MALICIOUS

Classifications: Spyware | Downloader

Threat Names: Mal/Generic-S | Mal/HTMLGen-A | Trojan.GenericKD.37670813 | Generic.Andromeda.4AA3DFD8 | Gen:Trojan.Heur.FU.gnZ@a0SiSGi

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe**
ID	#2782311
MD5	0bc97a36dc6135fc7a69c90c1c303439
SHA1	a3508e80c4e9bd20c04114c599be634107a49952
SHA256	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df
File Size	585.00 KB
Report Created	2021-09-28 10:42 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (15 rules, 54 matches)

Score	Category	Operation	Count	Classification
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Internet Explorer, CocCoc, CentBrowser, Mozilla Thunderbird, Comodo Dragon, Internet Explorer / E... ..., 7Star, Opera, Elements Browser, Uran, Epic Privacy Browser, Chedot, Torch, Vivaldi, Chromium, Kometa, Cyberfox, Total Commander.			
4/5	Antivirus	Malicious content was detected by heuristic scan	3	-
	• Built-in AV detected the sample itself as "Trojan.GenericKD.37670813". • Built-in AV detected a memory dump of (process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe as "Generic.Andromeda.4AA3DFD8". • Built-in AV detected a memory dump of (process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe as "Gen:Trojan.Heur.FU.gnZ@a0SiSGi".			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
4/5	Reputation	Contacts known malicious URL	7	-
	• Reputation analysis labels the URL "23.88.105.196/1008" which was contacted by (process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "23.88.105.196/freebl3.dll" which was contacted by (process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "23.88.105.196/mozglue.dll" which was contacted by (process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "23.88.105.196/msvcp140.dll" which was contacted by (process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "23.88.105.196/nss3.dll" which was contacted by (process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "23.88.105.196/softokn3.dll" which was contacted by (process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "23.88.105.196/vcruntime140.dll" which was contacted by (process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe as "Mal/HTMLGen-A".			
3/5	Hide Tracks	Deletes file after execution	1	-
	• File "c:\users\rdhj0cnfevzx\desktop\7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe" deletes itself by cmd.			
3/5	Network Connection	Uses HTTP to upload a large amount of data.	1	-
	• (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe uploads 114.774KB data using HTTP POST.			
2/5	Data Collection	Reads sensitive browser data	21	-

Score	Category	Operation	Count	Classification
		• (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "BlackHawk" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Opera" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Chromium" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Kometa" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Amigo" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Torch" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Orbitum" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Vivaldi" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Comodo Dragon" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Epic Privacy Browser" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "CocCoc" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Uran" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "CentBrowser" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "7Star" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Elements Browser" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of web browser "Chedot" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.		
2/5	Data Collection	Reads sensitive ftp data	2	-
		• (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of ftp application "FileZilla" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of ftp application "Total Commander" by file.		
2/5	Data Collection	Reads sensitive mail data	1	-
		• (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file.		
1/5	Discovery	Enumerates running processes	1	-
		• (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe enumerates running processes.		
1/5	Discovery	Possibly does reconnaissance	6	-
		• (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to gather information about application "Cyberfox" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to gather information about application "blackHawk" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to gather information about application "icecat" by file. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to gather information about application "WinSCP" by registry. • (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe tries to gather information about application "FileZilla" by file.		
1/5	Discovery	Reads system data	1	-
		• (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe reads the cryptographic machine GUID from registry.		
1/5	Hide Tracks	Creates process with hidden window	1	-
		• (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe starts (process #3) cmd.exe with a hidden window.		
1/5	Obfuscation	Resolves API functions dynamically	1	-
		• (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe resolves 235 API functions by name.		

Score	Category	Operation	Count	Classification
1/5	Network Connection	Downloads executable	6	Downloader

- (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe downloads executable via http from 23.88.105.196/freebl3.dll.
- (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe downloads executable via http from 23.88.105.196/mozglue.dll.
- (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe downloads executable via http from 23.88.105.196/msvcp140.dll.
- (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe downloads executable via http from 23.88.105.196/nss3.dll.
- (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe downloads executable via http from 23.88.105.196/softokn3.dll.
- (Process #1) 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe downloads executable via http from 23.88.105.196/vcruntime140.dll.

Score	Category	Operation	Count	Classification
-	Trusted	Known clean file	7	-

- File "Default.zip" is a known clean file.
- File "C:\ProgramData\\freebl3.dll" is a known clean file.
- File "C:\ProgramData\\mozglue.dll" is a known clean file.
- File "C:\ProgramData\\msvcp140.dll" is a known clean file.
- File "C:\ProgramData\\nss3.dll" is a known clean file.
- File "C:\ProgramData\\softokn3.dll" is a known clean file.
- File "C:\ProgramData\\vcruntime140.dll" is a known clean file.

Score	Category	Operation	Count	Classification
-	Trusted	Executable has a trusted signature	4	-

- Executable C:\ProgramData\\freebl3.dll has a trusted signature.
- Executable C:\ProgramData\\mozglue.dll has a trusted signature.
- Executable C:\ProgramData\\nss3.dll has a trusted signature.
- Executable C:\ProgramData\\softokn3.dll has a trusted signature.

Mitre ATT&CK Matrix

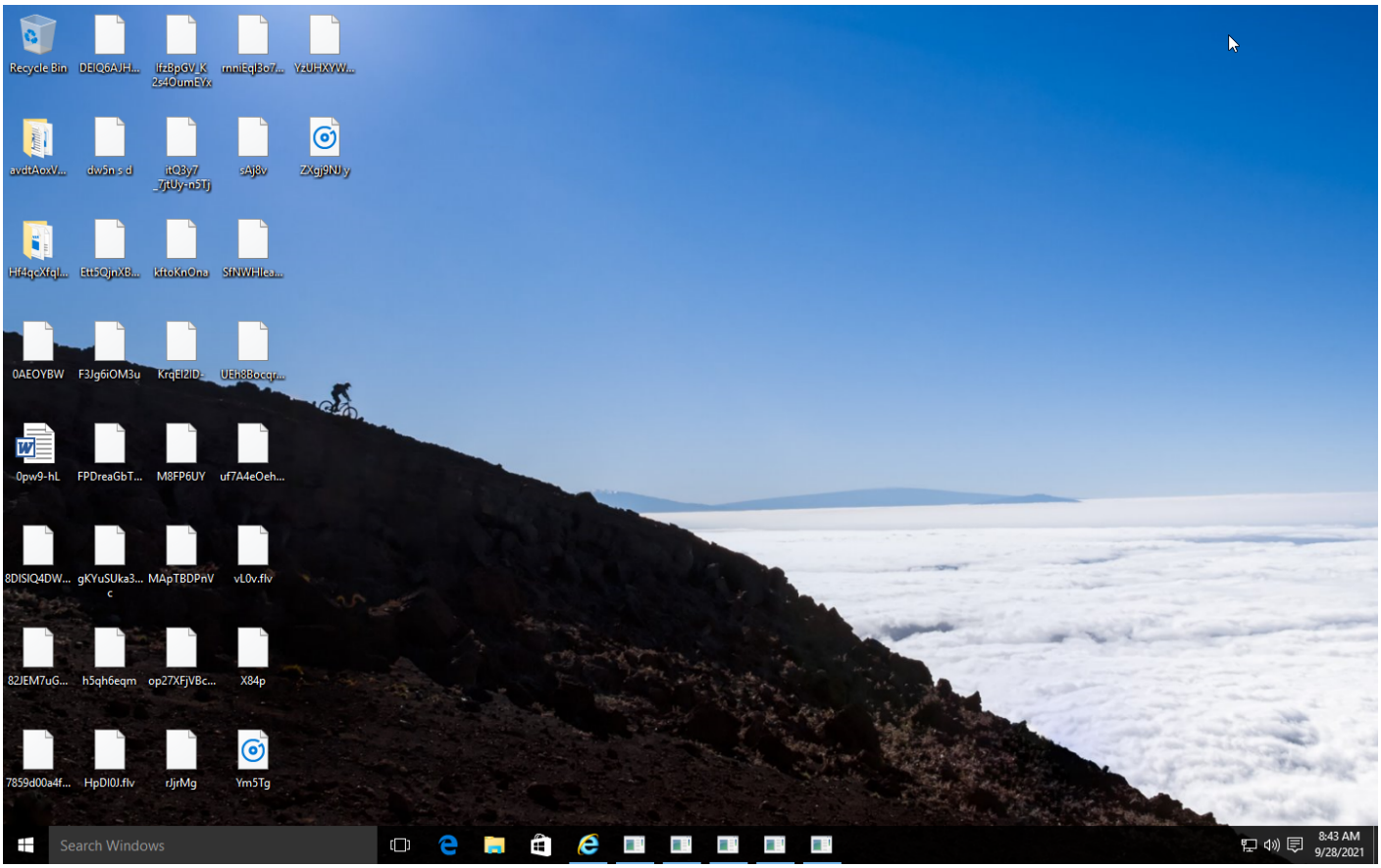
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File and Directory Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol	#T1020 Automated Exfiltration	
				#T1107 File Deletion	#T1003 Credential Dumping	#T1057 Process Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
				#T1070 Indicator Removal on Host		#T1012 Query Registry					
				#T1045 Software Packing		#T1082 System Information Discovery					

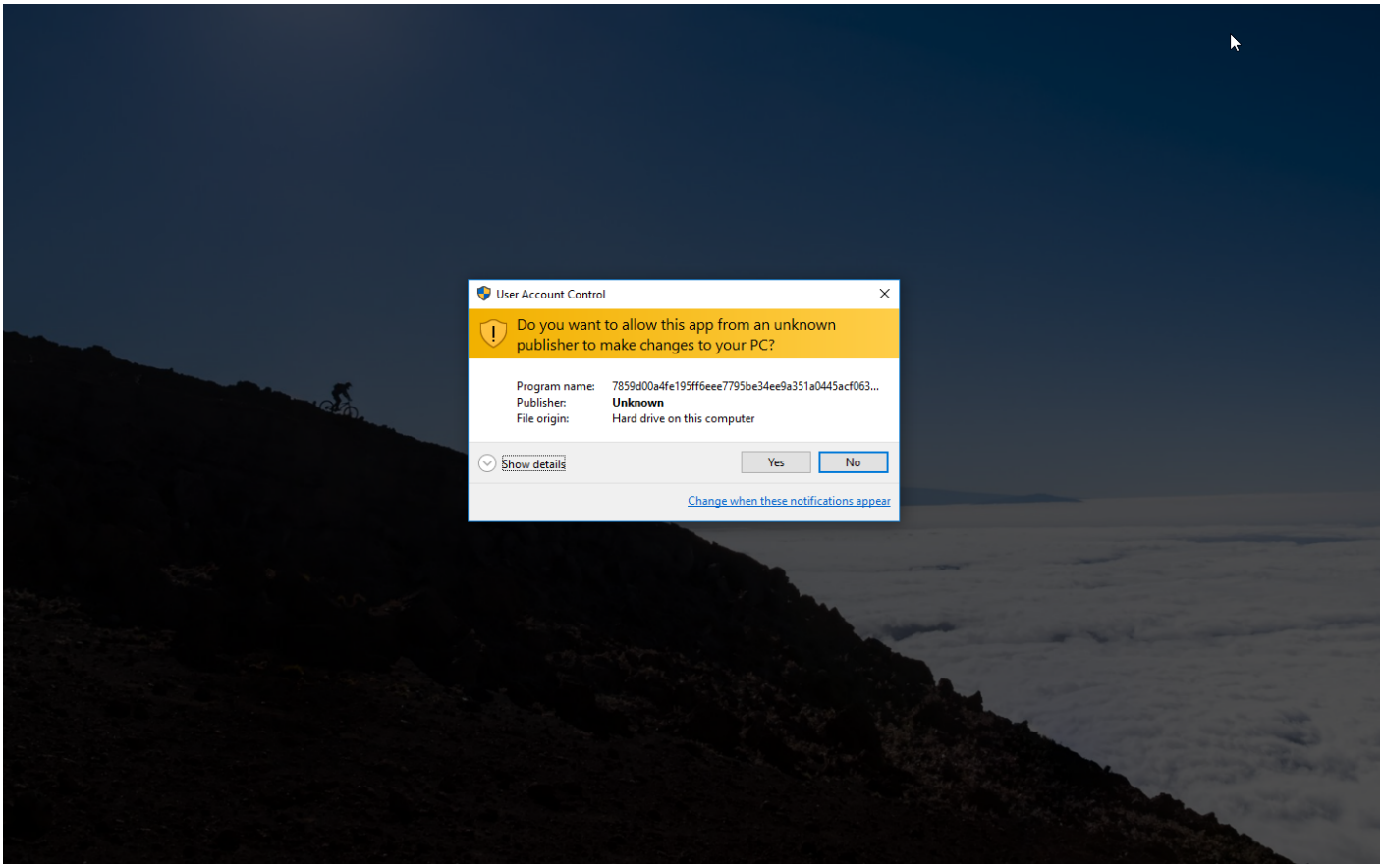
Sample Information

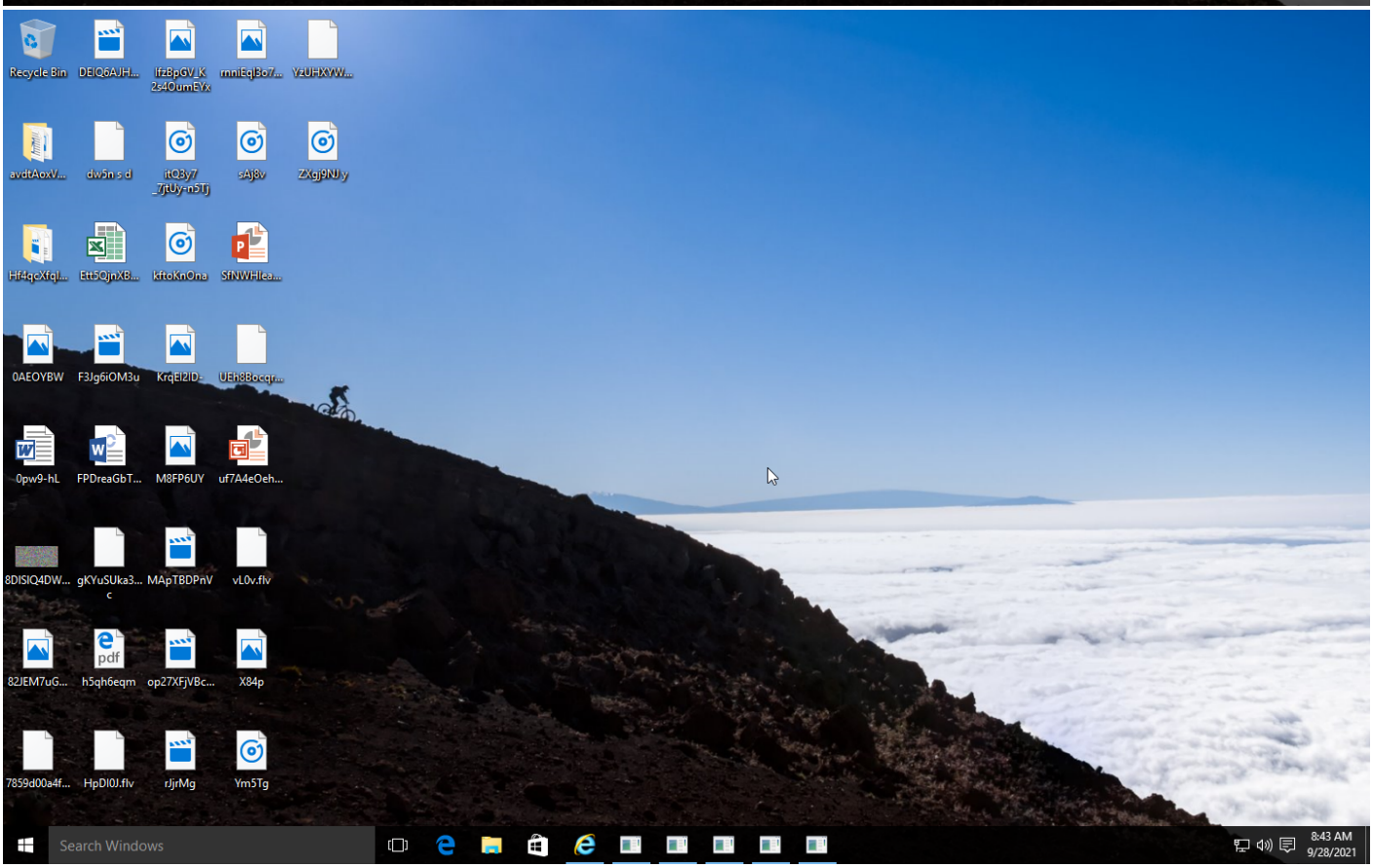
ID	#2782311
MD5	0bc97a36dc6135fc7a69c90c1c303439
SHA1	a3508e80c4e9bd20c04114c599be634107a49952
SHA256	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df
SSDeep	12288:c9OG5U3giCpd7Pq9m3QGpbSz9xLgo3/QwQf5gpZfQmzTO6sO99aO73pfqUtO:c9OGq50BZHpbOnUg/iOZfQ+Os9aOFf
ImpHash	f98cc9327e2d65cc6189a693f26e1c1d
File Name	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe
File Size	585.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 10:42 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✓
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	34
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
DEIQ6AJH...
IfzBpGV_K2s4OumEYx
rnniEqlBo7...
YzUHXYW...
avdtAoxV...
dw5n s d
itQ3y7_7jtUy-n5Tj
sAj8v
ZXgj9NJ y
Hf4qcXfqI...
Ett5QjnXB...
kftoKnOna
SfNWHlea...
0AEOYBW
F3Jg6iOM3u
KrqEl2lD...
UEh8Bocqr...
0pw9-hL
FPDreaGbT...
M8FP6UY
uf7A4eOeh...
8DISIQ4DW...
gKYuSUka3...c
MApTBDPnV
vL0v.flv
82JEM7uG...
h5qh6eqm
op27XFjVBc...
X84p
7859d00a4f...
HpDl0J.flv
rljrMg
Ym5Tg
Search Windows
8:43 AM
9/28/2021


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 7859d00a4fe195ff6eee7795be34ee9a351a0445acf063...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

124.62 KB total sent

2425.33 KB total received

2 ports 80, 443

3 contacted IP addresses

0 URLs extracted

7 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

10 URLs contacted, 3 servers

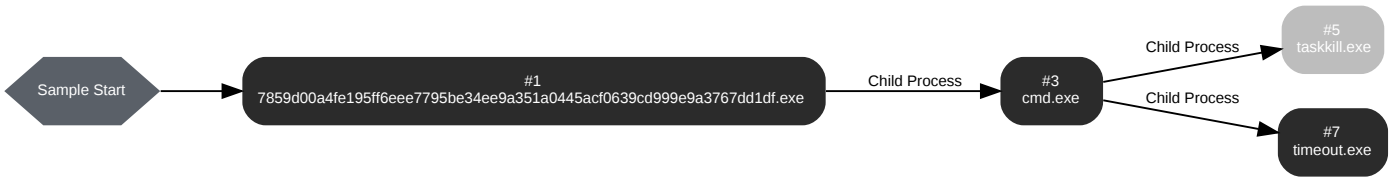
3 sessions, 124.62 KB sent, 2425.33 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	23.88.105.196/1008	-	-		0 bytes	NA
GET	23.88.105.196/freebl3.dll	-	-		0 bytes	NA
GET	23.88.105.196/mozglue.dll	-	-		0 bytes	NA
GET	23.88.105.196/msvcp140.dll	-	-		0 bytes	NA
GET	23.88.105.196/nss3.dll	-	-		0 bytes	NA
GET	23.88.105.196/softokn3.dll	-	-		0 bytes	NA
GET	23.88.105.196/vcruntime140.dll	-	-		0 bytes	NA
POST	23.88.105.196/	-	-		0 bytes	NA
GET	ok/	-	-		0 bytes	NA
GET	https://mas.to/@killern0	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 82283, Reason: Analysis Target
Unmonitor End Time	End Time: 168828, Reason: Terminated
Monitor duration	86.55s
Return Code	1
PID	1864
Parent PID	1600
Bitness	32 Bit

Dropped Files (10)

File Name	File Size	SHA256	YARA Match
-	326.45 KB	a770ecba3b08bbabd0a567fc978e50615f8b346709f8eb3cfacf3faab24090ba	✗
-	133.95 KB	3fe6b1c54b8cf28f571e0c5d6636b4069a8ab00b4f11dd842cfec00691d0c9cd	✗
-	429.80 KB	334e69ac9367f708ce601a6f490ff227d6c20636da5222f148b25831d22e13d4	✗
-	1216.95 KB	e2935b5b28550d47dc971f456d6961f20d1633b4892998750140e0eaa9ae9d78	✗
-	141.45 KB	43536adef2ddcc811c28d35fa6ce3031029a2424ad393989db36169ff2995083	✗
-	81.82 KB	c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d	✗
files\information.txt	4.76 KB	0104e7a72723fa470e498070a827824cd9ac1adf1500252bfb8379dcb19284b8	✗
Default.zip	22 bytes	8739c76e681f900923b900c9df0ef75cf421d39cabb54650c4b9ad19b6a76d85	✗
-	113.10 KB	1f39ed71e7ba03b350ffcc587a2e45e596534b08ce8f941e36b4b8e435c2343a	✗
03845cb8-7441-4a2f-8c0f-c90408af57788617605785.zip	111.16 KB	43a2fea6e4784454fca2610c3e81145ba08908237335502fb13caa01b11e7cf1	✗

Host Behavior

Type	Count
Module	304
File	497
Environment	2
System	50
User	5
Process	366
Registry	166
Keyboard	2

Network Behavior

Type	Count
HTTP	9
HTTPS	1
TCP	3

Process #3: cmd.exe

ID	3
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c taskkill /im 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe /f & timeout /t... ...Users\RDhJ0CNFevzX\Desktop\7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe" & del C:\ProgramData*.dll & exit
Initial Working Directory	C:\ProgramData\
Monitor Start Time	Start Time: 153686, Reason: Child Process
Unmonitor End Time	End Time: 175194, Reason: Terminated
Monitor duration	21.51s
Return Code	0
PID	3052
Parent PID	1864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	38
Environment	27
System	1
Process	2

Process #5: taskkill.exe

ID	5
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /im 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe /f
Initial Working Directory	C:\ProgramData\
Monitor Start Time	Start Time: 162015, Reason: Child Process
Unmonitor End Time	End Time: 168947, Reason: Terminated
Monitor duration	6.93s
Return Code	0
PID	4968
Parent PID	3052
Bitness	32 Bit

Process #7: timeout.exe

ID	7
File Name	c:\windows\syswow64\timeout.exe
Command Line	timeout /t 6
Initial Working Directory	C:\ProgramData\
Monitor Start Time	Start Time: 167974, Reason: Child Process
Unmonitor End Time	End Time: 175018, Reason: Terminated
Monitor duration	7.04s
Return Code	0
PID	4640
Parent PID	3052
Bitness	32 Bit

Host Behavior

Type	Count
Module	2
System	75
File	58

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df	C:\Users\RDhJ0CNFevzX\Desktop\7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	Sample File	585.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN
0104e7a72723fa470e498070a827824cd9ac1adf1500252bfb8379dcb19284b8	files\information.txt, C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\information.txt, information.txt	Dropped File	4.76 KB	text/plain	Access, Write, Read, Create	CLEAN
8739c76e681f900923b900c9df0ef75cf421d39cabb54650c4b9ad19b6a76d85	Files/Default.zip, C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Files\Default.zip, Default.zip	Dropped File	22 bytes	application/zip	Access, Delete, Read, Create	CLEAN
1f39ed71e7ba03b350ffcc587a2e45e596534b08ce8f941e36b4b8e435c2343a	screenshot.jpg	Dropped File	113.10 KB	image/jpeg	-	CLEAN
a770ecba3b08bbabd0a567fc978e50615f8b346709f8eb3cfacf3faab24090ba	C:\ProgramData\\freebl3.dll	Downloaded File	326.45 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	CLEAN
3fe6b1c54b8cf28f571e0c5d636b4069a8ab00b4f11dd842cfec00691d0c9cd	C:\ProgramData\\mozglue.dll	Downloaded File	133.95 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	CLEAN
334e69ac9367f708ce601a6f490ff227d6c20636da5222f148b25831d22e13d4	C:\ProgramData\\msvcp140.dll	Downloaded File	429.80 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	CLEAN
e2935b5b28550d47dc971f456d6961f20d1633b4892998750140e0eaa9ae9d78	C:\ProgramData\\nss3.dll	Downloaded File	1216.95 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	CLEAN
43536adef2ddcc811c28d35fa6ce3031029a2424ad393989db36169ff2995083	C:\ProgramData\\softokn3.dll	Downloaded File	141.45 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	CLEAN
c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d	C:\ProgramData\\vcruntime140.dll	Downloaded File	81.82 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	CLEAN
43a2fea6e4784454fca2610c3e81145ba08908237335502fb13caa01b11e7cf1	03845cb8-7441-4a2f-8c0f-c90408af57788617605785.zip	Downloaded File	111.16 KB	application/zip	Read, Write, Access, Delete, Create	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	Sample File	Access	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X	Accessed File	Access, Create	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files	Accessed File	Access, Create	CLEAN
C:\ProgramData\\freebl3.dll	Downloaded File	Access, Write, Create	CLEAN
C:\ProgramData\\mozglue.dll	Downloaded File	Access, Write, Create	CLEAN
C:\ProgramData\\msvcp140.dll	Downloaded File	Access, Write, Create	CLEAN
C:\ProgramData\\nss3.dll	Downloaded File	Access, Write, Create	CLEAN
C:\ProgramData\\softokn3.dll	Downloaded File	Access, Write, Create	CLEAN
C:\ProgramData\\vcruntime140.dll	Downloaded File	Access, Write, Create	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Autofill	Accessed File	Access, Delete, Create	CLEAN

File Name	Category	Operations	Verdict
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Cookies	Accessed File	Access, Delete, Create	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\CC	Accessed File	Access, Delete, Create	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\History	Accessed File	Access, Delete, Create	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Downloads	Accessed File	Access, Delete, Create	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Wallets	Accessed File	Access, Delete, Create	CLEAN
passwords.txt	Accessed File	Access, Create	CLEAN
Cookies\IE_Cookies.txt	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Cookies\Low\???	Accessed File	Access	CLEAN
Cookies\Edge_Cookies.txt	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cookies\??	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Waterfox\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHawk\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\icecat\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera GX Stable\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Nichrome\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Maxthon5\Users\\Local State	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\brave\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\ \Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data\ \Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\TorBro\Profile\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Suhba\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Rafotech\Mustang\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data\ \Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Browser\Browser\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CryptoTab Browser\User Data\\Local State	Accessed File	Access	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Soft	Accessed File	Access, Delete, Create	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Soft\Authy	Accessed File	Access, Delete, Create	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Soft\Authy\ 8	Accessed File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Authy Desktop\Local Storage ?8	Accessed File	Access	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Soft\AuthyNew	Accessed File	Access, Delete, Create	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Soft\AuthyNew\ (	Accessed File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Authy Desktop\Local Storage\leveldb\ ?(	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Telegram	Accessed File	Access, Delete, Create	CLEAN
c	Accessed File	Access, Delete	CLEAN
h	Accessed File	Access, Delete	CLEAN

File Name	Category	Operations	Verdict
files\information.txt	Dropped File	Access, Write, Create	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Files	Accessed File	Access, Delete, Create	CLEAN
Default.zip	Dropped File	Access, Create	CLEAN
03845cb8-7441-4a2f-8c0f-c90408af57788617605785.zip	Downloaded File	Read, Write, Access, Delete, Create	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Cookies\Edge_Cookies.txt	Accessed File	Access, Delete, Read	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Cookies\IE_Cookies.txt	Accessed File	Access, Delete, Read	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Files\Default.zip	Dropped File	Access, Delete, Read	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\information.txt	Dropped File	Access, Read	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Wallets\Atomic	Accessed File	Access, Delete	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Wallets\Binance	Accessed File	Access, Delete	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Wallets\Coinomi	Accessed File	Access, Delete	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Wallets\ElectronCash	Accessed File	Access, Delete	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Wallets\Electrum	Accessed File	Access, Delete	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Wallets\ElectrumLTC	Accessed File	Access, Delete	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Wallets\Exodus	Accessed File	Access, Delete	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Wallets\JAXX	Accessed File	Access, Delete	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Wallets\Jaxx_New	Accessed File	Access, Delete	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Wallets\Monero	Accessed File	Access, Delete	CLEAN
C:\ProgramData\H70J3BXQYS8LVFGZF6VKCOP1X\files\Wallets\MultiDoge	Accessed File	Access, Delete	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
C:\ProgramData	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\timeout.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\Desktop\7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	Accessed File	Access, Write	CLEAN
C:\ProgramData*.dll	Accessed File	Access	CLEAN
\??\C:\ProgramData\freebl3.dll	Accessed File	Access, Write	CLEAN

File Name	Category	Operations	Verdict
\??\C:\ProgramData\mozglue.dll	Accessed File	Access, Write	CLEAN
\??\C:\ProgramData\msvcp140.dll	Accessed File	Access, Write	CLEAN
\??\C:\ProgramData\nss3.dll	Accessed File	Access, Write	CLEAN
\??\C:\ProgramData\softokn3.dll	Accessed File	Access, Write	CLEAN
\??\C:\ProgramData\vcruntime140.dll	Accessed File	Access, Write	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://23.88.105.196/1008	-	23.88.105.196	-	POST	MALICIOUS
http://23.88.105.196/freebl3.dll	-	23.88.105.196	-	GET	MALICIOUS
http://23.88.105.196/mozglue.dll	-	23.88.105.196	-	GET	MALICIOUS
http://23.88.105.196/msvcp140.dll	-	23.88.105.196	-	GET	MALICIOUS
http://23.88.105.196/nss3.dll	-	23.88.105.196	-	GET	MALICIOUS
http://23.88.105.196/softokn3.dll	-	23.88.105.196	-	GET	MALICIOUS
http://23.88.105.196/vcruntime140.dll	-	23.88.105.196	-	GET	MALICIOUS
http://23.88.105.196	-	23.88.105.196	-	POST	CLEAN
https://mas.to/@killern0	-	88.99.75.82	-	GET	CLEAN
http://ok	-	-	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
mas.to	88.99.75.82	-	HTTPS	CLEAN
ok	, 23.88.105.196	-	HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
88.99.75.82	mas.to	Germany	HTTPS, DNS, TCP	CLEAN
23.88.105.196	-	Germany	HTTP, TCP	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Configuration	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	access	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayName	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayVersion	access, read	7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN

Process

Process Name	Commandline	Verdict
7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	"C:\Users\RDhJ0CNFevzX\Desktop\7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe"	MALICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /c taskkill /im 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe /f & timeout /t... ...Users\RDhJ0CNFevzX\Desktop\7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe" & del C:\ProgramData*.dll & exit	CLEAN
taskkill.exe	taskkill /im 7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe /f	CLEAN
timeout.exe	timeout /t 6	CLEAN

YARA / AV

Antivirus (34)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKD.37670813	C:\Users\RDhJ0CNFevzX\Desktop\7859d00a4fe195ff6eee7795be34ee9a351a0445acf0639cd999e9a3767dd1df.exe	MALICIOUS
Memory Dump	Generic.Andromeda.4AA3DFD8	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS

File Type	Threat Name	File Name	Verdict
Memory Dump	Gen:Trojan.Heur.FU.gnZ@a0SiSGi	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-28 01:56:46+00:00
Built-in AV Database Records	10476967

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB

User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows