MALICIOUS

Classifications: Spyware

Threat Names: RedNet

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe**
ID	#5069602
MD5	3333e40e61ff33675c26e7a712a7808d
SHA1	7e314834674c7bf514f68790a0e88b014e9115a4
SHA256	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3
File Size	399.50 KB
Report Created	2022-08-05 22:11 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (22 rules, 114 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	-
	• Rule "Packer_RedNet" from ruleset "Generic" has matched on a memory dump for (process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe.			
5/5	_data_collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Opera, Comodo IceDragon, Internet Explorer / Edge, k-Meleon, Mozilla Firefox, Exodus Cryptocurrency Wallet, Mozilla Thunderbird, Electrum Bitcoin Wallet, FileZilla, Cyberfox, Total Commander, The Bat!.			
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
	• Based on a combination of other detections, the sample gathers information about the running system to identify it.			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
3/5	_data_collection	Reads cryptocurrency wallet locations	2	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to read the cryptocurrency wallet "Electrum Bitcoin Wallet" for "BTC". • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to read the cryptocurrency wallet "Exodus Cryptocurrency Wallet".			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to detect antivirus software via WMI query: "SELECT * FROM AntivirusProduct".			
3/5	Defense Evasion	Tries to detect the presence of anti-spyware software	1	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to detect anti-spyware software via WMI query: "SELECT * FROM AntiSpyWareProduct".			
3/5	Defense Evasion	Tries to detect the presence of firewall software	1	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to detect firewall via WMI query: "SELECT * FROM FirewallProduct".			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe reads the network adapters' addresses by API.			
2/5	Discovery	Executes WMI query	8	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe executes WMI query: SELECT * FROM Win32_DiskDrive. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe executes WMI query: SELECT * FROM AntivirusProduct. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe executes WMI query: SELECT * FROM AntiSpyWareProduct. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe executes WMI query: SELECT * FROM FirewallProduct. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe executes WMI query: SELECT * FROM Win32_Process Where SessionId='1'. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe executes WMI query: SELECT * FROM Win32_Processor. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe executes WMI query: SELECT * FROM Win32_VideoController. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe executes WMI query: SELECT * FROM Win32_OperatingSystem.			
2/5	Discovery	Collects hardware properties	1	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe queries hardware properties via WMI.			
2/5	_data_collection	Reads sensitive browser data	6	-

Score	Category	Operation	Count	Classification
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to read sensitive data of web browser "Opera" by file. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to read sensitive data of web browser "k-Meleon" by file. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to read sensitive data of web browser "Comodo IceDragon" by file. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.		
2/5	_data_collection	Reads sensitive mail data	2	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to read sensitive data of mail application "The Bat!" by file.		
2/5	_data_collection	Reads sensitive ftp data	2	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to read sensitive data of ftp application "Total Commander" by file. • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to read sensitive data of ftp application "FileZilla" by file.		
2/5	Discovery	Enumerates running processes	1	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe enumerates running processes via WMI.		
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe queries OS version via WMI.		
1/5	Privilege Escalation	Enables process privilege	2	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe enables process privilege "SeDebugPrivilege". • (Process #3) wmiprvse.exe enables process privilege "SeDebugPrivilege".		
1/5	Obfuscation	Reads from memory of another process	75	-

- (Process #3) wmiprvse.exe reads from winlogon.exe.
- (Process #3) wmiprvse.exe reads from lsass.exe.
- (Process #3) wmiprvse.exe reads from svchost.exe.
- (Process #3) wmiprvse.exe reads from dwm.exe.
- (Process #3) wmiprvse.exe reads from (process #2) svchost.exe.
- (Process #3) wmiprvse.exe reads from spoolsv.exe.
- (Process #3) wmiprvse.exe reads from sihost.exe.
- (Process #3) wmiprvse.exe reads from runtimebroker.exe.
- (Process #3) wmiprvse.exe reads from explorer.exe.
- (Process #3) wmiprvse.exe reads from taskhostw.exe.
- (Process #3) wmiprvse.exe reads from shellexperiencehost.exe.
- (Process #3) wmiprvse.exe reads from searchui.exe.
- (Process #3) wmiprvse.exe reads from wmiadap.exe.
- (Process #3) wmiprvse.exe reads from (process #4) wmiprvse.exe.
- (Process #3) wmiprvse.exe reads from iexplore.exe.
- (Process #3) wmiprvse.exe reads from backgroundtaskhost.exe.
- (Process #3) wmiprvse.exe reads from final.exe.
- (Process #3) wmiprvse.exe reads from with-particular.exe.
- (Process #3) wmiprvse.exe reads from locationnotificationwindows.exe.
- (Process #3) wmiprvse.exe reads from include.exe.
- (Process #3) wmiprvse.exe reads from society-walk.exe.
- (Process #3) wmiprvse.exe reads from series girl into.exe.
- (Process #3) wmiprvse.exe reads from something.exe.
- (Process #3) wmiprvse.exe reads from at-produce.exe.
- (Process #3) wmiprvse.exe reads from management training.exe.
- (Process #3) wmiprvse.exe reads from better.exe.
- (Process #3) wmiprvse.exe reads from out_public.exe.
- (Process #3) wmiprvse.exe reads from start.exe.
- (Process #3) wmiprvse.exe reads from situation_group_head.exe.
- (Process #3) wmiprvse.exe reads from collection-will-husband.exe.
- (Process #3) wmiprvse.exe reads from foxmailincmail.exe.
- (Process #3) wmiprvse.exe reads from fling.exe.
- (Process #3) wmiprvse.exe reads from flashfxp.exe.
- (Process #3) wmiprvse.exe reads from filezilla.exe.
- (Process #3) wmiprvse.exe reads from far.exe.
- (Process #3) wmiprvse.exe reads from coreftp.exe.
- (Process #3) wmiprvse.exe reads from bitkinex.exe.
- (Process #3) wmiprvse.exe reads from barca.exe.
- (Process #3) wmiprvse.exe reads from alftp.exe.
- (Process #3) wmiprvse.exe reads from absolutetelnet.exe.
- (Process #3) wmiprvse.exe reads from 3dftp.exe.
- (Process #3) wmiprvse.exe reads from gmailnotifierpro.exe.
- (Process #3) wmiprvse.exe reads from icq.exe.
- (Process #3) wmiprvse.exe reads from leechftp.exe.
- (Process #3) wmiprvse.exe reads from ncftp.exe.
- (Process #3) wmiprvse.exe reads from notepad.exe.
- (Process #3) wmiprvse.exe reads from operamail.exe.
- (Process #3) wmiprvse.exe reads from outlook.exe.
- (Process #3) wmiprvse.exe reads from pidgin.exe.
- (Process #3) wmiprvse.exe reads from scriptftp.exe.
- (Process #3) wmiprvse.exe reads from skype.exe.
- (Process #3) wmiprvse.exe reads from smartftp.exe.
- (Process #3) wmiprvse.exe reads from thunderbird.exe.
- (Process #3) wmiprvse.exe reads from trillian.exe.
- (Process #3) wmiprvse.exe reads from webdrive.exe.
- (Process #3) wmiprvse.exe reads from whatsapp.exe.
- (Process #3) wmiprvse.exe reads from winscp.exe.
- (Process #3) wmiprvse.exe reads from yahoomessenger.exe.
- (Process #3) wmiprvse.exe reads from active-charge.exe.
- (Process #3) wmiprvse.exe reads from accupos.exe.

Score	Category	Operation	Count	Classification
1/5	Discovery	Possibly does reconnaissance	1	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe tries to gather information about application "FileZilla" by file.			
1/5	Network Connection	Performs DNS request	2	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe resolves host name "stcontact.top" to IP "91.203.192.233". • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe resolves host name "api.ip.sb" to IP "172.67.75.172".			
1/5	Network Connection	Connects to remote host	2	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe opens an outgoing TCP connection to host "172.67.75.172:443". • (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe opens an outgoing TCP connection to host "91.203.192.233:80".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe resolves 165 API functions by name.			

Mitre ATT&CK Matrix

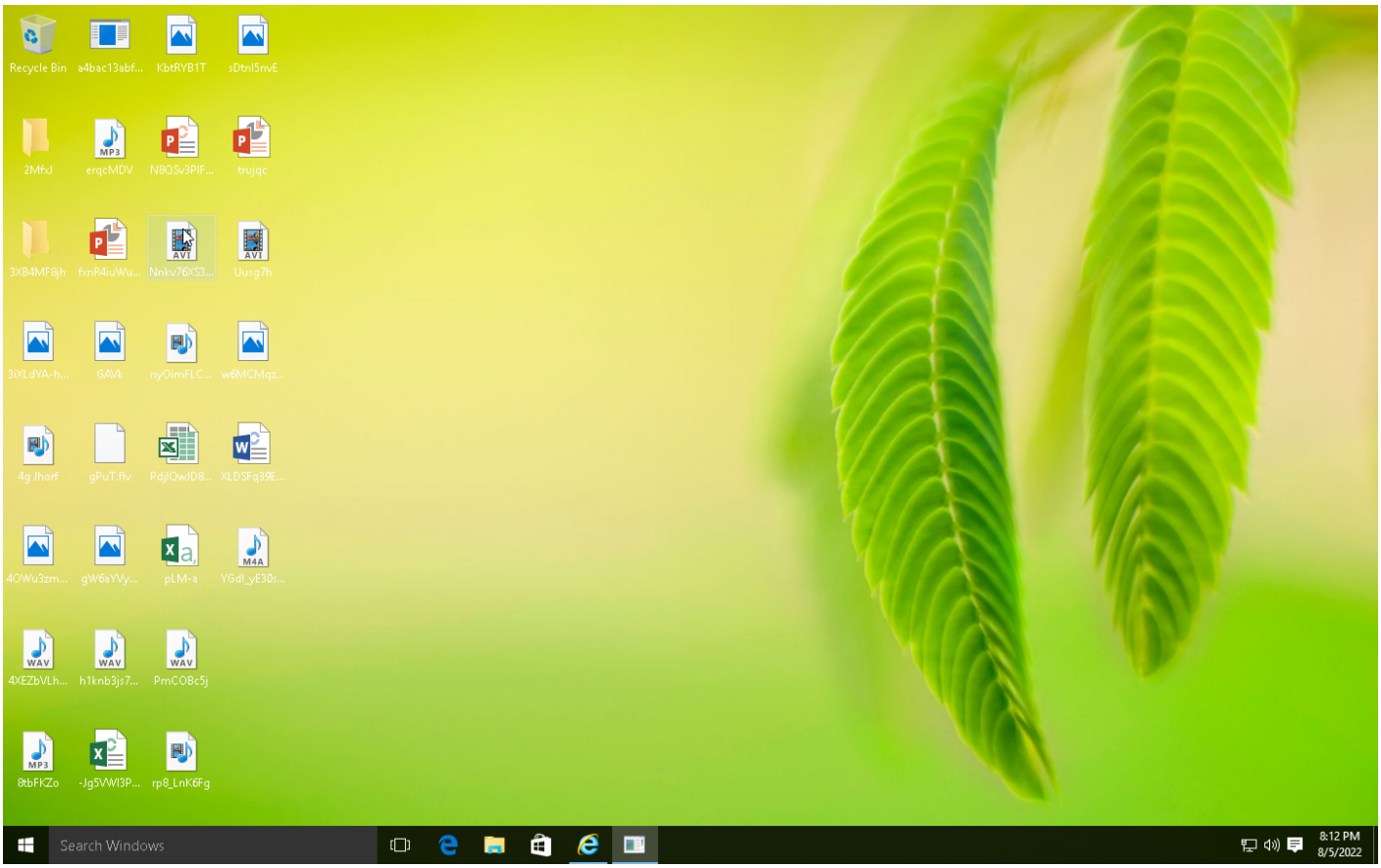
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1045 Software Packing	#T1081 Credentials in Files	#T1016 System Network Configuration Discovery		#T1119 Automated Collection			
						#T1082 System Information Discovery		#T1005 Data from Local System			
						#T1083 File and Directory Discovery					
						#T1063 Security Software Discovery					

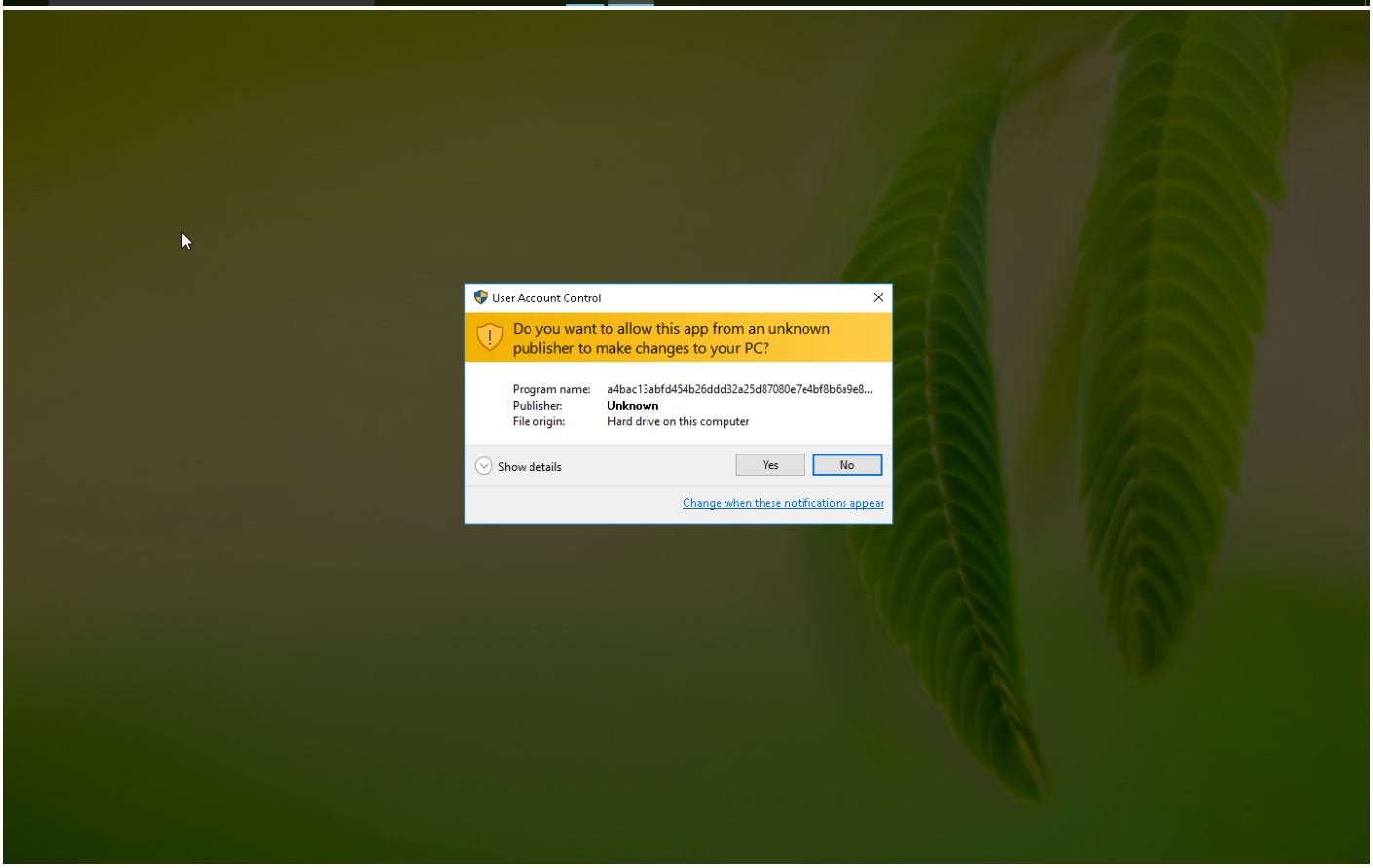
Sample Information

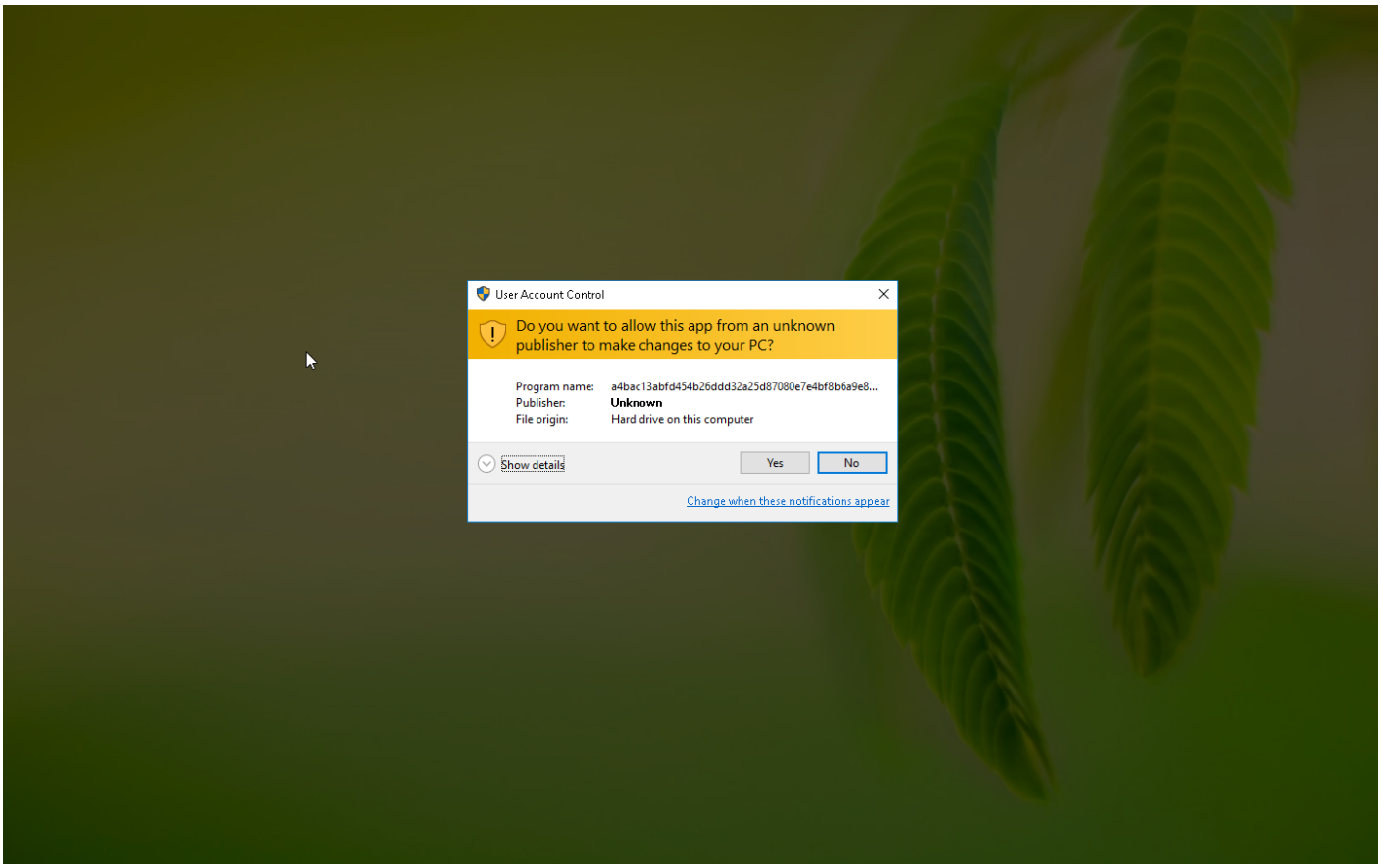
ID	#5069602
MD5	3333e40e61ff33675c26e7a712a7808d
SHA1	7e314834674c7bf514f68790a0e88b014e9115a4
SHA256	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3
SSDeep	12288:SAAqMeiD2Fr/cJZtfc9GVM5tQHOBR/F+L412g:xAFDem3EMWPQHOL9X
ImpHash	dc0513b2e8e866ceee30009dd51093dc
File Name	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe
File Size	399.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

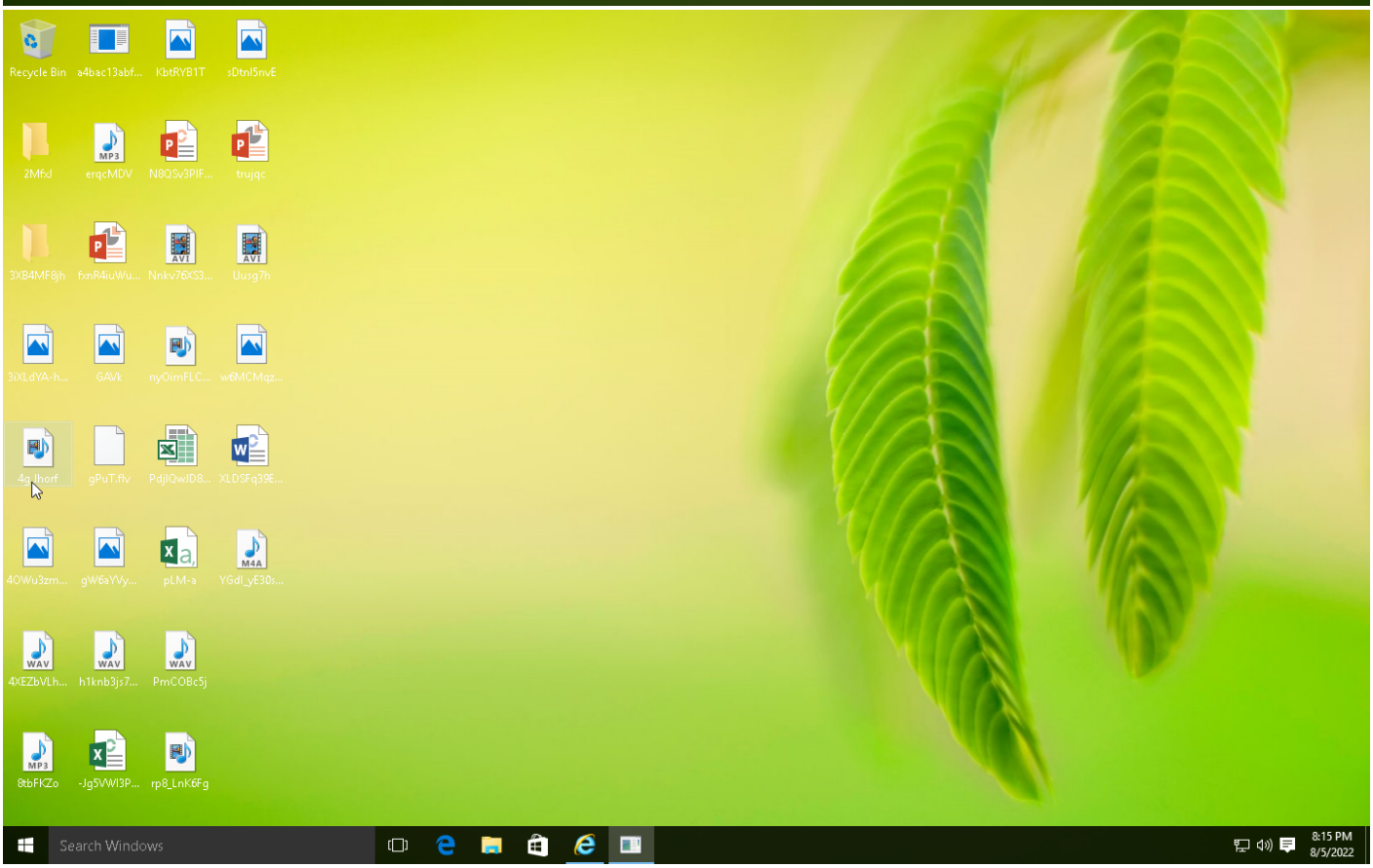
Analysis Information

Creation Time	2022-08-05 22:11 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	3
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	16


Recycle Bin
a4bac13abf...
KbtRYB1T
sDtnl5nvE
2MfxJ
erqcMDV
N8QSv3PIF...
trujqc
3XB4MF8jh
fxnR4iuWu...
Nnkv76XS3...
Uusg7h
3iXLdYA-h...
GAVk
nyOimFLC...
w6MCMqz...
4g Jhorf
gPuT.flv
PdjIQwJD8...
XLDSFq39E...
4OWu3zm...
gW6aYVy...
pLM-a
YGdI_yE30s...
4XEZbVLh...
h1knb3js7...
PmCOBc5j
8tbFKZo
-Jg5VWI3P...
rp8_LnK6Fg
Search Windows
8:12 PM
8/5/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e8...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

857.78 KB total sent

23.31 KB total received

3 ports 80, 443, 53

3 contacted IP addresses

0 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

1 sessions, 761 bytes sent, 4.04 KB received

HTTP Requests

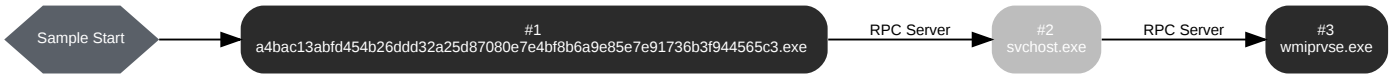
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://api.ip.sb/ip	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	stcontact.top	NO_ERROR	91.203.192.233		NA
A	api.ip.sb, api.ip.sb.cdn.cloudflare.net	NO_ERROR	172.67.75.172, 104.26.12.31, 104.26.13.31	api.ip.sb.cdn.cloudflare.net	NA

BEHAVIOR

Process Graph



Process #1: a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 69180, Reason: Analysis Target
Unmonitor End Time	End Time: 224469, Reason: Terminated
Monitor duration	155.29s
Return Code	0
PID	4532
Parent PID	1972
Bitness	32 Bit

Host Behavior

Type	Count
Module	310
File	385
Environment	11
System	13
User	3
Registry	388
-	3
-	173
COM	198
-	12
Window	2
Keyboard	3

Network Behavior

Type	Count
HTTPS	1
DNS	2
TCP	2

Process #2: svchost.exe

ID	2
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: 163101, Reason: RPC Server
Unmonitor End Time	End Time: 309252, Reason: Terminated by timeout
Monitor duration	146.15s
Return Code	Unknown
PID	864
Parent PID	4532
Bitness	64 Bit

Process #3: wmiprvse.exe

ID	3
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 163101, Reason: RPC Server
Unmonitor End Time	End Time: 309252, Reason: Terminated by timeout
Monitor duration	146.15s
Return Code	Unknown
PID	3048
Parent PID	864
Bitness	64 Bit

Host Behavior

Type	Count
User	2
System	218
Process	715
-	1209
Registry	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3	C:\Users\RDhJ0CNFevzX\Desktop\a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	Sample File	399.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
b14bcf7e766be0d5ea1f045fa63bc03a3d5c18687539e66f42a3051e5ea8d0af	-	Downloaded File	14 bytes	text/plain	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Windows\SYSTEM32\KERNELBASE.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\combase.dll	Accessed File	Access	CLEAN
C:\Program Files\Internet Explorer\iexplore.exe	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\system32\rsaenh.dll	Accessed File	Access	CLEAN
C:\Windows\system32\apphelp.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\bcryptPrimitives.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\mscoree.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\msimg32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ADVAPI32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\sitemanager.xml	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\psapi.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\KERNEL32.DLL	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\sechost.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\bcrypt.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\NordVPN	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\SYSTEM32\CRYPTSP.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe.config	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSVCR120_CLR0400.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\kernel.appcore.dll	Accessed File	Access	CLEAN
C:\Windows\system32\uxtheme.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\SHLWAPI.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows	Accessed File	Access, Create	CLEAN
C:\Windows\SYSTEM32\USER32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\GDI32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ole32.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\OLEAUT32.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\CRYPTBASE.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\IMM32.DLL	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\RPCRT4.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\msvcr100.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\msvcrt.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\SspiCli.dll	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://api.ip.sb/ip	-	104.26.12.31, 172.67.75.172, 104.26.13.31	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
stcontact.top	91.203.192.233	-	TCP, DNS	CLEAN
api.ip.sb	104.26.12.31, 172.67.75.172, 104.26.13.31	-	TCP, DNS, HTTPS	CLEAN
api.ip.sb.cdn.cloudflare.net	104.26.12.31, 172.67.75.172, 104.26.13.31	-	TCP, DNS, HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
104.26.12.31	api.ip.sb.cdn.cloudflare.net, api.ip.sb	United States	DNS	CLEAN
91.203.192.233	stcontact.top	Russia	TCP, DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
104.26.13.31	api.ip.sb.cdn.cloudflare.net, api.ip.sb	United States	DNS	CLEAN
172.67.75.172	api.ip.sb.cdn.cloudflare.net, api.ip.sb	United States	TCP, DNS, HTTPS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00A1-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0018-0409-0000-0000000FF1CE}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Net Framework Setup\NDP\v4\Client	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0019-0409-0000-0000000FF1CE}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0044-0409-0000-0000000FF1CE}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E2-0409-0000-0000000FF1CE}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Clients\StartMenuInternet\IEXPLORE.EXE\shell\open\command	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00A1-0409-0000-0000000FF1CE}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0115-0409-0000-0000000FF1CE}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Net Framework Setup\NDP\v4\Client\InstallPath	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00BA-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0019-0409-0000-0000000FF1CE}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0117-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0409-0000-0000000FF1CE}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Office16.PROPLUS\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0117-0409-0000-0000000FF1CE}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00A1-0409-0000-0000000FF1CE}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00BA-0409-0000-0000000FF1CE}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E1-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0090-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002C-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E2-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0011-0000-0000-0000000FF1CE}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0018-0409-0000-0000000FF1CE}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E1-0409-0000-0000000FF1CE}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Office16.PROPLUS	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Office16.PROPLUS\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0115-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001B-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001A-0409-0000-0000000FF1CE}\DisplayName	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayVersion	read, access	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe	"C:\Users\RDhJ0CNFevzX\Desktop\a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3.exe"	MALICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN

YARA / AV

YARA (16)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5

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	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.14 / 2022-08-03 12:19:21
YARA Built-in Ruleset Version	4.6.1.10

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