DYNAMIC ANALYSIS REPORT

#10833256

MALICIOUS

Classifications:	Spyware Injector Downloader
Threat Names:	SmokeLoader Mal/Generic-S C2/Generic-A Mal/HTMLGen-A
Verdict Reason:	-

Sample Type	**Windows Exe (x86-32)**
File Name	**19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe**
ID	#5056518
MD5	a8ef2558341a5ca8ac58ee543e260ee4
SHA1	5585cc5f17f424639dae06d6feba403c78232f6a
SHA256	19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb
File Size	182.00 KB
Report Created	2022-08-03 21:29 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (31 rules, 88 matches)

Score	Category	Operation	Count	Classification
5/5	Data Collection	Takes screenshot	1	-
	• (Process #8) 2eae.exe takes a screenshot using BitBlt API.			
5/5	Extracted Configuration	Smoke Loader configuration was extracted	1	Downloader
	• A configuration for Smoke Loader was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	4	Downloader
	• Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #9) bcatcih. • Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #3) explorer.exe. • Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #2) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe. • Rule "SmokeLoaderStrings" from ruleset "Malware" has matched on the function strings for (process #3) explorer.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Electrum Bitcoin Wallet, Electron Cash Bitcoin Cash Wallet, Epic Privacy Browser, CentBrowser, In... ..., MultiDoge DogeCoin wallet, Chromium, Torch, BlackHawk, Mozilla Thunderbird, CocCoc, Amigo, Cyberfox, Ethereum, Elements Browser.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #3) explorer.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih".			
4/5	Injection	Writes into the memory of another process	2	Injector
	• (Process #9) bcatcih modifies memory of (process #3) explorer.exe. • (Process #2) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe modifies memory of (process #3) explorer.exe.			
4/5	Injection	Modifies control flow of another process	2	Injector
	• (Process #9) bcatcih creates thread in (process #3) explorer.exe. • (Process #2) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe creates thread in (process #3) explorer.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
4/5	Reputation	Contacts known malicious URL	3	-
	• Reputation analysis labels the URL "http://host-file-host6.com/" which was contacted by (process #3) explorer.exe as Mal/HTMLGen-A. • (Process #8) 2eae.exe contacted known malicious URL http://moneye.link/request. • Reputation analysis labels the URL "http://moneye.link/8sd87v7.php" which was contacted by (process #8) 2eae.exe as C2/Generic-A.			
4/5	Reputation	Resolves known malicious domain	2	-
	• Reputation analysis labels the resolved domain "host-file-host6.com" as Mal/HTMLGen-A. • Resolved domain "moneye.link" is a known malicious domain.			
3/5	Data Collection	Reads cryptocurrency wallet locations	4	-

Score	Category	Operation	Count	Classification
	• (Process #8) 2eae.exe tries to read the cryptocurrency wallet "Ethereum" for "ETH". • (Process #8) 2eae.exe tries to read the cryptocurrency wallet "Electrum Bitcoin Wallet" for "BTC". • (Process #8) 2eae.exe tries to read the cryptocurrency wallet "Electron Cash Bitcoin Cash Wallet" for "BCH". • (Process #8) 2eae.exe tries to read the cryptocurrency wallet "MultiDoge DogeCoin wallet" for "DOGE".			
3/5	Network Connection	Uses HTTP to upload a large amount of data.	1	-
	• (Process #8) 2eae.exe uploads 262.15KB data using HTTP POST.			
3/5	YARA	Suspicious content matched by YARA rules	6	-
	• Rule "VMDeviceStrings" from ruleset "Generic" has matched on the function strings for (process #9) bcatcih. • Rule "VMModuleNames" from ruleset "Generic" has matched on the function strings for (process #9) bcatcih. • Rule "VMProcessNames" from ruleset "Generic" has matched on the function strings for (process #9) bcatcih. • Rule "VMModuleNames" from ruleset "Generic" has matched on the function strings for (process #2) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe. • Rule "VMDeviceStrings" from ruleset "Generic" has matched on the function strings for (process #2) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe. • Rule "VMProcessNames" from ruleset "Generic" has matched on the function strings for (process #2) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe.			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #2) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Hide Tracks	Deletes file after execution	3	-
	• (Process #3) explorer.exe deletes executed executable "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih". • (Process #3) explorer.exe deletes executed executable "C:\Users\RDhJ0CNFevzX\Desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe". • (Process #10) cmd.exe deletes executed executable "\??\C:\Users\RDHJ0C~1\AppData\Local\Temp\2EAE.exe".			
2/5	Data Collection	Reads sensitive browser data	20	-
	• (Process #8) 2eae.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Chrome Canary" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Chromium" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Kometa" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Amigo" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Torch" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Orbitum" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Comodo Dragon" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Epic Privacy Browser" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Vivaldi" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "CocCoc" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Uran" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "CentBrowser" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Elements Browser" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Opera" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #8) 2eae.exe tries to read sensitive data of web browser "BlackHawk" by file. • (Process #8) 2eae.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault. • (Process #8) 2eae.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Data Collection	Reads sensitive mail data	2	-
	• (Process #8) 2eae.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file. • (Process #8) 2eae.exe tries to read sensitive data of mail application "The Bat!" by file.			

Score	Category	Operation	Count	Classification
2/5	Anti Analysis	Delays execution	1	-
	• (Process #3) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	3	-
	• (Process #1) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe modifies memory of (process #2) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe. • (Process #5) 2eae.exe modifies memory of (process #8) 2eae.exe. • (Process #6) bcatcih modifies memory of (process #9) bcatcih.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	3	-
	• (Process #1) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe alters context of (process #2) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe. • (Process #5) 2eae.exe alters context of (process #8) 2eae.exe. • (Process #6) bcatcih alters context of (process #9) bcatcih.			
2/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih", to be triggered by LOGON. • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih", to be triggered by TIME. Task has been rescheduled by the analyzer.			
1/5	Obfuscation	Reads from memory of another process	3	-
	• (Process #1) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe reads from (process #1) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe. • (Process #5) 2eae.exe reads from (process #5) 2eae.exe. • (Process #6) bcatcih reads from (process #6) bcatcih.			
1/5	Obfuscation	Creates a page with write and execute permissions	3	-
	• (Process #1) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #5) 2eae.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #6) bcatcih allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #3) explorer.exe enumerates running processes.			
1/5	Mutex	Creates mutex	1	-
	• (Process #3) explorer.exe creates mutex with name "FE7F15060B875FB9FB2A49F08D5D03120C287F38".			
1/5	Hide Tracks	Creates process with hidden window	4	-
	• (Process #3) explorer.exe starts (process #3) explorer.exe with a hidden window. • (Process #5) 2eae.exe starts (process #5) 2eae.exe with a hidden window. • (Process #6) bcatcih starts (process #6) bcatcih with a hidden window. • (Process #8) 2eae.exe starts (process #10) cmd.exe with a hidden window.			
1/5	Discovery	Possibly does reconnaissance	4	-
	• (Process #8) 2eae.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #8) 2eae.exe tries to gather information about application "Cyberfox" by file. • (Process #8) 2eae.exe tries to gather information about application "blackHawk" by file. • (Process #8) 2eae.exe tries to gather information about application "icecat" by file.			
1/5	Discovery	Reads system data	1	-

Score	Category	Operation	Count	Classification
	• (Process #8) 2eae.exe reads the cryptographic machine GUID from registry.			
1/5	Network Connection	Downloads executable	1	Downloader
	• (Process #3) explorer.exe downloads Windows executable via http from https://dl.uploadgram.me/62e9795c1e118h?raw.			
1/5	Network Connection	Downloads file	2	-
	• (Process #3) explorer.exe downloads file via http from http://host-file-host6.com. • (Process #8) 2eae.exe downloads file via http from http://moneye.link/request.			
1/5	Obfuscation	Resolves API functions dynamically	4	-
	• (Process #1) 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe resolves 39 API functions by name. • (Process #5) 2eae.exe resolves 43 API functions by name. • (Process #8) 2eae.exe resolves 172 API functions by name. • (Process #6) bcatcih resolves 39 API functions by name.			
-	Trusted	Known clean file	7	-
	• Embedded file "mozglue.dll" is a known clean file. • Embedded file "sqlite3.dll" is a known clean file. • Embedded file "freebl3.dll" is a known clean file. • Embedded file "softokn3.dll" is a known clean file. • Embedded file "msvcp140.dll" is a known clean file. • Embedded file "vcruntime140.dll" is a known clean file. • Embedded file "nss3.dll" is a known clean file.			
-	Trusted	Executable has a trusted signature	4	-
	• Executable mozglue.dll has a trusted signature. • Executable freebl3.dll has a trusted signature. • Executable softokn3.dll has a trusted signature. • Executable nss3.dll has a trusted signature.			

Malware Configuration: SmokeLoader

Metadata	Key	Extracted Value
Mission ID	Value	2020
Encryption Key	Key Tags Algorithm Key Tags Algorithm	u4gEqg== Network Communication Decryption Key RC4 0vD4Mw== Network Communication Encryption Key RC4
URL	Url Url	http://host-file-host6.com/ http://host-host-file8.com/

Mitre ATT&CK Matrix

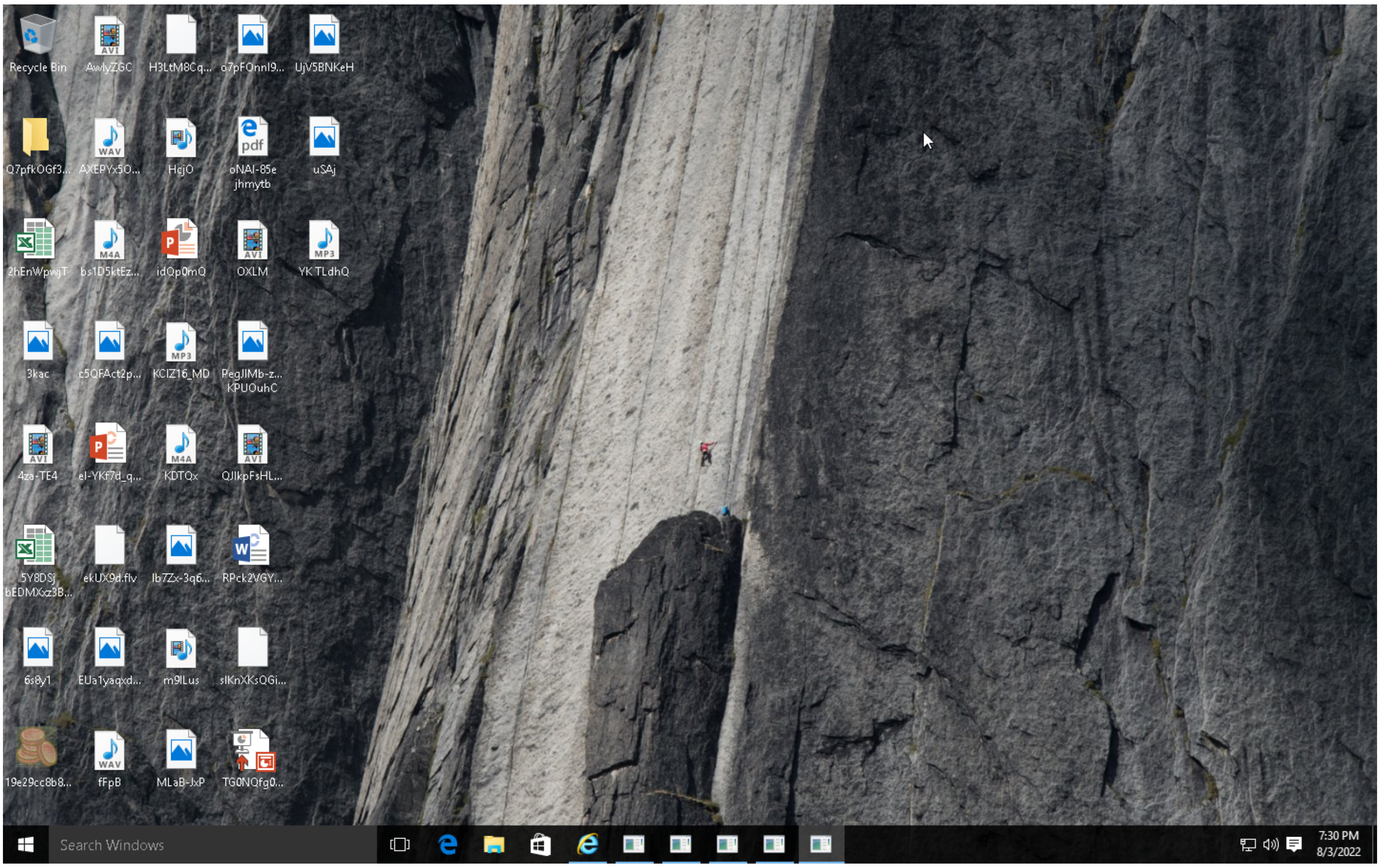
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1045 Software Packing	#T1081 Credentials in Files	#T1057 Process Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol	#T1020 Automated Exfiltration	
				#T1096 NTFS File Attributes	#T1003 Credential Dumping	#T1083 File and Directory Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
				#T1143 Hidden Window		#T1082 System Information Discovery		#T1113 Screen Capture			
						#T1012 Query Registry					

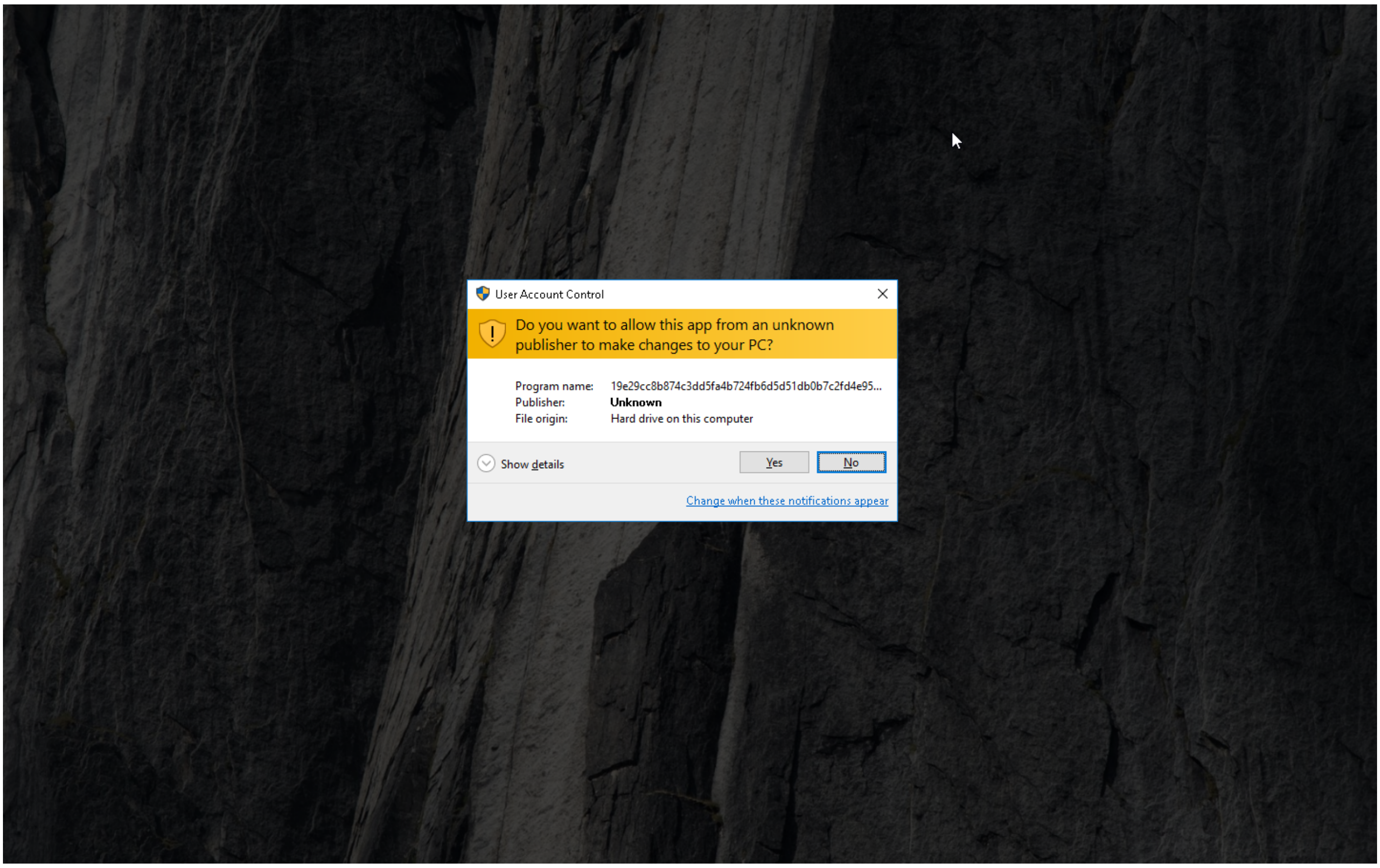
Sample Information

ID	#5056518
MD5	a8ef2558341a5ca8ac58ee543e260ee4
SHA1	5585cc5f17f424639dae06d6feba403c78232f6a
SHA256	19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb
SSDeep	3072:8xxxgL2AzyQ6w1x7O7SDpJspsrqdzd99r/wKPWKfJUY:8hMbzyY1x7O7SDp+iW399TPWKfJ
ImpHash	4cfbd807e4155075766f9f516fa9a7f3
File Name	19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe
File Size	182.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-03 21:29 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	10
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	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	10

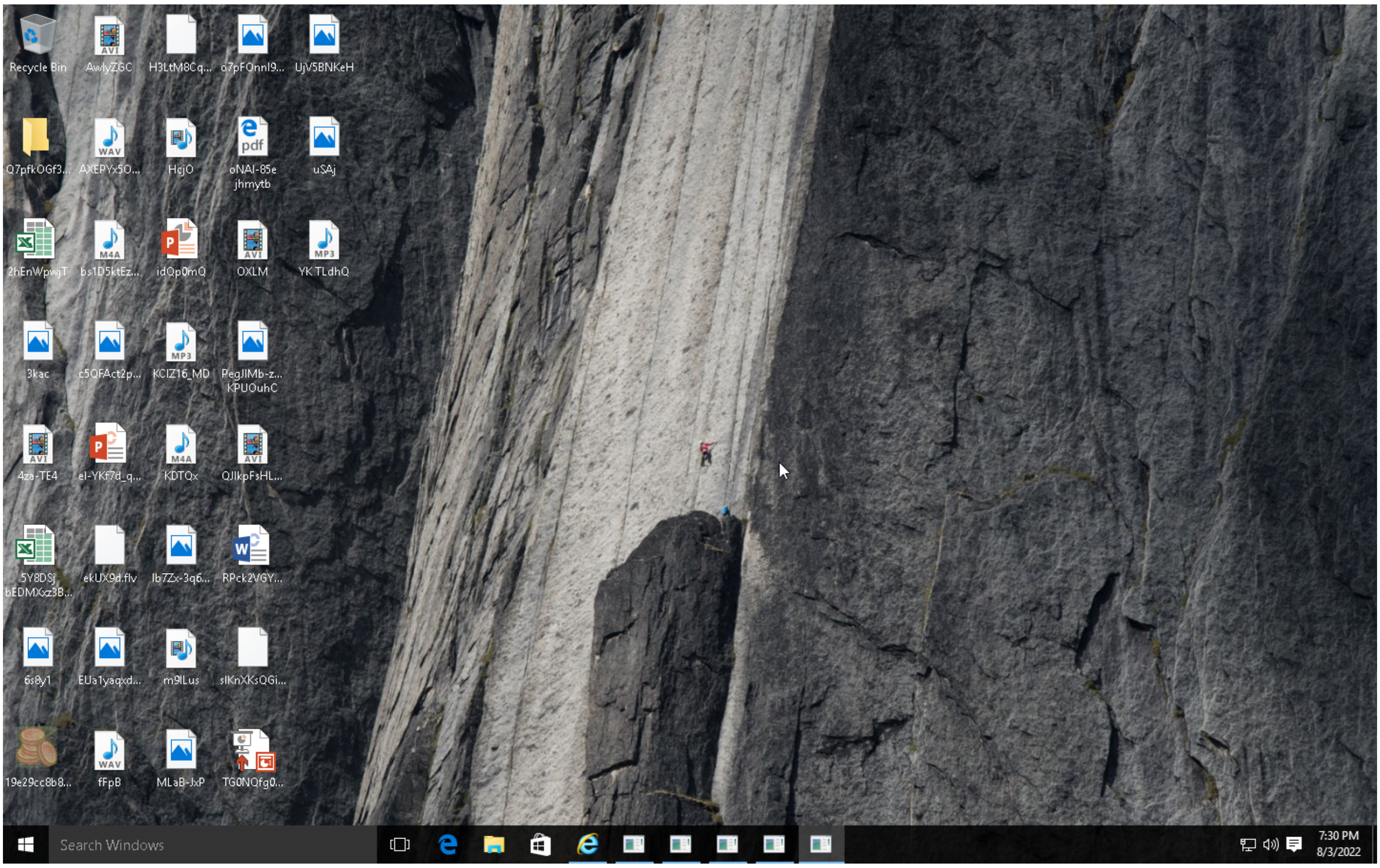




User Account Control

Do you want to allow this app from an unknown publisher to make changes to your PC?

Program name: 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e95...
Publisher: **Unknown**
File origin: Hard drive on this computer



Screenshots truncated

NETWORK

General

284.75 KB total sent

1998.60 KB total received

3 ports 80, 443, 53

4 contacted IP addresses

1 URLs extracted

7 files downloaded

0 malicious hosts detected

DNS

3 DNS requests for 3 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

4 URLs contacted, 3 servers

7 sessions, 303.20 KB sent, 2012.40 KB received

HTTP Requests

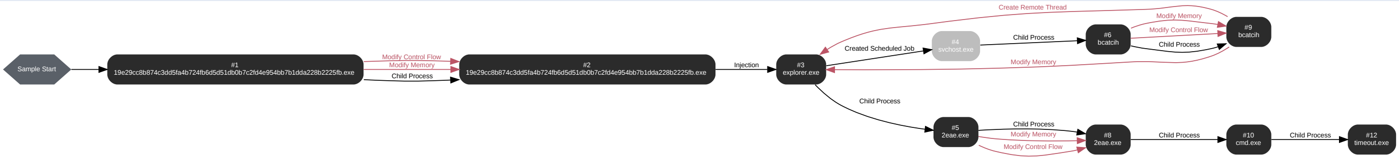
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	http://host-file-host6.com	-	-		0 bytes	NA
GET	http://moneye.link/request	-	-		0 bytes	NA
GET	http://moneye.link/8sd87v7.php	-	-		0 bytes	NA
GET	https://dl.uploadgram.me/62e9795c1e118h?raw	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	host-file-host6.com	NO_ERROR	34.118.39.10		NA
A	moneye.link	NO_ERROR	193.42.113.12		NA
A	dl.uploadgram.me	NO_ERROR	176.9.247.226		NA

BEHAVIOR

Process Graph



Process #1: 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 64751, Reason: Analysis Target
Unmonitor End Time	End Time: 90816, Reason: Terminated
Monitor duration	26.07s
Return Code	0
PID	4952
Parent PID	1972
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe	182.00 KB	19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb	✖

Host Behavior

Type	Count
Module	52
File	6
Environment	1
Window	1
Process	1
-	3
-	5

Process #2: 19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 83044, Reason: Child Process
Unmonitor End Time	End Time: 105903, Reason: Terminated
Monitor duration	22.86s
Return Code	0
PID	4976
Parent PID	4952
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe	0x135c	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe	0x135c	0x401000(4198400)	0x7200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe	0x135c	0x262008(2498568)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe	0x135c / 0x1374	0x77248fe0(1998884832)	-	✔	1

Host Behavior

Type	Count
Module	17
Keyboard	2
File	1
System	6
-	1
Registry	14
Process	1
-	1

Process #3: explorer.exe

ID	3
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 98564, Reason: Injection
Unmonitor End Time	End Time: 306430, Reason: Terminated by timeout
Monitor duration	207.87s
Return Code	Unknown
PID	1972
Parent PID	-
Bitness	64 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe	0x1374	0x540000(5505024)	0x5000	✔	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe	0x1374	0x3d20000(64094208)	0x16000	✔	1
Create Remote Thread	#2: c:\users\rdhj0cnfevzx\desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe	0x1374	0x3d21930(64100656)	-	✔	1
Modify Memory	#9: c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih	0xcc4	0x1e50000(31784960)	0x5000	✔	1
Modify Memory	#9: c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih	0xcc4	0x1e60000(31850496)	0x16000	✔	1
Create Remote Thread	#9: c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih	0xcc4	0x1e61930(31856944)	-	✔	1

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\2EAE.exe	404.50 KB	2748cff8786b1f19ff60478ade8c443336602a8d47fc6f3beec13d4edb70692d	✖
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	182.00 KB	19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\2EAE.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	43
System	8949
Process	17645
Mutex	2

Type	Count
Registry	2
File	19
User	1
COM	1

Network Behavior

Type	Count
HTTP	8
HTTPS	1

Process #4: svchost.exe

ID	4
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 132088, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 306430, Reason: Terminated by timeout
Monitor duration	174.34s
Return Code	Unknown
PID	864
Parent PID	1972
Bitness	64 Bit

Process #5: 2eae.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\2eae.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\2EAE.exe
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 135868, Reason: Child Process
Unmonitor End Time	End Time: 150371, Reason: Terminated
Monitor duration	14.50s
Return Code	0
PID	324
Parent PID	1972
Bitness	32 Bit

Host Behavior

Type	Count
Module	76
File	6
Environment	1
Window	1
Process	1
-	3
-	9

Process #6: bcatcih

ID	6
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 142080, Reason: Child Process
Unmonitor End Time	End Time: 172531, Reason: Terminated
Monitor duration	30.45s
Return Code	0
PID	1280
Parent PID	864
Bitness	32 Bit

Host Behavior

Type	Count
Module	51
File	6
Environment	1
Window	1
Process	1
-	3
-	5

Process #8: 2eae.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\2eae.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\2EAE.exe
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 147578, Reason: Child Process
Unmonitor End Time	End Time: 184376, Reason: Terminated
Monitor duration	36.80s
Return Code	0
PID	332
Parent PID	324
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\users\rdhj0cnfevzx\appdata\local\temp\2eae.exe	0x480	0x400000(4194304)	0x400	✔	1
Modify Memory	#5: c:\users\rdhj0cnfevzx\appdata\local\temp\2eae.exe	0x480	0x401000(4198400)	0x1c800	✔	1
Modify Memory	#5: c:\users\rdhj0cnfevzx\appdata\local\temp\2eae.exe	0x480	0x41e000(4317184)	0x8600	✔	1
Modify Memory	#5: c:\users\rdhj0cnfevzx\appdata\local\temp\2eae.exe	0x480	0x427000(4354048)	0x200	✔	1
Modify Memory	#5: c:\users\rdhj0cnfevzx\appdata\local\temp\2eae.exe	0x480	0x439000(4427776)	0x2600	✔	1
Modify Memory	#5: c:\users\rdhj0cnfevzx\appdata\local\temp\2eae.exe	0x480	0x43c000(4440064)	0x400	✔	1
Modify Control Flow	#5: c:\users\rdhj0cnfevzx\appdata\local\temp\2eae.exe	0x480 / 0x5ac	0x77248fe0(1998884832)	-	✔	1
Modify Memory	#5: c:\users\rdhj0cnfevzx\appdata\local\temp\2eae.exe	0x480	0x38e008(3727368)	0x4	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	200
System	15
Mutex	1
File	492
Keyboard	2
Registry	243

Type	Count
User	1
Process	1

Network Behavior

Type	Count
HTTP	3

Process #9: bcatcih

ID	9
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 153863, Reason: Child Process
Unmonitor End Time	End Time: 202886, Reason: Terminated
Monitor duration	49.02s
Return Code	0
PID	3276
Parent PID	1280
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih	0x4ec	0x400000(4194304)	0x200	✔	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih	0x4ec	0x401000(4198400)	0x7200	✔	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih	0x4ec	0x2c7008(2912264)	0x4	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih	0x4ec / 0xcc4	0x77248fe0(1998884832)	-	✔	1

Host Behavior

Type	Count
Module	17
Keyboard	2
File	1
System	6
-	1
Registry	14
Process	1
-	1

Process #10: cmd.exe

ID	10
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\RDHJ0C~1\AppData\Local\Temp\2EAE.exe" & exit
Initial Working Directory	C:\ProgramData\
Monitor Start Time	Start Time: 180576, Reason: Child Process
Unmonitor End Time	End Time: 192870, Reason: Terminated
Monitor duration	12.29s
Return Code	0
PID	3376
Parent PID	332
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	10
Process	1

Process #12: timeout.exe

ID	12
File Name	c:\windows\syswow64\timeout.exe
Command Line	timeout /t 5
Initial Working Directory	C:\ProgramData\
Monitor Start Time	Start Time: 185538, Reason: Child Process
Unmonitor End Time	End Time: 192532, Reason: Terminated
Monitor duration	6.99s
Return Code	0
PID	3272
Parent PID	3376
Bitness	32 Bit

Host Behavior

Type	Count
Module	2
System	49
File	52

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih, C:\Users\RDhJ0CNFevzX\Desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe	Sample File	182.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	MALICIOUS
2748cff8786b1f19ff60478ade8c443336602a8d47fc6f3beec13d4edb70692d	C:\Users\RDHJ0C~1\AppData\Local\Temp\2EAE.exe, \??\C:\Users\RDHJ0C~1\AppData\Local\Temp\2EAE.exe	Downloaded File	404.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	SUSPICIOUS
f02d38c231490b79375250343ff0237e1f3d5ff0abc6a7e84cb3eac13d96a485	-	Downloaded File	24 bytes	application/octet-stream	-	CLEAN
43536adef2ddcc811c28d35fa6ce3031029a2424ad393989db36169ff2995083	softokn3.dll	Extracted File	141.45 KB	application/vnd.microsoft.portable-executable	-	CLEAN
e2935b5b28550d47dc971f456d6961f20d1633b4892998750140e0eaa9ae9d78	nss3.dll	Extracted File	1216.95 KB	application/vnd.microsoft.portable-executable	-	CLEAN
a770ecba3b08bbabd0a567fc978e50615f8b346709f8eb3cfacf3faab24090ba	freebl3.dll	Extracted File	326.45 KB	application/vnd.microsoft.portable-executable	-	CLEAN
f4f3e0e22200f4613071047a8ba60a18876a5d930958c1994047295b0e2b3d60	-	Downloaded File	24 bytes	application/octet-stream	-	CLEAN
3de1fb0d1108907fd61d6d6b9a4c6b856af509e0af35578f158cfce5d634fe07	-	Downloaded File	1529.15 KB	application/zip	-	CLEAN
c5a6490b15d4b395cf907d364f24d1cfe6ffcc9090237305effdf5969bdddf4a	-	Downloaded File	55 bytes	application/octet-stream	-	CLEAN
c58a8dce6575fdfa6e503e20f23f266cb301d1a7c1c996be6d2246098d19df86	-	Downloaded File	28 bytes	text/plain	-	CLEAN
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	-	Modified File	128 bytes	application/octet-stream	-	CLEAN
3fe6b1c54b8cf28f571e0c5d6636b4069a8ab00b4f11dd842cfec00691d0c9cd	mozglue.dll	Extracted File	133.95 KB	application/vnd.microsoft.portable-executable	-	CLEAN
c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d	vcruntime140.dll	Extracted File	81.82 KB	application/vnd.microsoft.portable-executable	-	CLEAN
a1aaaf3a627c8a4f9e25bd0ecb3b446a79fe46d1695d03790c8c8f89eba402dc	-	Downloaded File	407 bytes	text/html	-	CLEAN
16574f51785b0e2fc29c2c61477eb47bb39f714829999511dc8952b43ab17660	sqlite3.dll	Memory Dump	630.46 KB	application/vnd.microsoft.portable-executable	-	CLEAN
334e69ac9367f708ce601a6f490ff227d6c20636da5222f148b25831d22e13d4	msvcp140.dll	Extracted File	429.80 KB	application/vnd.microsoft.portable-executable	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	Dropped File, Accessed File, VM File	Access, Create, Delete, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe	Sample File, Accessed File, VM File	Access, Delete	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data\Local State	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Maxthon5\Users\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\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\Local\QIP Surf\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Opera Software\Opera Neon\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\Roaming\Waterfox\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\ProgramData\sqlite3.dll	Accessed File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\timeout.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome SxS\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\CryptoTab Browser\User Data\Local State	Accessed File	Access	CLEAN
C:\ProgramData\nss3.dll	Accessed File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHawk\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
sqlite3.dll	Archive File	-	CLEAN
vcruntime140.dll	Archive File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\2EAE.exe	Accessed File, Downloaded File, Extracted File	Access, Create, Write	CLEAN
nss3.dll	Archive File	-	CLEAN
apfHQ	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera GX Stable\\Local State	Accessed File	Access	CLEAN
C:\ProgramData\mozglue.dll	Accessed File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih:Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\2EAE.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN

File Name	Category	Operations	Verdict
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\Roaming\K-Meleon\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FlashPeak\SlimBrowser\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\ProgramData\vcruntime140.dll	Accessed File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\wvhwbfa	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data\Local State	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\system32\advapi32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome Beta\User Data\Local State	Accessed File	Access	CLEAN
C:\ProgramData\softokn3.dll	Accessed File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\TorBro\Profile\Local State	Accessed File	Access	CLEAN
msvcp140.dll	Archive File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Local State	Accessed File	Access	CLEAN
softokn3.dll	Archive File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\\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\Microsoft\Edge\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data\Local State	Accessed File	Access	CLEAN
c:\lsarpc	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\Local State	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
C:\ProgramData\freebl3.dll	Accessed File	Access, Delete	CLEAN
C:\ProgramData\msvcp140.dll	Accessed File	Access, Delete	CLEAN
mozglue.dll	Archive File	-	CLEAN
freebl3.dll	Archive File	-	CLEAN
apfHQ	Accessed File	Access	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Access	CLEAN
apfHQ	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data\Local State	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://host-host-file8.com	-	-	-	-	MALICIOUS
http://host-file-host6.com	-	34.118.39.10	-	POST	MALICIOUS
http://moneye.link/request	-	193.42.113.12	-	GET	MALICIOUS
http://moneye.link/8sd87v7.php	-	193.42.113.12	-	GET, POST	MALICIOUS
https://dl.uploadgram.me/62e9795c1e118h?raw	-	176.9.247.226	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
host-file-host6.com	34.118.39.10	-	TCP, DNS, HTTP	MALICIOUS
moneye.link	193.42.113.12	-	TCP, DNS, HTTP	MALICIOUS
host-host-file8.com	-	-	-	CLEAN
dl.uploadgram.me	176.9.247.226	-	TCP, HTTPS, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
193.42.113.12	moneye.link	Russia	TCP, DNS, HTTP	CLEAN
176.9.247.226	dl.uploadgram.me	Germany	TCP, HTTPS, DNS	CLEAN
34.118.39.10	host-file-host6.com	Poland	TCP, DNS, HTTP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
FE7F15060B875FB9FB2A49F08D5D03120C287F38	access	explorer.exe	CLEAN
-	access	2eae.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\IE4Data\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\MobileOptionPack\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-0011-0000-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0409-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0019-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-012B-0409-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayName	access, read	2eae.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0019-0409-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00BA-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002C-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0115-0409-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}	access	2eae.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00BA-0409-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00A1-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002C-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0018-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Office16.PROPLUS\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00A1-0409-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E2-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0090-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	access, read	2eae.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0117-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001A-0409-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0018-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0044-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001B-0409-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00A1-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E1-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0115-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0117-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-012B-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0011-0000-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	access, read	2eae.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0090-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-006E-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E2-0409-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	access, read	2eae.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\DirectDrawEx\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-0019-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-0011-0000-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-0115-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\IEData\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-00E2-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\IE5BAKEX	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\WIC\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-001B-0409-0000-0000000FF1CE}	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-001B-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\Office16.PROPLUS	access	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-0117-0409-0000-0000000FF1CE}\DisplayName	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayVersion	access, read	2eae.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-001F-0409-0000-0000000FF1CE}\DisplayVersion	access, read	2eae.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe"	MALICIOUS
bcatcih	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	MALICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\RDHJ0C~1\AppData\Local\Temp\2EAE.exe" & exit	SUSPICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\19e29cc8b874c3dd5fa4b724fb6d5d51db0b7c2fd4e954bb7b1dda228b2225fb.exe"	SUSPICIOUS
2eae.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\2EAE.exe	SUSPICIOUS
2eae.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\2EAE.exe	SUSPICIOUS
bcatcih	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	SUSPICIOUS
timeout.exe	timeout /t 5	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

YARA (10)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Malware	SmokeLoaderStrings	SmokeLoader strings	Function Strings	-	Downloader	5/5
Generic	VMDeviceStrings	VM detection via known device names	Function Strings	-	-	3/5
Generic	VMModuleNames	VM detection via known module names	Function Strings	-	-	3/5
Generic	VMProcessNames	VM detection via known process names	Function Strings	-	-	3/5
Generic	VMModuleNames	VM detection via known module names	Function Strings	-	-	3/5
Generic	VMDeviceStrings	VM detection via known device names	Function Strings	-	-	3/5
Generic	VMProcessNames	VM detection via known process names	Function Strings	-	-	3/5

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	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.0.1 / 2022-07-04 05:54:12
Link Detonation Heuristics Version	4.6.0.3 / 2022-07-11 12:34:44
Smart Memory Dumping Rules Version	4.6.0.1 / 2022-07-04 05:54:12
Config Extractors Version	4.6.0.6 / 2022-07-25 08:17:36
Signature Trust Store Version	4.6.0.1 / 2022-07-04 05:54:12
VMRay Threat Identifiers Version	4.6.0.8 / 2022-07-26 09:34:25
YARA Built-in Ruleset Version	4.6.0.5

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
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