MALICIOUS

Classifications: Downloader, Spyware

Threat Names: Mal/Generic-S, Trojan.GenericKD.37569209

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe**
ID	#2732345
MD5	14e351015c5d632f888dbcac03871fae
SHA1	b5471c5eea356ce87ac5c2df8bbd9bc72cf84da9
SHA256	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa
File Size	458.48 KB
Report Created	2021-09-13 18:03 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (17 rules, 39 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: Chromium, CocCoc, Amigo, Mozilla Thunderbird, Cyberfox, CentBrowser, Google Chrome, Comodo Dragon... ...ements Browser, Internet Explorer, BlackHawk, Kometa, Opera, Uran, Epic Privacy Browser, Torch, Orbitum, Vivaldi, Mozilla Firefox.			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected the sample itself as "Trojan.GenericKD.37569209".			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
3/5	Network Connection	Uses HTTP to upload a large amount of data.	1	-
	• (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe uploads 112.021KB data using HTTP POST.			
2/5	Data Collection	Reads sensitive browser data	18	-
	• (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Chromium" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Kometa" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Amigo" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Torch" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Orbitum" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Comodo Dragon" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Epic Privacy Browser" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Vivaldi" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "CocCoc" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Uran" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "CentBrowser" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Elements Browser" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Opera" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of web browser "BlackHawk" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.		
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file.			
2/5	Hide Tracks	Deletes file after execution	1	-
	• (Process #4) cmd.exe deletes executed executable "c:\users\rdhj0cnfevzx\desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe".			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe modifies memory of (process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-

Score	Category	Operation	Count	Classification
	• (Process #1) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe alters context of (process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #1) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe enables process privilege "SeDebugPrivilege".			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe starts (process #1) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe with a hidden window. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe starts (process #4) cmd.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	2	-
	• (Process #1) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe reads from (process #1) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe. • (Process #1) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe reads from (process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Discovery	Possibly does reconnaissance	4	-
	• (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to gather information about application "Cyberfox" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to gather information about application "blackHawk" by file. • (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe tries to gather information about application "icecat" by file.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe resolves 90 API functions by name.			
1/5	Network Connection	Downloads executable	1	Downloader
	• (Process #2) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe downloads executable via http from http://77.222.42.92/public/sqlite3.dll.			
1/5	Execution	Executes itself	1	-
	• (Process #1) 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe.			
-	Trusted	Known clean file	1	-
	• File "C:\ProgramData\sqlite3.dll" is a known clean file.			

Mitre ATT&CK Matrix

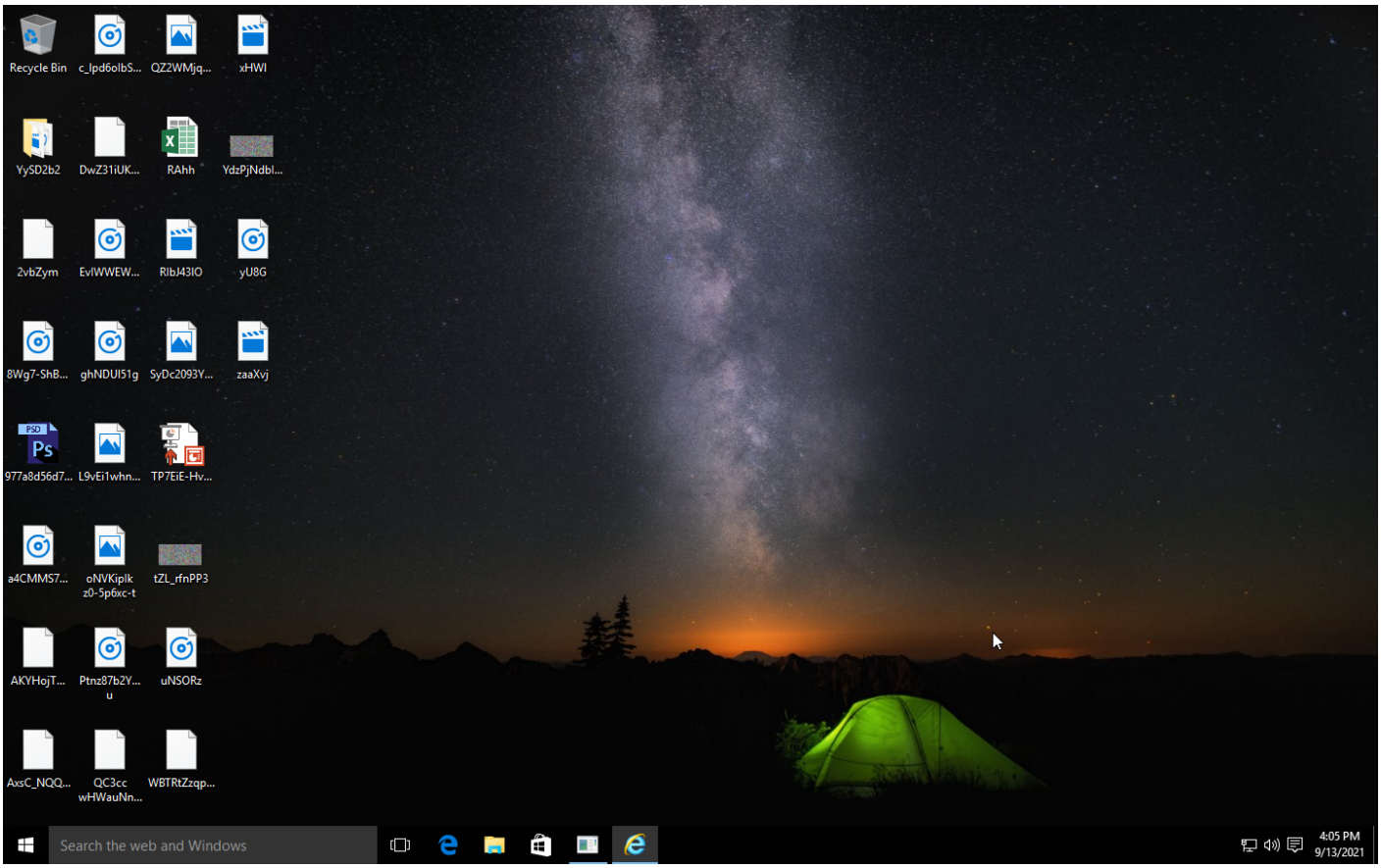
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File and Directory Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol	#T1020 Automated Exfiltration	
				#T1045 Software Packing	#T1003 Credential Dumping			#T1005 Data from Local System	#T1105 Remote File Copy		

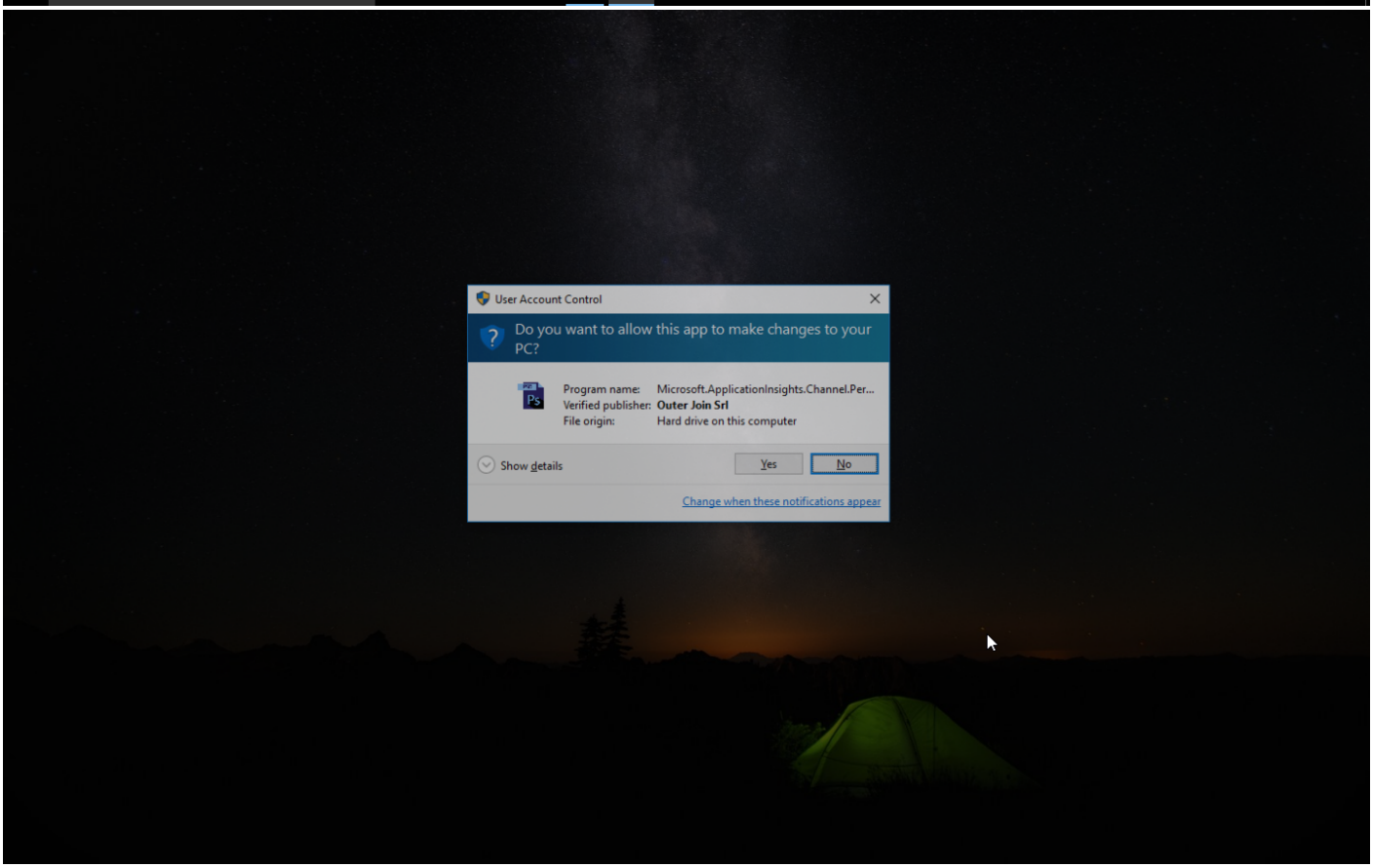
Sample Information

ID	#2732345
MD5	14e351015c5d632f888dbcac03871fae
SHA1	b5471c5eea356ce87ac5c2df8bbd9bc72cf84da9
SHA256	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa
SSDeep	6144:ebzheqatJY9oxu70Y7uh0doi9g9aPmaq/Ox4:O9aJYacQSuhqUaeb/L
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe
File Size	458.48 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-13 18:03 (UTC+2)
Analysis Duration	00:03:47
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	1
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
c_lpd6olbS...
QZ2WMjq...
xHWI
VySD2b2
DwZ31iUK...
RAhh
YdzPjNdbl...
2vbZym
EvlWWEW...
RIbJ43IO
yU8G
8Wg7-ShB...
ghNDUI51g
SyDc2093Y...
zaaXvj
977a8d56d7...
L9vEi1whn...
TP7EiE-Hv...
a4CMMS7...
oNVKiplk z0-5p6xc-t
tZL_rfnPP3
AKYHojT...
Ptnz87b2Y... u
uNSORz
AxsC_NQQ...
QC3cc wHWauNn...
WBTRtZzqp...
Search the web and Windows
4:05 PM
9/13/2021


User Account Control
Do you want to allow this app to make changes to your PC?
Program name: Microsoft.ApplicationInsights.Channel.Per...
Verified publisher: Outer Join Srl
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

NETWORK

General

112.55 KB total sent

649.27 KB total received

1 ports 80

1 contacted IP addresses

0 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 1 servers

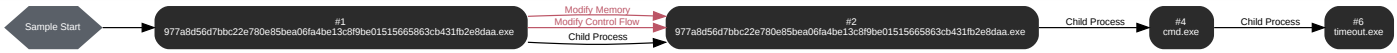
1 sessions, 112.55 KB sent, 649.27 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://77.222.42.92/public/sqlite3.dll	-	-		0 bytes	NA
GET	77.222.42.92/goodnews.php	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 95495, Reason: Analysis Target
Unmonitor End Time	End Time: 322825, Reason: Terminated by Timeout
Monitor duration	227.33s
Return Code	Unknown
PID	4888
Parent PID	1744
Bitness	32 Bit

Host Behavior

Type	Count
Process	2
System	1
Module	392
Window	3
Registry	3
File	1
User	1
-	3
-	259

Process #2: 977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 167945, Reason: Child Process
Unmonitor End Time	End Time: 226669, Reason: Terminated
Monitor duration	58.72s
Return Code	0
PID	328
Parent PID	4888
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	0xd30	0x400000(4194304)	0x400	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	0xd30	0x401000(4198400)	0x11600	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	0xd30	0x413000(4272128)	0x3e00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	0xd30	0x417000(4288512)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	0xd30	0x419000(4296704)	0x1a00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	0xd30	0x41b000(4304896)	0x1e00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	0xd30	0x2c1008(2887688)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	0xd30 / 0x4dc		-	✓	1

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\ProgramData\sqlite3.dll	630.46 KB	16574f51785b0e2fc29c2c61477eb47bb39f714829999511dc8952b43ab17660	✗

Host Behavior

Type	Count
Module	109
System	16
Mutex	1
File	290
Keyboard	2
Registry	157
User	1
Process	1

Network Behavior

Type	Count
HTTP	3
TCP	1

Process #4: cmd.exe

ID	4
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\RDhJ0CNFevzX\Desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe" & exit
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 221789, Reason: Child Process
Unmonitor End Time	End Time: 248812, Reason: Terminated
Monitor duration	27.02s
Return Code	0
PID	3360
Parent PID	328
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
Process	1
File	17

Process #6: timeout.exe

ID	6
File Name	c:\windows\syswow64\timeout.exe
Command Line	timeout /t 5
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 238220, Reason: Child Process
Unmonitor End Time	End Time: 247278, Reason: Terminated
Monitor duration	9.06s
Return Code	0
PID	1204
Parent PID	3360
Bitness	32 Bit

Host Behavior

Type	Count
Module	2
System	23
File	52

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa	C:\Users\RDhJ0CNFevzX\Desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	Sample File	458.48 KB	application/vnd.microsoft.portable-executable	Access, Delete	MALICIOUS
16574f51785b0e2fc29c2c61477eb47bb39f714829999511dc8952b43ab17660	C:\ProgramData\sqlite3.dll	Downloaded File	630.46 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	Sample File	Access, Delete	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSCOREE.DLL	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\KERNEL32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\KERNELBASE.dll	Accessed File	Access	CLEAN
C:\Windows\system32\apphelp.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ADVAPI32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\msvcrt.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\sechost.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\RPCRT4.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\SspiCli.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\CRYPTBASE.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\bcryptPrimitives.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\SHLWAPI.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\combase.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\GDI32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\USER32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\IMM32.DLL	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\kernel.appcore.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\VERSION.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSVCR120_CLR0400.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\8062d427acd64e37f4fded7b00f4a869\mscorlib.ni.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ole32.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\uxtheme.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\CRYPTSP.dll	Accessed File	Access	CLEAN
C:\Windows\system32\rsaenh.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\bcrypt.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\OLEAUT32.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\cc4e5d110dd318e8b7d61a9ed184ab74\System.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\9b645a48c9bcfc95aaadf6a069bb4ebe\System.Drawing.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\8cd2187094ba6cade0ca0fab4f932654\System.Windows.Forms.ni.dll	Accessed File	Access	CLEAN
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.10586.0_none_811bc0006c44242b\comctl32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\dwmapi.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73a1fc9d#\8d483c399064a7bdd1f920630af5a265\System.Runtime.Remoting.ni.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\amsi.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\abad45b9cc652ba7e38c4c837234c0ab\System.Core.ni.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\psapi.dll	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\ProgramData\sqlite3.dll	Downloaded File	Access, Create, Delete, Write	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\Microsoft\Edge\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\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
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\User Data\Local State	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
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\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\CentBrowser\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\CryptoTab Browser\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data\Local State	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\Opera Software\Opera Neon\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FlashPeak\SlimBrowser\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\Thunderbird\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\ProgramData\freebl3.dll	Accessed File	Access, Delete	CLEAN
C:\ProgramData\mozglue.dll	Accessed File	Access, Delete	CLEAN
C:\ProgramData\msvcp140.dll	Accessed File	Access, Delete	CLEAN
C:\ProgramData\nss3.dll	Accessed File	Access, Delete	CLEAN
C:\ProgramData\softokn3.dll	Accessed File	Access, Delete	CLEAN
C:\ProgramData\vcruntime140.dll	Accessed File	Access, Delete	CLEAN
C:\Windows\SysWOW64\timeout.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\Desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	Accessed File	Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\Desktop\977A8D~1.EXE	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\977A8D~1.EXE	Accessed File	Access, Delete	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://77.222.42.92/public/sqlite3.dll	-	77.222.42.92	-	GET	CLEAN
http://77.222.42.92/goodnews.php	-	77.222.42.92	-	GET, POST	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
77.222.42.92	-	Russia	HTTP, TCP	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\\DESCRIPTION\\System\\CentralProcessor\\0	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\\DESCRIPTION\\System\\CentralProcessor\\0\ProcessorNameString	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\ProductName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Cryptography	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Cryptography\MachineGuid	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\AddressBook	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\AddressBook\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\Connection Manager	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\Connection Manager\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\DirectDrawEx	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\DirectDrawEx\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\DXM_Runtime	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\DXM_Runtime\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\Fontcore	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\Fontcore\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\IE40	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\IE40\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\IE4Data	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\IE4Data\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\IE5BAKEX	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\IE5BAKEX\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\IEData	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\IEData\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\MobileOptionPack	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\MobileOptionPack\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\MPlayer2	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\MPlayer2\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\SchedulingAgent	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\SchedulingAgent\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\WIC	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\WIC\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\ \Uninstall\{90160000-008C-0000-0000-0000000FF1CE}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\ \Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\ \Uninstall\{90160000-008C-0000-0000-0000000FF1CE} \DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\ \Uninstall\{90160000-008C-0409-0000-0000000FF1CE}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\ \Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\ \Uninstall\{90160000-008C-0409-0000-0000000FF1CE} \DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {B175520C-86A2-35A7-8619-86DC379688B9}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d} \DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d} \DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\Display Name	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\Display Name	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\Display Name	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\Display Name	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\Display Name	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\Display Name	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566586 3cb431fb2e8daa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	access	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayName	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayVersion	access, read	977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	CLEAN

Process

Process Name	Commandline	Verdict
977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	"C:\Users\RDhJ0CNFevzX\Desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe"	MALICIOUS
977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	"C:\Users\RDhJ0CNFevzX\Desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe"	MALICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\RDhJ0CNFevzX\Desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe" & exit	SUSPICIOUS
timeout.exe	timeout /t 5	CLEAN

YARA / AV

Antivirus (1)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKD.37569209	C:\Users\RDhJ0CNFevzX\Desktop\977a8d56d7bbc22e780e85bea06fa4be13c8f9be01515665863cb431fb2e8daa.exe	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

Analyzer Information

Analyzer Version	4.2.2
Dynamic Engine Version	4.2.2 / 07/23/2021 03:44
Static Engine Version	4.2.2.0
Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-13 13:15:16+00:00
AV Exceptions Version	4.2.2.54 / 2021-07-23 03:00:10
VTI Ruleset Version	4.2.2.44 / 2021-09-01 14:38:52
YARA Built-in Ruleset Version	4.2.2.41
Link Detonation Heuristics Version	-
Signature Trust Store Version	4.2.2.54 / 2021-07-23 03:00:10
Analysis Report Layout Version	10

Software Information

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