MALICIOUS

Classifications: -

Threat Names: CryptOne | Gen:Heur.Mint.Jamg.1 | Generic.Mint.Zamg.3.3897D085 | Trojan.Ransom.Shade.E | Gen:Trojan.Heur.1mLfX8U67Udc

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe**
ID	#969367
MD5	1d46afb839b846ede01cb925470f0488
SHA1	8cffc99cda16d5d6b5192c62fefae6c0ac89b33d
SHA256	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1
File Size	1215.26 KB
Report Created	2021-09-28 14:52 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (13 rules, 17 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	-
	• Rule "CryptOne_Packer" from ruleset "Generic" has matched on a memory dump for (process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	4	-
	• Built-in AV detected the sample itself as "Gen:Heur.Mint.Jamg.1". • Built-in AV detected a memory dump of (process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe as "Generic.Mint.Zamg.3.3897D085". • Built-in AV detected a memory dump of (process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe as "Trojan.Ransom.Shade.E". • Built-in AV detected a memory dump of (process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe as "Gen:Trojan.Heur.1mLfX8U67Udc".			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe queries OS version via WMI.			
2/5	Discovery	Executes WMI query	1	-
	• (Process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe executes WMI query: SELECT * FROM Win32_OperatingSystem.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe reads the network adapters' addresses by API.			
2/5	Heuristics	Signed executable failed signature validation	1	-
	• C:\Users\RDhJ0CNFevzX\Desktop\d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe is signed, but signature validation failed.			
2/5	Network Connection	Sets up server that accepts incoming connections	2	-
	• (Process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe starts a TCP server listening on localhost port 49702. • (Process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe starts a TCP server listening on localhost port 61439.			
1/5	Discovery	Tries to get network statistics	1	-
	• (Process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe gets network statistics via API.			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe adds ""C:\ProgramData\Windows\csrss.exe"" to Windows startup via registry.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe enumerates running processes.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe resolves 288 API functions by name.			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #1) d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe opens an outgoing TCP connection to host "131.188.40.189:443".			

Mitre ATT&CK Matrix

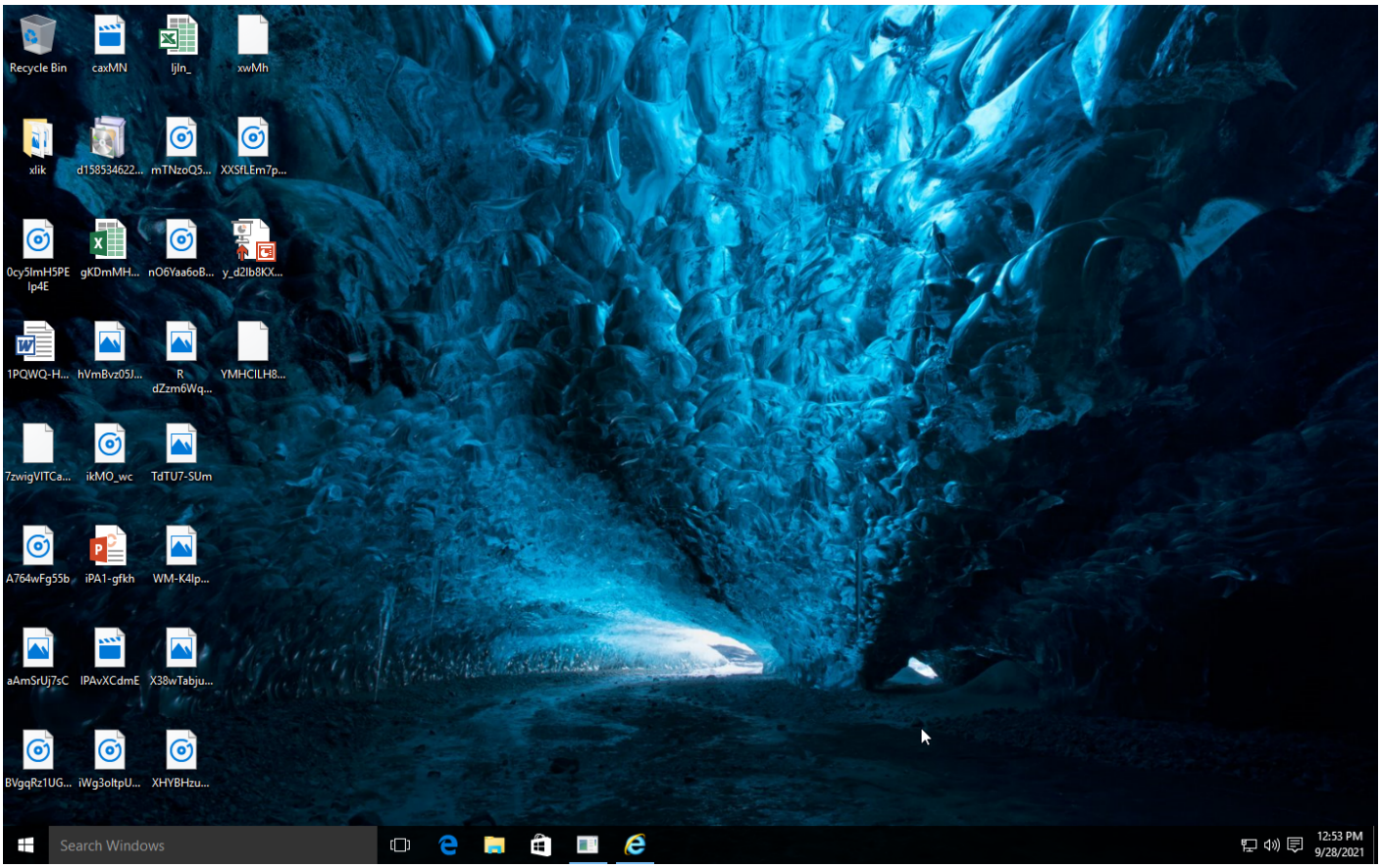
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1060 Registry Run Keys / Startup Folder		#T1112 Modify Registry		#T1082 System Information Discovery					
				#T1045 Software Packing		#T1016 System Network Configuration Discovery					
						#T1049 System Network Connections Discovery					
						#T1057 Process Discovery					

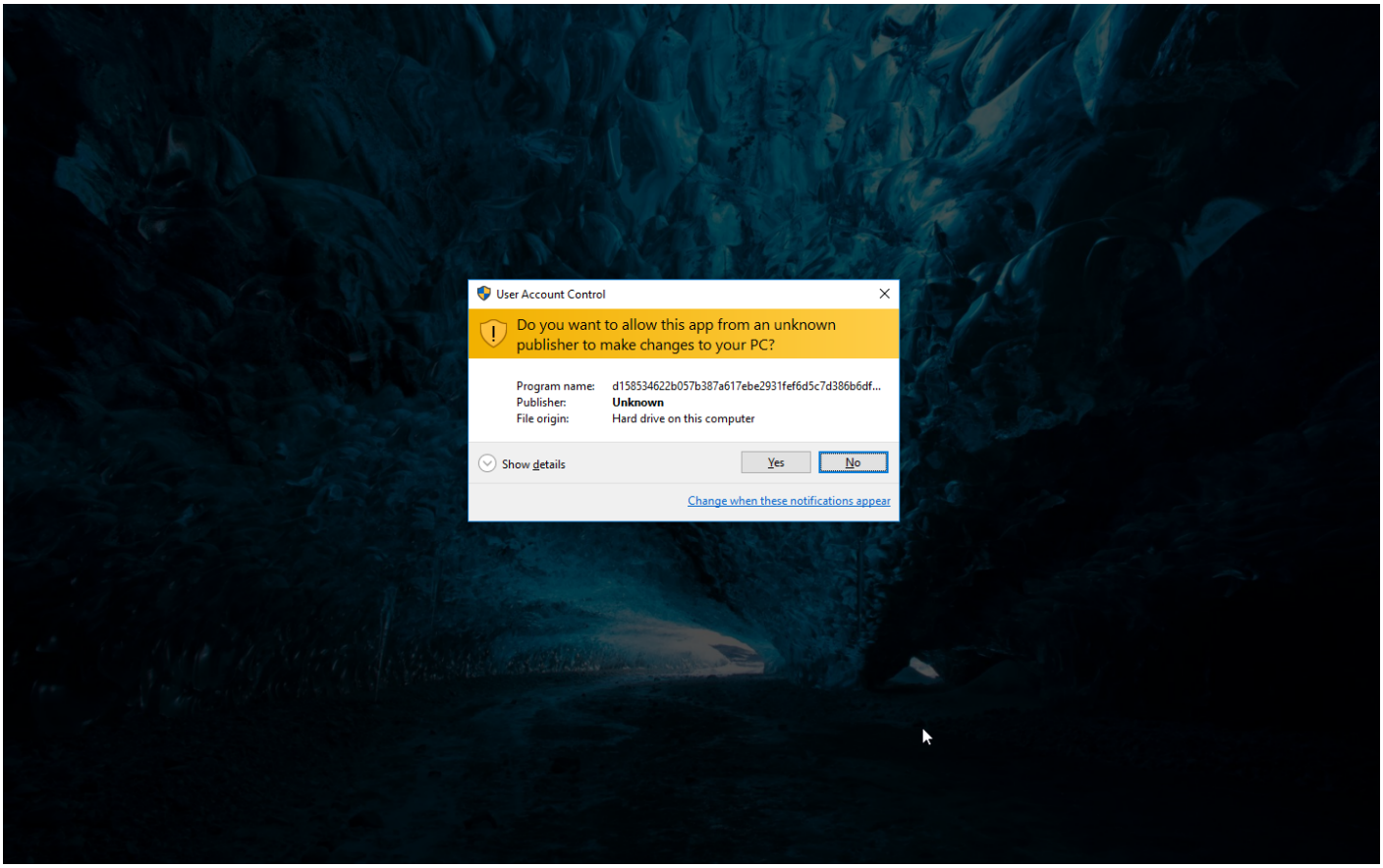
Sample Information

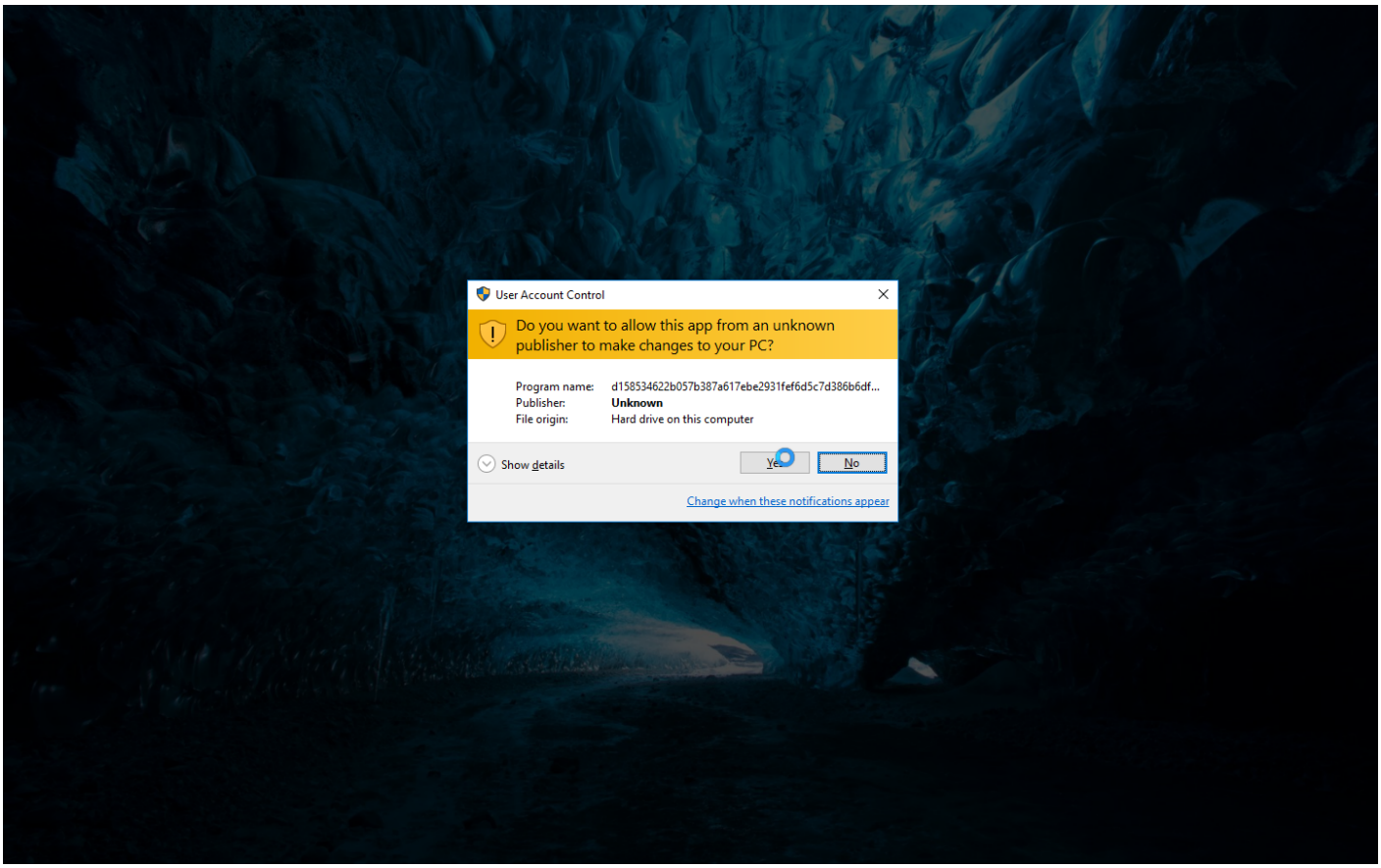
ID	#969367
MD5	1d46afb839b846ede01cb925470f0488
SHA1	8cffc99cda16d5d6b5192c62fefae6c0ac89b33d
SHA256	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1
SSDeep	24576:XHtrdKYVVSrqGDohJ3STZG8vIn/sCBGnWsY0Dy0:XHtV7GwBSTc8An/4YF0
ImpHash	b90027f65707ca9644c551e337fa02ad
File Name	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe
File Size	1215.26 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

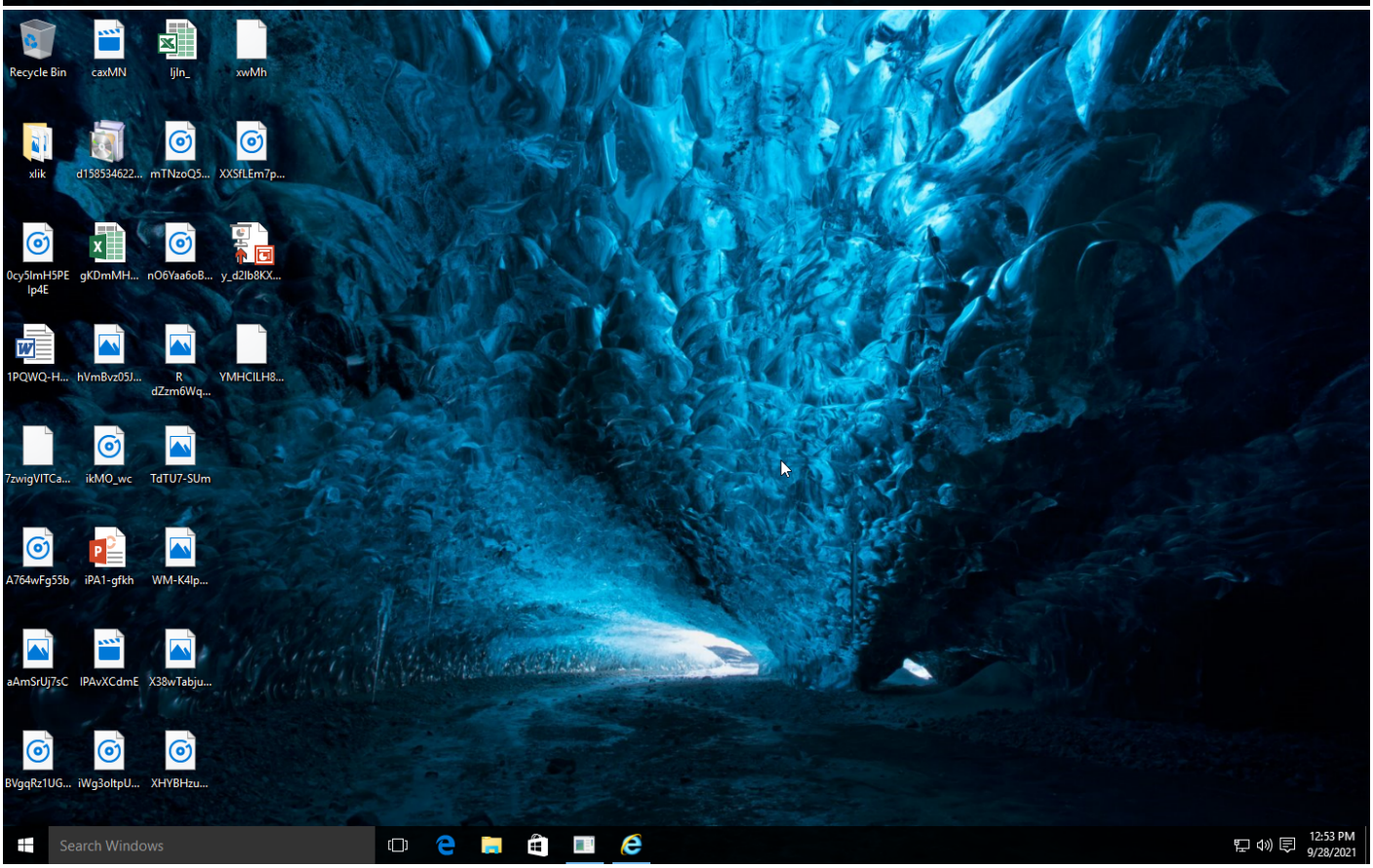
Analysis Information

Creation Time	2021-09-28 14:52 (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	5
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	1


Recycle Bin
caxMN
IjIn_
xwMh
xlik
d158534622...
mTNzoQ5...
XXSfLEm7p...
0cy5ImH5PE lp4E
gKDmMH...
nO6Yaa6oB...
y_d2Ib8KX...
1PQWQ-H...
hVmBvz05J...
R dZzm6Wq...
YMHCILH8...
7zwigVITCa...
ikMO_wc
TdTU7-SUm
A764wFg55b
iPA1-gfkh
WM-K4Ip...
aAmSrUj7sC
lPAvXCdmE
X38wTabju...
BVgqRz1UG...
iWg3oltpU...
XHYBHzu...
Search Windows
12:53 PM
9/28/2021


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: d158534622b057b387a617ebe2931fef6d5c7d386b6df...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

20.21 KB total sent

572.54 KB total received

2 ports 443, 49702

2 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

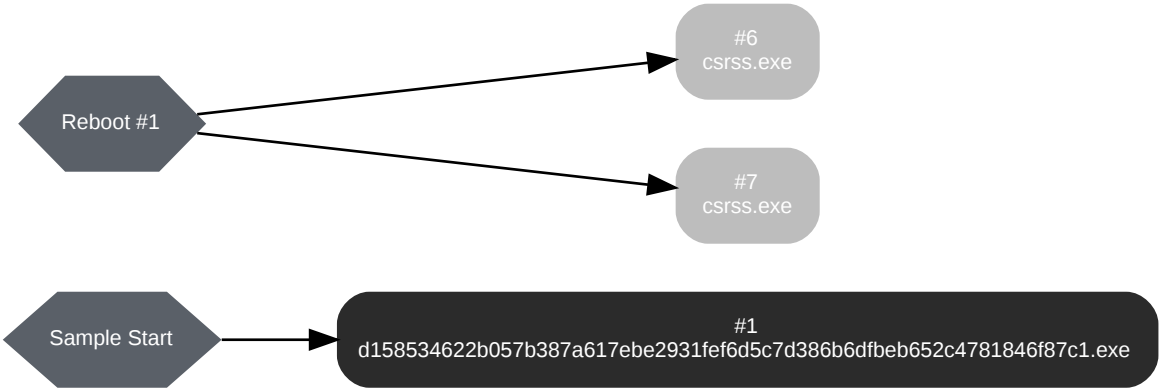
HTTP/S

0 URLs contacted, 1 servers

1 sessions, 20.21 KB sent, 572.54 KB received

BEHAVIOR

Process Graph



Process #1: d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 65946, Reason: Analysis Target
Unmonitor End Time	End Time: 159103, Reason: Terminated
Monitor duration	93.16s
Return Code	1073807364
PID	1664
Parent PID	1636
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\ProgramData\Windows\csrss.exe	1215.26 KB	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\lock	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\state.tmp	199 bytes	08254868a618fce4061ba6803e228bd9ecd53d37e4e0ba586184667db6db5cdb	✗

Host Behavior

Type	Count
Keyboard	1
Registry	192
Module	452
System	6084
File	376
Environment	1
COM	1
-	1
-	4
Process	128

Network Behavior

Type	Count
TCP	2

Process #6: csrss.exe

ID	6
File Name	c:\windows\system32\csrss.exe
Command Line	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 185392, Reason: Autostart
Unmonitor End Time	End Time: 305976, Reason: Terminated by Timeout
Monitor duration	120.58s
Return Code	Unknown
PID	372
Parent PID	364
Bitness	64 Bit

Process #7: csrss.exe

ID	7
File Name	c:\windows\system32\csrss.exe
Command Line	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 188587, Reason: Autostart
Unmonitor End Time	End Time: 305976, Reason: Terminated by Timeout
Monitor duration	117.39s
Return Code	Unknown
PID	460
Parent PID	440
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1	C:\ProgramData\Windows\csrss.exe, C:\Users\RDhJ0CNFevzX\Desktop\d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe, \\?\C:\Users\RDhJ0CNFevzX\Desktop\d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	Sample File	1215.26 KB	application/vnd.microsoft.portable-executable	Write, Read, Create, Access	MALICIOUS
08254868a618fce4061ba6803e228bd9ecd53d37e4e0ba586184667db6db5cdb	C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\state.tmp, C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\state	Dropped File	199 bytes	text/plain	Write, Create, Delete, Access	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	Sample File	Access	CLEAN
\\?\C:\ProgramData\System32\xmail	Accessed File	Access	CLEAN
\\?\C:\Users\RDhJ0CNFevzX\AppData\Roaming\System32\xmail	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5D897\	Accessed File	Create, Access	CLEAN
\\?\C:\ProgramData\System32\xVersion	Accessed File	Access	CLEAN
\\?\C:\Users\RDhJ0CNFevzX\AppData\Roaming\System32\xVersion	Accessed File	Access	CLEAN
C:\ProgramData\Windows\	Accessed File	Create, Access	CLEAN
\\?\C:\Users\RDhJ0CNFevzX\Desktop\d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	Sample File	Read, Access	CLEAN
C:\ProgramData\Windows\csrss.exe	Sample File	Write, Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\lock	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\state.tmp	Dropped File	Write, Create, Delete, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\state	Dropped File	Write, Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\router-stability	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\tor\geoip	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\tor\geoip6	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\cached-certs	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\cached-consensus	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\unverified-consensus	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\cached-microdesc-consensus	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\unverified-microdesc-consensus	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\cached-microdescs	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\cached-microdescs.new	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\cached-descriptors	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\6893A5~1\cached-extrainfo	Accessed File	Access	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
131.188.40.189	-	Germany	TCP, TLS	CLEAN
127.0.0.1	-	-	TCP	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CLASSES_ROOT\interface\{aa5b6a80-b834-11d0-932f-00a0c90dcaa9}	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\System32\Configuration\	create, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\System32\Configuration\	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\System32\Configuration\xi	write, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\System32\Configuration\xmail	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\System32\Configuration\xVersion	write, read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\ParentKeyName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\WindowsInstaller	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\ParentKeyName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\WindowsInstaller	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\ParentKeyName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\WindowsInstaller	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\ParentKeyName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\WindowsInstaller	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\ParentKeyName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\WindowsInstaller	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\ParentKeyName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\WindowsInstaller	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\ParentKeyName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\WindowsInstaller	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\ParentKeyName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\WindowsInstaller	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\ParentKeyName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\WindowsInstaller	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayName	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\SystemComponent	read, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\	access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\	create, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Client Server Runtime Subsystem	write, access	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	CLEAN

Process

Process Name	Commandline	Verdict
d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	"C:\Users\RDhJ0CNFevzX\Desktop\d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe"	MALICIOUS
csrss.exe	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Generic	CryptOne_Packer	Shellcode used by the CryptOne packer	Memory Dump	-	-	5/5

Antivirus (5)

File Type	Threat Name	File Name	Verdict
Sample File	Gen:Heur.Mint.Jamg.1	C:\Users\RDhJ0CNFevzX\Desktop\d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1.exe	MALICIOUS
Memory Dump	Generic.Mint.Zamg.3.3897D085	-	MALICIOUS
Memory Dump	Trojan.Ransom.Shade.E	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.1mLfX8U67Udc	-	MALICIOUS
Memory Dump	Trojan.Ransom.Shade.E	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

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

Platform Information

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

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-28 08:04:18+00:00
Built-in AV Database Records	10477558

Software Information

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

System Information

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

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