MALICIOUS

Classifications: -

Threat Names: Mal/HTMLGen-A | Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe**
ID	#4262891
MD5	310eb5bd45ac9c5767d28e63ab64635b
SHA1	4ac0d40abb71e9fcff34c8f67511fc590f495f3e
SHA256	d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6
File Size	1542.05 KB
Report Created	2022-05-05 06:28 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (31 rules, 214 matches)

Score	Category	Operation	Count	Classification
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Total Commander, Mozilla Thunderbird, Internet Explorer / Edge, k-Meleon, FileZilla, Opera, Comodo IceDragon, The Bat!, Mozilla Firefox, Cyberfox.			
4/5	Injection	Writes into the memory of another process	2	Injector
	• (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe modifies memory of (process #2) installutil.exe. • (Process #6) fname.exe modifies memory of (process #9) applaunch.exe.			
4/5	Injection	Modifies control flow of another process	2	-
	• (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe alters context of (process #2) installutil.exe. • (Process #6) fname.exe alters context of (process #9) applaunch.exe.			
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels embedded file "C:\Users\RDHJ0C~1\AppData\Local\Temp\fname.exe" as Mal/Generic-S. • Reputation analysis labels embedded file "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\filename.exe" as Mal/Generic-S.			
4/5	Reputation	Contacts known malicious URL	2	-
	• Reputation analysis labels the URL "http://45.9.20.31/asdasdasd.exe" which was contacted by (process #2) installutil.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "http://45.9.20.31/rigx.exe" which was contacted by (process #2) installutil.exe as Mal/HTMLGen-A.			
3/5	Data Collection	Reads memory of user process	62	-

- (Process #5) wmiprvse.exe reads memory of unmonitored process according.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process areaspaceanother.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process weight-employee.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process cellresource.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process firm_against_member.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process listen_art.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process animallikely.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process strategy-approach-thousand.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process responsibility.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process sea.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process kitchen_sea_answer.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process official.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process southern_who_police.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process administration somebody few.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process white_effort_certain.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process test_two.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process watch reveal.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process restratedegree.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process sign_he.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process 3dftp.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process absolutetelnet.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process alftp.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process barca.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process bitkinex.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process coreftp.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process far.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process filezilla.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process flashfxp.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process fling.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process gmailnotifierpro.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process icq.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process leechftp.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process ncftp.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process notepad.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process operamail.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process outlook.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process pidgin.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process scriptftp.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process skype.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process smartftp.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process thunderbird.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process trillian.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process webdrive.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process whatsapp.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process winscp.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process yahoomessenger.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process active-charge.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process accupos.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process afr38.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process foxmailincmail.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process ccv_server.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process utg2.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process spgagentservice.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process spcwin.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process omnipos.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process mxslipstream.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process isspos.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process fpos.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process edcsvr.exe.
- (Process #5) wmiprvse.exe reads memory of unmonitored process frdeservice.exe.

Score	Category	Operation	Count	Classification
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #2) installutil.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 #2) installutil.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 #2) installutil.exe tries to detect firewall via WMI query: "SELECT * FROM FirewallProduct".			
2/5	Anti Analysis	Tries to detect debugger	2	-
	• (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe tries to detect a debugger via API "CheckRemoteDebuggerPresent". • (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe tries to detect a debugger via API "IsDebuggerPresent".			
2/5	Anti Analysis	Tries to detect application sandbox	8	-
	• (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe tries to detect "Sandboxie" by checking for existence of module "SbieDll.dll". • (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe tries to detect "SunBelt Sandbox" by checking for existence of module "api_log.dll". • (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe tries to detect "SunBelt Sandbox" by checking for existence of module "dir_watch.dll". • (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe tries to detect "SunBelt Sandbox" by checking for existence of module "pstorec.dll". • (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe tries to detect "ThreatExpert" by checking for existence of module "dbghelp.dll". • (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe tries to detect "Comodo Sandbox" by checking for existence of module "cmdvrt32.dll". • (Process #6) fname.exe tries to detect "Comodo Sandbox" by checking for existence of module "cmdvrt32.dll". • (Process #6) fname.exe tries to detect "Sandboxie" by checking for existence of module "SbieDll.dll".			
2/5	Discovery	Executes WMI query	8	-
	• (Process #2) installutil.exe executes WMI query: SELECT * FROM Win32_DiskDrive. • (Process #2) installutil.exe executes WMI query: SELECT * FROM Win32_Process Where SessionId='1'. • (Process #2) installutil.exe executes WMI query: SELECT * FROM AntivirusProduct. • (Process #2) installutil.exe executes WMI query: SELECT * FROM AntiSpyWareProduct. • (Process #2) installutil.exe executes WMI query: SELECT * FROM FirewallProduct. • (Process #2) installutil.exe executes WMI query: SELECT * FROM Win32_Processor. • (Process #2) installutil.exe executes WMI query: SELECT * FROM Win32_VideoController. • (Process #2) installutil.exe executes WMI query: SELECT * FROM Win32_OperatingSystem.			
2/5	Discovery	Collects hardware properties	1	-
	• (Process #2) installutil.exe queries hardware properties via WMI.			
2/5	Data Collection	Reads sensitive ftp data	2	-
	• (Process #2) installutil.exe tries to read sensitive data of ftp application "Total Commander" by file. • (Process #2) installutil.exe tries to read sensitive data of ftp application "FileZilla" by file.			
2/5	Discovery	Enumerates running processes	2	-
	• (Process #2) installutil.exe enumerates running processes via WMI. • (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe enumerates running processes.			
2/5	Data Collection	Reads sensitive mail data	2	-
	• (Process #2) installutil.exe tries to read sensitive data of mail application "The Bat!" by file. • (Process #2) installutil.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file.			

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive browser data	6	-
	• (Process #2) installutil.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #2) installutil.exe tries to read sensitive data of web browser "Opera" by file. • (Process #2) installutil.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #2) installutil.exe tries to read sensitive data of web browser "k-Meleon" by file. • (Process #2) installutil.exe tries to read sensitive data of web browser "Comodo IceDragon" by file. • (Process #2) installutil.exe tries to read sensitive data of web browser "Cyberfox" by file.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #2) installutil.exe queries OS version via WMI.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #2) installutil.exe reads the network adapters' addresses by API.			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• (Process #6) fname.exe reads out system information, commonly used to detect "VirtualBox" via registry. (Key is "HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__").			
1/5	Anti Analysis	Tries to detect analyzer sandbox	1	-
	• (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe is possibly trying to detect analyzer sandbox by checking for patched sleep.			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe starts (process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe with a hidden window. • (Process #6) fname.exe starts (process #6) fname.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	88	-

- (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe reads from (process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe.
- (Process #5) wmiprvse.exe reads from winlogon.exe.
- (Process #5) wmiprvse.exe reads from lsass.exe.
- (Process #5) wmiprvse.exe reads from svchost.exe.
- (Process #5) wmiprvse.exe reads from dwm.exe.
- (Process #5) wmiprvse.exe reads from (process #3) svchost.exe.
- (Process #5) wmiprvse.exe reads from spoolsv.exe.
- (Process #5) wmiprvse.exe reads from sihost.exe.
- (Process #5) wmiprvse.exe reads from skypehost.exe.
- (Process #5) wmiprvse.exe reads from officeclicktorun.exe.
- (Process #5) wmiprvse.exe reads from explorer.exe.
- (Process #5) wmiprvse.exe reads from runtimebroker.exe.
- (Process #5) wmiprvse.exe reads from taskhostw.exe.
- (Process #5) wmiprvse.exe reads from shellexperiencehost.exe.
- (Process #5) wmiprvse.exe reads from searchui.exe.
- (Process #5) wmiprvse.exe reads from systemsettingsbroker.exe.
- (Process #5) wmiprvse.exe reads from wmiadap.exe.
- (Process #5) wmiprvse.exe reads from (process #4) wmiprvse.exe.
- (Process #5) wmiprvse.exe reads from iexplore.exe.
- (Process #5) wmiprvse.exe reads from according.exe.
- (Process #5) wmiprvse.exe reads from areaspaceanother.exe.
- (Process #5) wmiprvse.exe reads from weight-employee.exe.
- (Process #5) wmiprvse.exe reads from cellresource.exe.
- (Process #5) wmiprvse.exe reads from firm_against_member.exe.
- (Process #5) wmiprvse.exe reads from listen_art.exe.
- (Process #5) wmiprvse.exe reads from animallikely.exe.
- (Process #5) wmiprvse.exe reads from strategy-approach-thousand.exe.
- (Process #5) wmiprvse.exe reads from responsibility.exe.
- (Process #5) wmiprvse.exe reads from sea.exe.
- (Process #5) wmiprvse.exe reads from kitchen_sea_answer.exe.
- (Process #5) wmiprvse.exe reads from official.exe.
- (Process #5) wmiprvse.exe reads from southern_who_police.exe.
- (Process #5) wmiprvse.exe reads from administration somebody few.exe.
- (Process #5) wmiprvse.exe reads from white_effort_certain.exe.
- (Process #5) wmiprvse.exe reads from test_two.exe.
- (Process #5) wmiprvse.exe reads from watch reveal.exe.
- (Process #5) wmiprvse.exe reads from restratedegree.exe.
- (Process #5) wmiprvse.exe reads from sign_he.exe.
- (Process #5) wmiprvse.exe reads from 3dftp.exe.
- (Process #5) wmiprvse.exe reads from absolutetelnet.exe.
- (Process #5) wmiprvse.exe reads from alftp.exe.
- (Process #5) wmiprvse.exe reads from barca.exe.
- (Process #5) wmiprvse.exe reads from bitkinex.exe.
- (Process #5) wmiprvse.exe reads from coreftp.exe.
- (Process #5) wmiprvse.exe reads from far.exe.
- (Process #5) wmiprvse.exe reads from filezilla.exe.
- (Process #5) wmiprvse.exe reads from flashfxp.exe.
- (Process #5) wmiprvse.exe reads from fling.exe.
- (Process #5) wmiprvse.exe reads from gmailnotifierpro.exe.
- (Process #5) wmiprvse.exe reads from icq.exe.
- (Process #5) wmiprvse.exe reads from leechftp.exe.
- (Process #5) wmiprvse.exe reads from ncftp.exe.
- (Process #5) wmiprvse.exe reads from notepad.exe.
- (Process #5) wmiprvse.exe reads from operamail.exe.
- (Process #5) wmiprvse.exe reads from outlook.exe.
- (Process #5) wmiprvse.exe reads from pidgin.exe.
- (Process #5) wmiprvse.exe reads from scriptftp.exe.
- (Process #5) wmiprvse.exe reads from skype.exe.
- (Process #5) wmiprvse.exe reads from smartftp.exe.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Creates a page with write and execute permissions	2	-
	• (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READWRITE"). • (Process #6) fname.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.		
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #2) installutil.exe tries to gather information about application "FileZilla" by file. • (Process #2) installutil.exe tries to gather information about application "Steam" by registry.			
1/5	Privilege Escalation	Enables process privilege	2	-
	• (Process #2) installutil.exe enables process privilege "SeDebugPrivilege". • (Process #5) wmiprvse.exe enables process privilege "SeDebugPrivilege".			
1/5	Network Connection	Connects to remote host	2	-
	• (Process #2) installutil.exe opens an outgoing TCP connection to host "45.9.20.31:80". • (Process #2) installutil.exe opens an outgoing TCP connection to host "65.21.213.209:32936".			
1/5	Network Connection	Downloads executable	2	Downloader
	• (Process #2) installutil.exe downloads executable via http from http://45.9.20.31/rigx.exe. • (Process #2) installutil.exe downloads executable via http from http://45.9.20.31/asdasdasd.exe.			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #2) installutil.exe tries to connect to TCP port 32936 at 65.21.213.209.			
1/5	Obfuscation	Obfuscates control flow	1	-
	• Modifies exception handler (e.g., the instruction pointer is modified within an exception handler filter).			
1/5	Obfuscation	Resolves API functions dynamically	3	-
	• (Process #1) d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe resolves 110 API functions by name. • (Process #2) installutil.exe resolves 52 API functions by name. • (Process #6) fname.exe resolves 30 API functions by name.			

Mitre ATT&CK Matrix

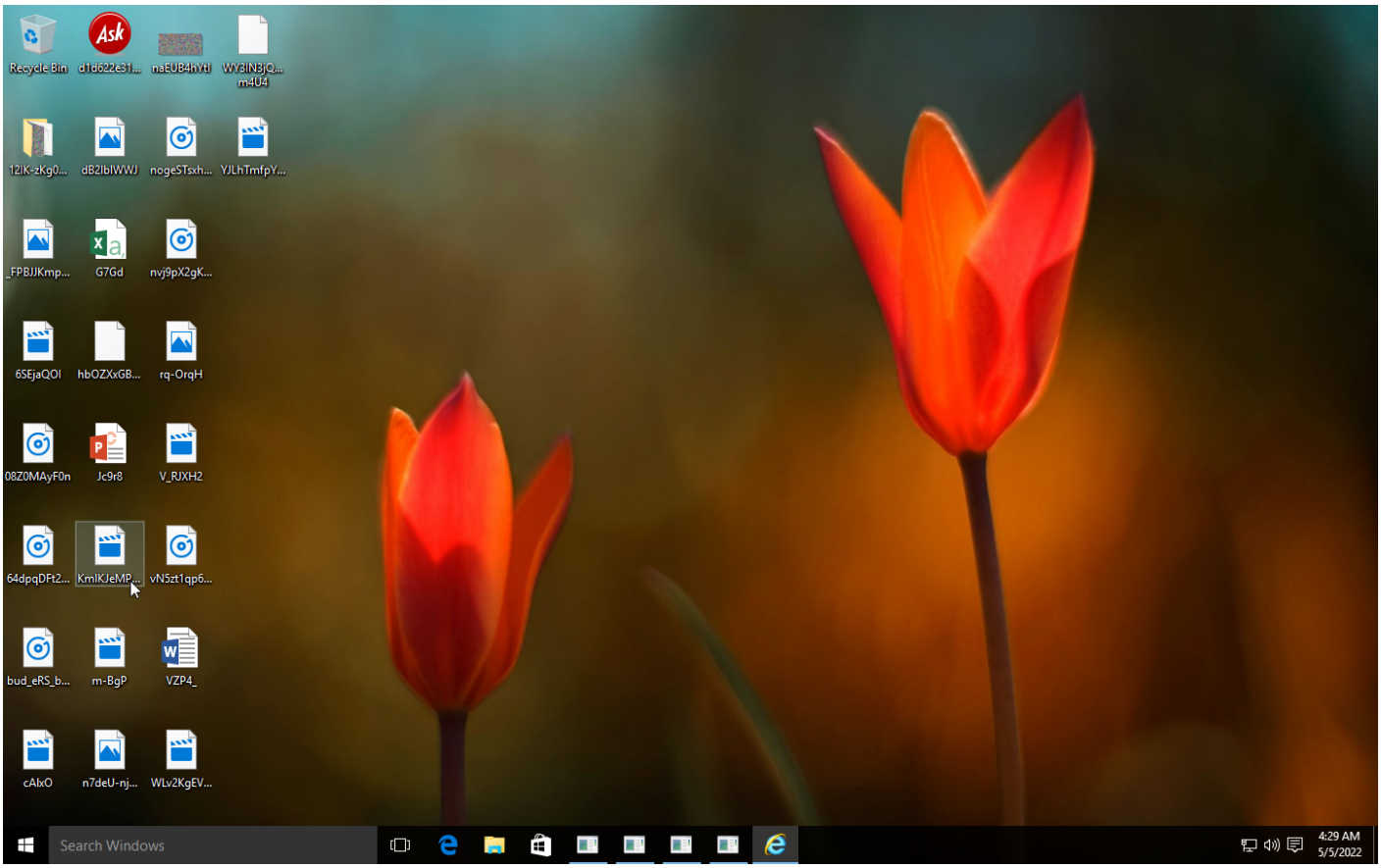
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1497 Virtualization/ Sandbox Evasion	#T1081 Credentials in Files	#T1497 Virtualization/ Sandbox Evasion	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol		
				#T1143 Hidden Window		#T1057 Process Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
				#T1045 Software Packing		#T1124 System Time Discovery			#T1065 Uncommonly Used Port		
				#T1027 Obfuscated Files or Information		#T1082 System Information Discovery					
						#T1083 File and Directory Discovery					
						#T1063 Security Software Discovery					
						#T1012 Query Registry					
						#T1016 System Network Configuration Discovery					

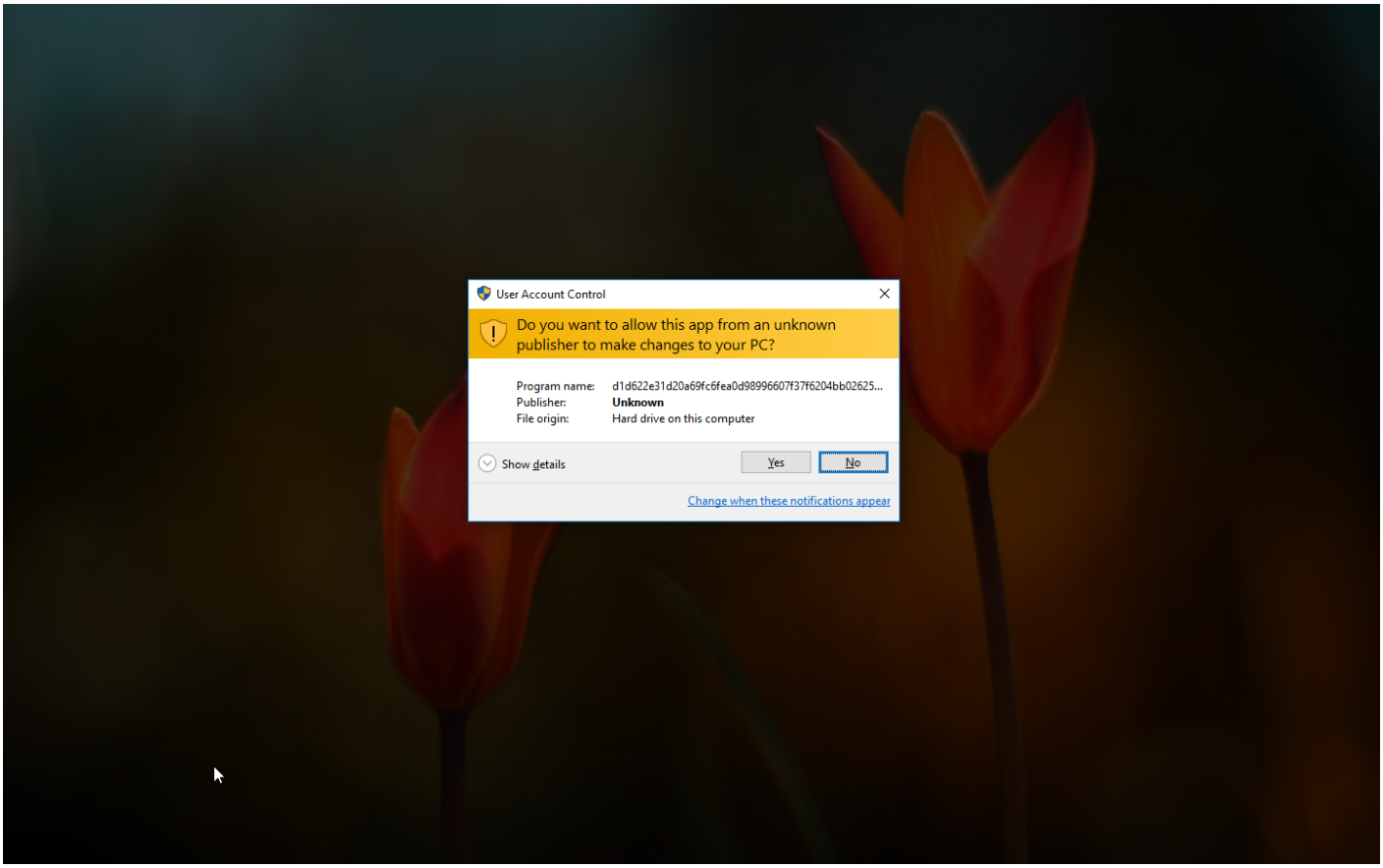
Sample Information

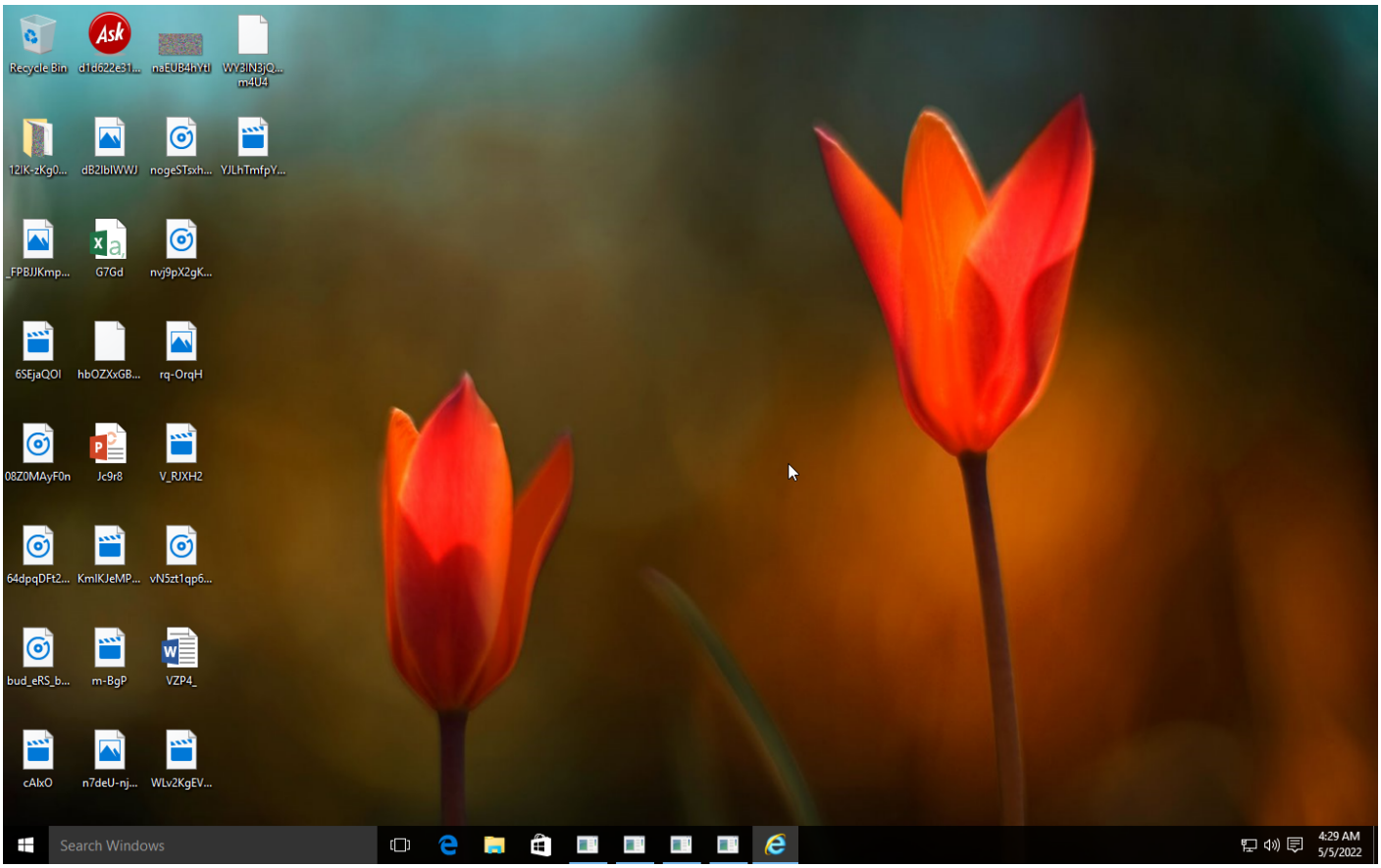
ID	#4262891
MD5	310eb5bd45ac9c5767d28e63ab64635b
SHA1	4ac0d40abb71e9fcff34c8f67511fc590f495f3e
SHA256	d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6
SSDeep	24576:07L4j8tb74F0xt7ruJV/QujUOycEvgyJrDybsxXX+ZVGNVooHI9s5KCfj2:07L4jIlct7w/QujMvOgUwLoKIG2
ImpHash	efad26290bf4d1a676b7ad79139e8cdb
File Name	d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe
File Size	1542.05 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

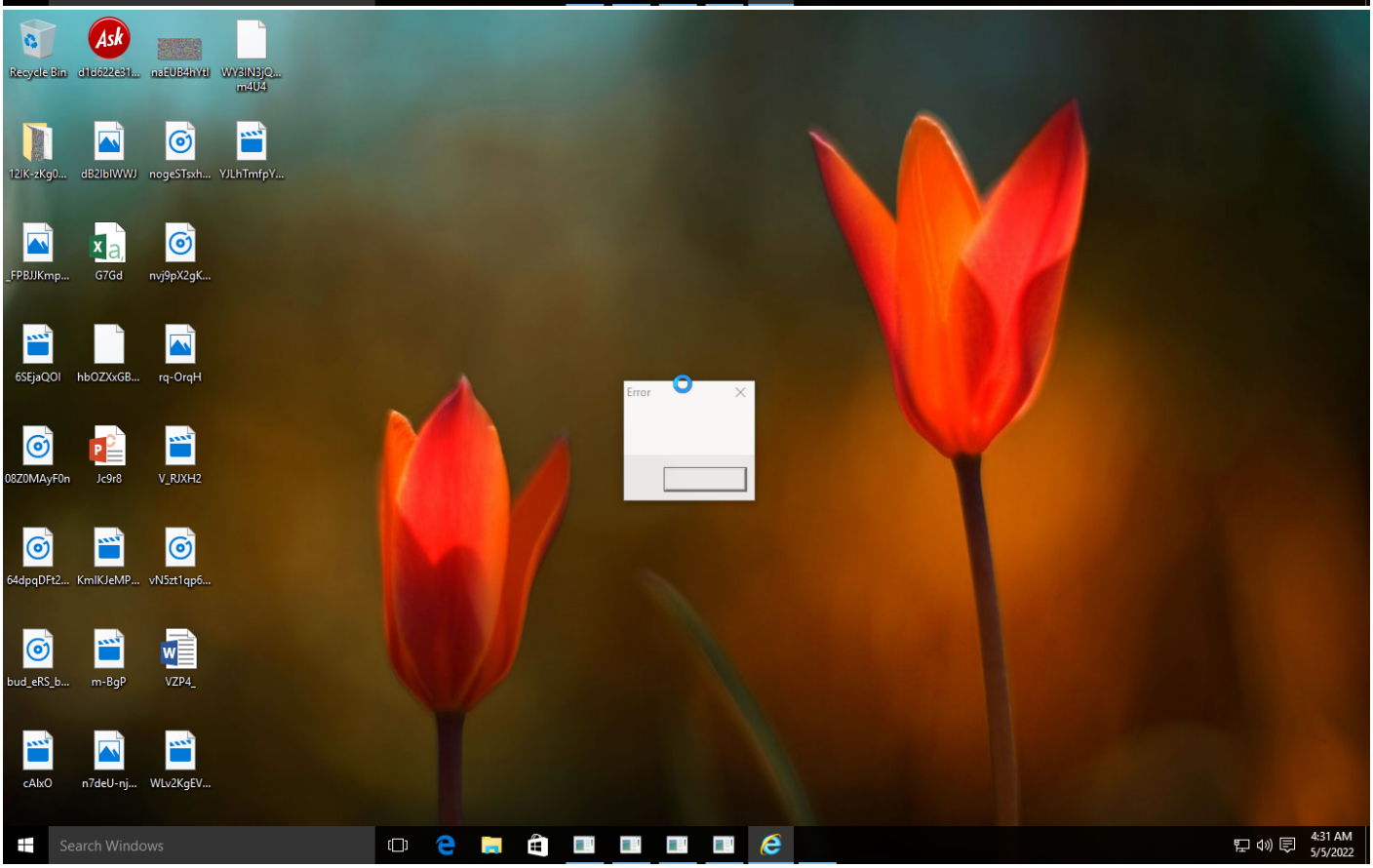
Analysis Information

Creation Time	2022-05-05 06:28 (UTC+2)
Analysis Duration	00:03:55
Termination Reason	Timeout
Number of Monitored Processes	7
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	0


Recycle Bin
d1d622e31...
naEUB4hYtl
WY3INBjQ...
m4U4
12iK-zKg0...
dB2lbIWWJ
nogeSTsxh...
YJLhTmfpY...
_FPBJJKmp...
G7Gd
nvj9pX2gK...
6SEjaQOI
hbOZXxGB...
rq-OrqH
08Z0MAyF0n
Jc9r8
V_RJXH2
64dpqDFt2...
KmlKJeMP...
vN5zt1qp6...
bud_eRS_b...
m-BgP
VZP4_
cAlxO
n7deU-nj...
WLv2KgEV...
Search Windows
4:29 AM
5/5/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: d1d622e31d20a69fc6fea0d98996607f37f6204bb02625...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

1575.69 KB total sent

8598.66 KB total received

2 ports 80, 32936

2 contacted IP addresses

1 URLs extracted

2 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 1 servers

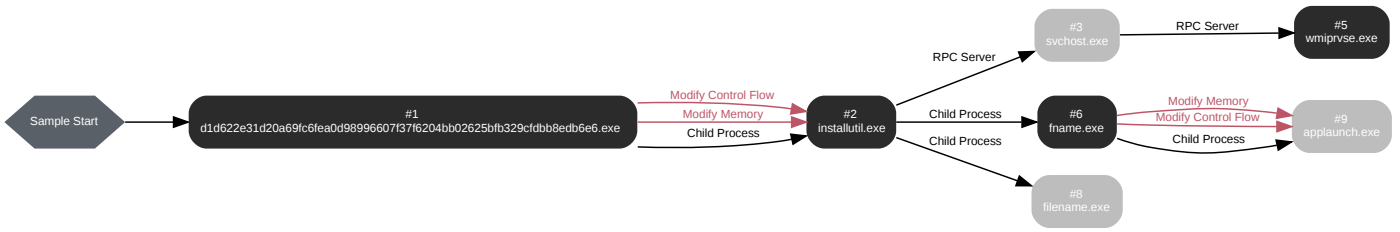
1 sessions, 50.64 KB sent, 17172.59 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://45.9.20.31/rigx.exe	-	-		0 bytes	NA
GET	http://45.9.20.31/asdasdasd.exe	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 87465, Reason: Analysis Target
Unmonitor End Time	End Time: 215073, Reason: Terminated
Monitor duration	127.61s
Return Code	1702172
PID	2908
Parent PID	1932
Bitness	32 Bit

Host Behavior

Type	Count
System	40
Process	256
Module	148
File	6
-	2
Environment	3
-	5
-	2
User	1

Process #2: installutil.exe

ID	2
File Name	c:\windows\microsoft.net\framework\v4.0.30319\installutil.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 204676, Reason: Child Process
Unmonitor End Time	End Time: 319558, Reason: Terminated
Monitor duration	114.88s
Return Code	0
PID	2504
Parent PID	2908
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe	0x1200	0x400000(4194304)	0x20000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe	0x1200	0x374008(3620872)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe	0x1200 / 0xafc	0x778a8fe0(2005569504)	-	✔	1

Host Behavior

Type	Count
Module	70
File	475
Registry	255
COM	121
-	13
System	202
-	11
Process	2
Environment	5
User	3
Keyboard	3
Window	2

Network Behavior

Type	Count
HTTP	2
TCP	2

Process #3: svchost.exe

ID	3
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: 257189, Reason: RPC Server
Unmonitor End Time	End Time: 322572, Reason: Terminated by timeout
Monitor duration	65.38s
Return Code	Unknown
PID	868
Parent PID	2504
Bitness	64 Bit

Process #5: wmiprvse.exe

ID	5
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: 257189, Reason: RPC Server
Unmonitor End Time	End Time: 322572, Reason: Terminated by timeout
Monitor duration	65.38s
Return Code	Unknown
PID	3608
Parent PID	868
Bitness	64 Bit

Host Behavior

Type	Count
Process	407
-	691
System	120
Module	16
User	1
Registry	2

Process #6: fname.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\fname.exe
Command Line	"C:\Users\RDHJ0C~1\AppData\Local\Temp\fname.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\
Monitor Start Time	Start Time: 292078, Reason: Child Process
Unmonitor End Time	End Time: 316738, Reason: Terminated
Monitor duration	24.66s
Return Code	0
PID	3988
Parent PID	2504
Bitness	32 Bit

Host Behavior

Type	Count
Window	400
File	54
Module	62
-	9
Registry	9
-	3
Process	1
Environment	1
System	3

Process #8: filename.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\filename.exe
Command Line	"C:\Users\RDHJ0C~1\AppData\Local\Temp\filename.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\
Monitor Start Time	Start Time: 308345, Reason: Child Process
Unmonitor End Time	End Time: 322572, Reason: Terminated by timeout
Monitor duration	14.23s
Return Code	Unknown
PID	4972
Parent PID	2504
Bitness	64 Bit

Process #9: applaunch.exe

ID	9
File Name	c:\windows\microsoft.net\framework\v4.0.30319\applaunch.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\
Monitor Start Time	Start Time: 310192, Reason: Child Process
Unmonitor End Time	End Time: 322572, Reason: Terminated by timeout
Monitor duration	12.38s
Return Code	Unknown
PID	952
Parent PID	3988
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\fname.exe	0xbe0	0x1d0000(1900544)	0x22000	✔	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\fname.exe	0xbe0	0x4f2008(5185544)	0x4	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\fname.exe	0xbe0 / 0x594	0x778a8fe0(2005569504)	-	✔	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
84a5a26f1748c3ad1f0b98c438908e8dc842eacc6390484527ee1fe7e56264f5	C:\Users\RDHJ0C~1\AppData\Local\Temp\fname.exe, C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\fname.exe	Accessed File	3591.40 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
f9bff1ac8e6c15dde928e87a8bf733006ca805d42302387b2c24e11e555b7ee6	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\filename.exe	Accessed File	4765.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6	C:\Users\RDhJ0CNFevzX\Desktop\d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe	Sample File	1542.05 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	-	Modified File	128 bytes	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\sitemanager.xml	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\fname.exe	Downloaded File, Accessed File, Extracted File	Access, Create, Write	CLEAN
C:\Program Files\Internet Explorer\iexplore.exe	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\NordVPN	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YaAddon	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\filename.exe	Accessed File, Downloaded File, Extracted File	Access, Create, Write	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.Config	Accessed File	Access, Read	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://45.9.20.31/asdasdasd.exe	-	45.9.20.31	-	GET	MALICIOUS
http://45.9.20.31/rigx.exe	-	45.9.20.31	-	GET	MALICIOUS
http://7tr0l4pn2f71dc3wylh5klcnxk6uis.yhnog6p59mruwnpfi4zy	-	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
45.9.20.31	-	Russia	TCP, HTTP	CLEAN
65.21.213.209	-	Finland	TCP	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	access, read	fname.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Net Framework Setup\NDP\v4\Client	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Valve\Steam	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	installutil.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Clients\StartMenuInternet	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\Hardware\description\System\VideoBiosVersion	access, read	fname.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Clients\StartMenuInternet\IEXPLORE.EXE\shell\open\command	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063	access	installutil.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000\DriverDesc	access, read	fname.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\Hardware\description\System\SystemBiosVersion	access, read	fname.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Net Framework Setup\NDP\v4\Client\InstallPath	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	access, read	installutil.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	access	fname.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CSDVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	access, read	installutil.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000	access	fname.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Clients\StartMenuInternet\IEXPLORE.EXE	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	access, read	installutil.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayVersion	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\Hardware\description\System	access	fname.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe	"C:\Users\RDhJ0CNFevzX\Desktop\d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6.exe"	MALICIOUS
fname.exe	"C:\Users\RDHJ0C~1\AppData\Local\Temp\fname.exe"	MALICIOUS
installutil.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe"	SUSPICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
filename.exe	"C:\Users\RDHJ0C~1\AppData\Local\Temp\filename.exe"	CLEAN
applaunch.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe"	CLEAN

YARA / AV

No YARA or AV matches available.

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	4.5.0
Dynamic Engine Version	4.5.0 / 04/22/2022 19:04
Static Engine Version	4.5.0.0 / 2022-04-22 17:45:13
AV Exceptions Version	4.5.0.2 / 2022-04-03 15:57:54
Link Detonation Heuristics Version	4.5.0.19 / 2022-04-20 05:46:11
Smart Memory Dumping Rules Version	4.5.0.2 / 2022-04-03 15:57:54
Config Extractors Version	4.5.0.14 / 2022-04-07 17:00:08
Signature Trust Store Version	4.5.0.2 / 2022-04-03 15:57:54
VMRay Threat Identifiers Version	4.5.0.24 / 2022-04-26 09:10:00
YARA Built-in Ruleset Version	4.5.0.2

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