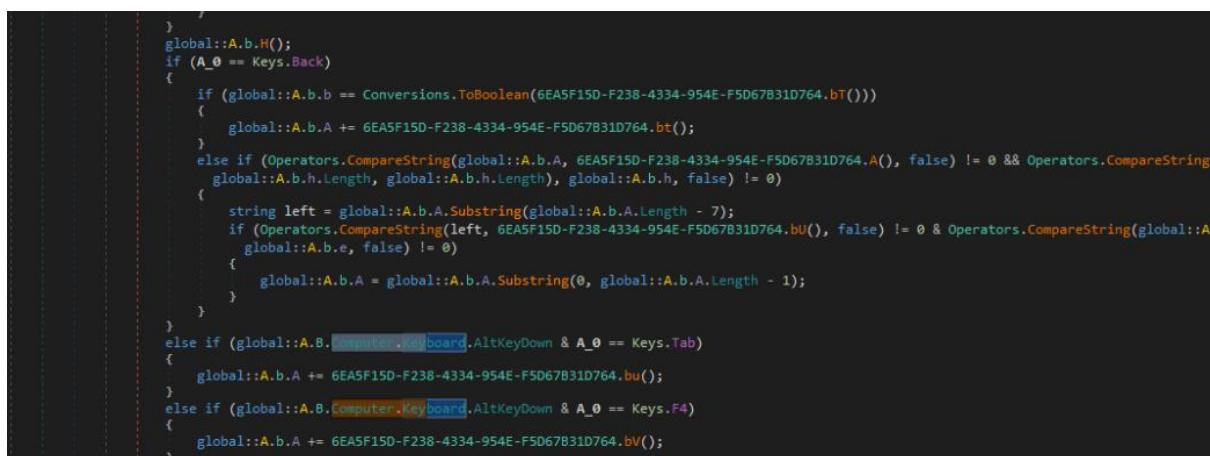


Fig 32: DNSpy: 2nd Stage Malware (Keylogger)

```

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
Procmn64.exe		4,756 K	14,880 K	7308 Process Monitor
cmd.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
v16Widget.exe	< 0.01	23,588 K	36,284 K	408 v16Widget
				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
Procmn64.exe		4,756 K	14,880 K	7308 Process Monitor
Procmn64.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
v16Widget.exe	0.77	23,588 K	36,796 K	408 v16Widget
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 RegSvcs. 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.

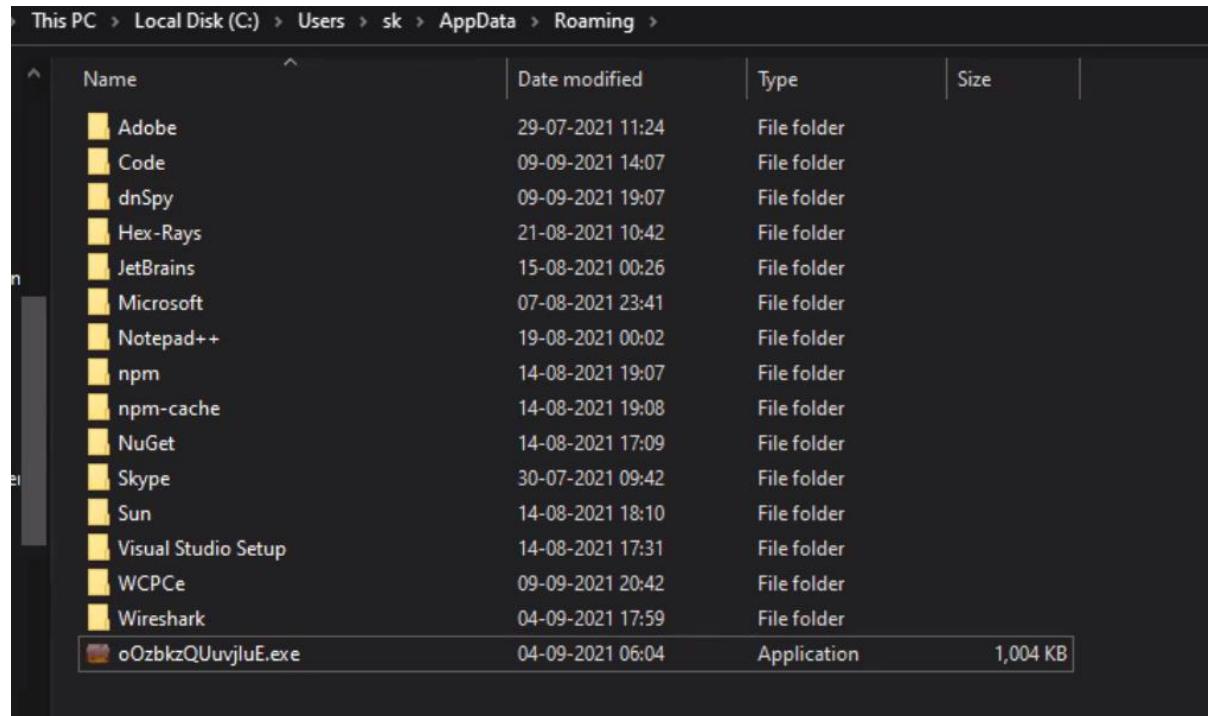


Fig 39: Malware creates an exe file in AppData folder

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.

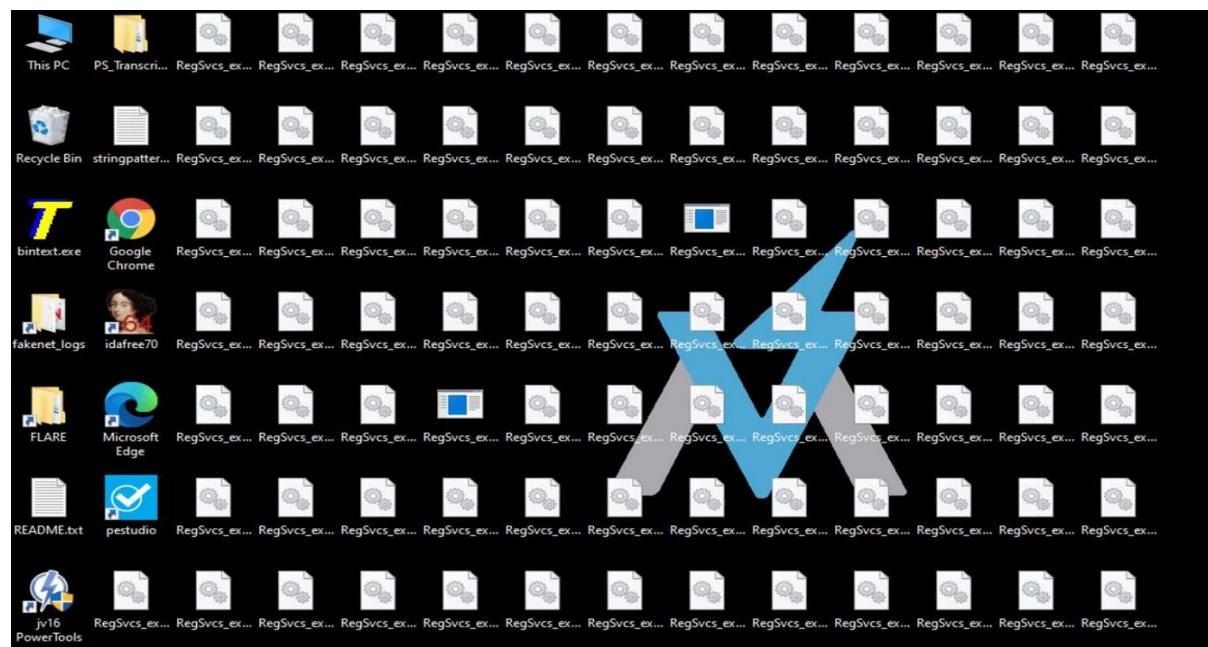


Fig 40: Malware activities after some time of execution where it copies the RegSvcs.exe multiple times

RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\CentBrowser\User Data
RegSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\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
DnsSvcs.exe	2540	CreateFile	C:\Users\Analyst\AppData\Local\Cloudflare\Cloudflare 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\Roamind\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 .\sample
\$\
AgentTeslaStaticDynamicRule .\samples\\5ace35afb13d16d5b21ae38befde4a0418c4ffffabe3c09f06888eb5aa83c063.exe
AgentTeslaStaticDynamicRule .\samples\\90c99275bfea4f40840d7b4a0a044f81e6c9fbe19fba688a7fe8a0be46004acf.exe
AgentTeslaStaticDynamicRule .\samples\\5f1b12bf79f227f26c489ff998c4d3f3c73e7bf1eb885b2405c962d0ef915dd77.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.



NIIT UNIVERSITY, NEEMRANA
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

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://georgemakakisblog.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>