MALICIOUS

Classifications: Downloader | Injector | Spyware

Threat Names: SmokeLoader | Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**d609a21245d77dccd6d4a659cbd9466a.virus.exe**
ID	#3266311
MD5	d609a21245d77dccd6d4a659cbd9466a
SHA1	a8775ccb1d6b7b941e5b37d59db5d25f4b736cf9
SHA256	a0f70f88c9a376e7c0f7e508c796bf1dbbf58ff8b172b9aff3421be63e2d7f78
File Size	278.00 KB
Report Created	2022-01-11 19:49 (UTC+1)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (41 rules, 108 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	3	Downloader
	• Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #2) d609a21245d77dccd6d4a659cbd9466a.virus.exe. • Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #3) explorer.exe. • Rule "SmokeLoaderStrings" from ruleset "Malware" has matched on the function strings for (process #3) explorer.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: The Bat!, FileZilla, Mozilla Thunderbird, Cyberfox, Exodus Cryptocurrency Wallet, Total Commander, Comodo IceDragon, Windows Mail, Mozilla Firefox, k-Meleon, Opera, Electrum Bitcoin Wallet, Internet Explorer / Edge.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #3) explorer.exe tries to delete zone identifier of file "C:\Users\kEecfMwgj\AppData\Roaming\cdieedr".			
4/5	Reputation	Contacts known malicious URL	3	-
	• Reputation analysis labels the URL "host-data-coin-11.com/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "data-host-coin-8.com/files/9718_1641769402_1919.exe" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "https://cdn.discordapp.com/attachments/917178535238586432/922560115226312704/StopScam.vmp.exe" which was contacted by (process #8) applaunch.exe as "Mal/HTMLGen-A".			
4/5	Reputation	Resolves known malicious domain	1	-
	• Reputation analysis labels the resolved domain "yabynennet.xyz" as "Mal/HTMLGen-A".			
4/5	Injection	Writes into the memory of another process	3	Injector
	• (Process #2) d609a21245d77dccd6d4a659cbd9466a.virus.exe modifies memory of (process #3) explorer.exe. • (Process #7) 52b4.exe modifies memory of (process #8) applaunch.exe. • (Process #12) 69be.exe modifies memory of (process #13) applaunch.exe.			
4/5	Injection	Modifies control flow of another process	3	-
	• (Process #7) 52b4.exe alters context of (process #8) applaunch.exe. • (Process #12) 69be.exe alters context of (process #13) applaunch.exe. • (Process #2) d609a21245d77dccd6d4a659cbd9466a.virus.exe creates thread in (process #3) explorer.exe.			
3/5	Data Collection	Reads cryptocurrency wallet locations	4	-
	• (Process #8) applaunch.exe tries to read the cryptocurrency wallet "Electrum Bitcoin Wallet" for "BTC". • (Process #8) applaunch.exe tries to read the cryptocurrency wallet "Exodus Cryptocurrency Wallet". • (Process #13) applaunch.exe tries to read the cryptocurrency wallet "Electrum Bitcoin Wallet" for "BTC". • (Process #13) applaunch.exe tries to read the cryptocurrency wallet "Exodus Cryptocurrency Wallet".			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #8) applaunch.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 #8) applaunch.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	-

Score	Category	Operation	Count	Classification
	• (Process #8) applaunch.exe tries to detect firewall via WMI query: "SELECT * FROM FirewallProduct".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #2) d609a21245d77dccd6d4a659cbd9466a.virus.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Hide Tracks	Deletes file after execution	2	-
	• (Process #3) explorer.exe deletes executed executable "c:\users\keecfmwgj\appdata\roaming\cdieedr". • (Process #3) explorer.exe deletes executed executable "c:\users\keecfmwgj\desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe".			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #3) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Discovery	Reads network adapter information	2	-
	• (Process #8) applaunch.exe reads the network adapters' addresses by API. • (Process #13) applaunch.exe reads the network adapters' addresses by API.			
2/5	Discovery	Executes WMI query	10	-
	• (Process #8) applaunch.exe executes WMI query: SELECT * FROM Win32_DiskDrive. • (Process #8) applaunch.exe executes WMI query: SELECT * FROM Win32_Process Where SessionId='1'. • (Process #8) applaunch.exe executes WMI query: SELECT * FROM Win32_Processor. • (Process #8) applaunch.exe executes WMI query: SELECT * FROM Win32_VideoController. • (Process #8) applaunch.exe executes WMI query: SELECT * FROM Win32_OperatingSystem. • (Process #8) applaunch.exe executes WMI query: SELECT * FROM AntivirusProduct. • (Process #8) applaunch.exe executes WMI query: SELECT * FROM AntiSpyWareProduct. • (Process #8) applaunch.exe executes WMI query: SELECT * FROM FirewallProduct. • (Process #13) applaunch.exe executes WMI query: SELECT * FROM Win32_DiskDrive. • (Process #13) applaunch.exe executes WMI query: SELECT * FROM Win32_Process Where SessionId='1'.			
2/5	Discovery	Collects hardware properties	2	-
	• (Process #8) applaunch.exe queries hardware properties via WMI. • (Process #13) applaunch.exe queries hardware properties via WMI.			
2/5	Data Collection	Reads sensitive mail data	6	-
	• (Process #8) applaunch.exe tries to read sensitive data of mail application "The Bat!" by file. • (Process #8) applaunch.exe tries to read sensitive data of mail application "Windows Mail" by file. • (Process #8) applaunch.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file. • (Process #13) applaunch.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file. • (Process #13) applaunch.exe tries to read sensitive data of mail application "The Bat!" by file. • (Process #13) applaunch.exe tries to read sensitive data of mail application "Windows Mail" by file.			
2/5	Data Collection	Reads sensitive browser data	12	-

Score	Category	Operation	Count	Classification
	• (Process #8) applaunch.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #8) applaunch.exe tries to read sensitive data of web browser "Opera" by file. • (Process #8) applaunch.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #8) applaunch.exe tries to read sensitive data of web browser "k-Meleon" by file. • (Process #8) applaunch.exe tries to read sensitive data of web browser "Comodo IceDragon" by file. • (Process #8) applaunch.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #13) applaunch.exe tries to read sensitive data of web browser "Opera" by file. • (Process #13) applaunch.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #13) applaunch.exe tries to read sensitive data of web browser "k-Meleon" by file. • (Process #13) applaunch.exe tries to read sensitive data of web browser "Comodo IceDragon" by file. • (Process #13) applaunch.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #13) applaunch.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.		
2/5	Discovery	Enumerates running processes	3	-
	• (Process #8) applaunch.exe enumerates running processes via WMI. • (Process #13) applaunch.exe enumerates running processes via WMI. • (Process #3) explorer.exe enumerates running processes.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #8) applaunch.exe queries OS version via WMI.			
2/5	Data Collection	Reads sensitive ftp data	3	-
	• (Process #8) applaunch.exe tries to read sensitive data of ftp application "Total Commander" by file. • (Process #8) applaunch.exe tries to read sensitive data of ftp application "FileZilla" by file. • (Process #13) applaunch.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• Multiple processes are possibly trying to detect a VM via rdtsc.			
2/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\cdieedr", to be triggered by Logon. • Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\cdieedr", to be triggered by Time. Task has been rescheduled by the analyzer.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	2	-
	• (Process #7) 52b4.exe makes a direct system call to "NtProtectVirtualMemory". • (Process #12) 69be.exe makes a direct system call to "NtProtectVirtualMemory".			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) d609a21245d77dccd6d4a659cbd9466a.virus.exe modifies memory of (process #2) d609a21245d77dccd6d4a659cbd9466a.virus.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) d609a21245d77dccd6d4a659cbd9466a.virus.exe alters context of (process #2) d609a21245d77dccd6d4a659cbd9466a.virus.exe.			
2/5	Heuristics	Signed executable failed signature validation	1	-
	• C:\Users\KEECFM~1\AppData\Local\Temp\52B4.exe is signed, but signature validation failed.			
1/5	Obfuscation	Reads from memory of another process	3	-

Score	Category	Operation	Count	Classification
	• (Process #1) d609a21245d77dccd6d4a659cbd9466a.virus.exe reads from (process #2) d609a21245d77dccd6d4a659cbd9466a.virus.exe. • (Process #7) 52b4.exe reads from (process #8) applaunch.exe. • (Process #12) 69be.exe reads from (process #13) applaunch.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	3	-
	• (Process #1) d609a21245d77dccd6d4a659cbd9466a.virus.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #7) 52b4.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #12) 69be.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Mutex	Creates mutex	1	-
	• (Process #3) explorer.exe creates mutex with name "4BCD659AD8F347B5B451918CD891C8238443A5AF".			
1/5	Hide Tracks	Creates process with hidden window	4	-
	• (Process #3) explorer.exe starts (process #7) 52b4.exe with a hidden window. • (Process #7) 52b4.exe starts (process #8) applaunch.exe with a hidden window. • (Process #3) explorer.exe starts (process #12) 69be.exe with a hidden window. • (Process #12) 69be.exe starts (process #13) applaunch.exe with a hidden window.			
1/5	Privilege Escalation	Enables process privilege	2	-
	• (Process #8) applaunch.exe enables process privilege "SeDebugPrivilege". • (Process #13) applaunch.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #8) applaunch.exe tries to gather information about application "FileZilla" by file. • (Process #8) applaunch.exe tries to gather information about application "Steam" by registry.			
1/5	Obfuscation	Resolves API functions dynamically	4	-
	• (Process #1) d609a21245d77dccd6d4a659cbd9466a.virus.exe resolves 41 API functions by name. • (Process #7) 52b4.exe resolves 249 API functions by name. • (Process #8) applaunch.exe resolves 51 API functions by name. • (Process #12) 69be.exe resolves 249 API functions by name.			
1/5	Obfuscation	The binary file was created with a packer	1	-
	• File "C:\Users\KEECFM~1\AppData\Local\Temp\52B4.exe" is packed with "ASProtect v1.23 RC1".			
1/5	Execution	Executes itself	2	-
	• (Process #1) d609a21245d77dccd6d4a659cbd9466a.virus.exe executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe. • (Process #4) taskeng.exe executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe.			
1/5	Network Connection	Performs DNS request	5	-
	• (Process #8) applaunch.exe resolves host name "yabynennet.xyz" to IP "185.82.202.246". • (Process #8) applaunch.exe resolves host name "api.ip.sb" to IP "104.26.13.31". • (Process #8) applaunch.exe resolves host name "cdn.discordapp.com" to IP "162.159.129.233". • (Process #13) applaunch.exe resolves host name "yabynennet.xyz" to IP "185.82.202.246". • (Process #13) applaunch.exe resolves host name "api.ip.sb" to IP "104.26.13.31".			
1/5	Network Connection	Connects to remote host	5	-

Score	Category	Operation	Count	Classification
	• (Process #8) applaunch.exe opens an outgoing TCP connection to host "162.159.129.233:443". • (Process #8) applaunch.exe opens an outgoing TCP connection to host "185.82.202.246:81". • (Process #8) applaunch.exe opens an outgoing TCP connection to host "104.26.13.31:443". • (Process #13) applaunch.exe opens an outgoing TCP connection to host "104.26.13.31:443". • (Process #13) applaunch.exe opens an outgoing TCP connection to host "185.82.202.246:81".			
1/5	Network Connection	Downloads executable	1	Downloader
	• (Process #3) explorer.exe downloads executable via http from data-host-coin-8.com/files/9718_1641769402_1919.exe.			
1/5	Network Connection	Tries to connect using an uncommon port	2	-
	• (Process #8) applaunch.exe tries to connect to TCP port 81 at 185.82.202.246. • (Process #13) applaunch.exe tries to connect to TCP port 81 at 185.82.202.246.			

Mitre ATT&CK Matrix

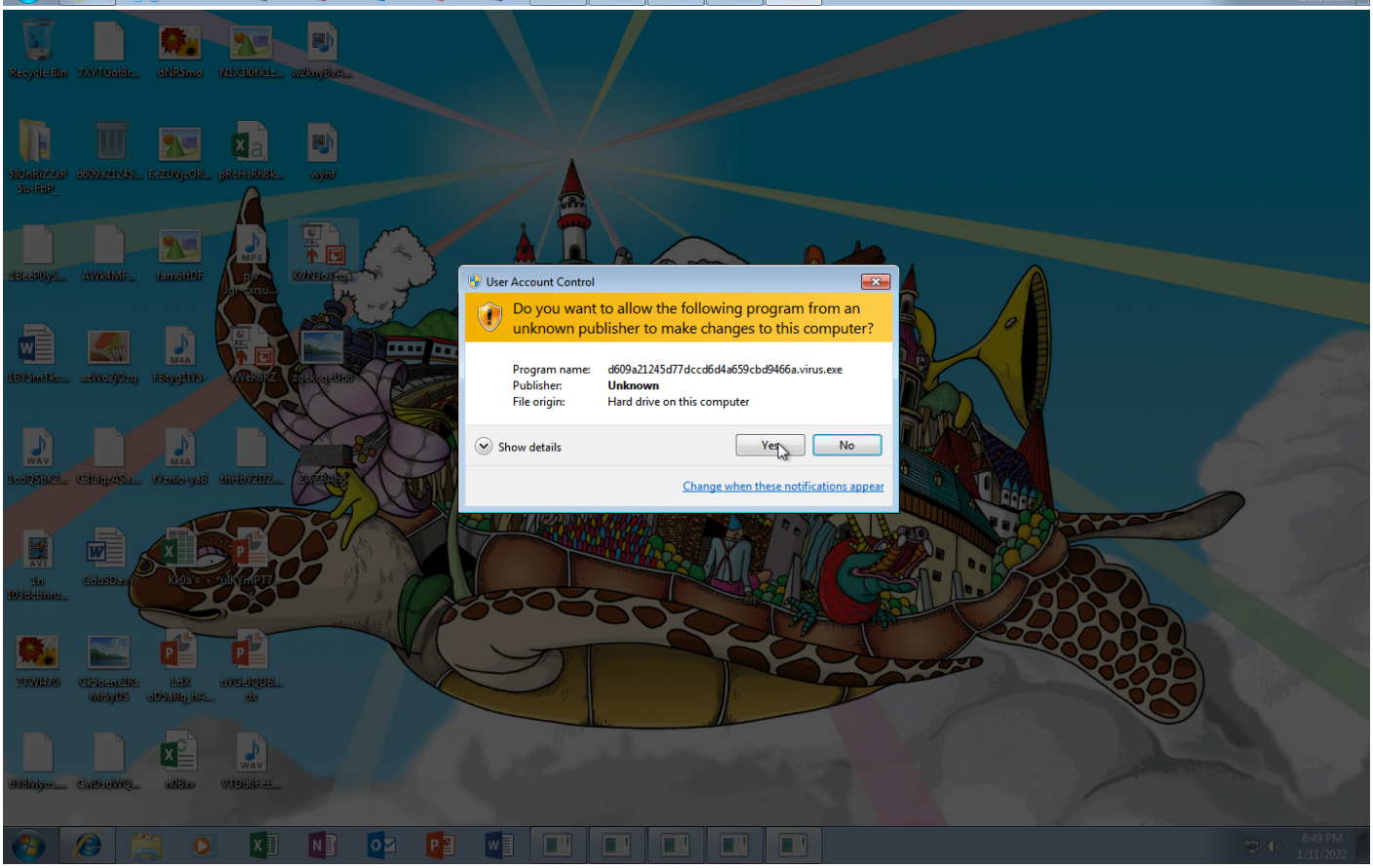
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1045 Software Packing	#T1081 Credentials in Files	#T1057 Process Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol		
	#T1053 Scheduled Task			#T1096 NTFS File Attributes		#T1016 System Network Configuration Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
				#T1143 Hidden Window		#T1082 System Information Discovery			#T1065 Uncommonly Used Port		
				#T1497 Virtualization/ Sandbox Evasion		#T1083 File and Directory Discovery					
				#T1027 Obfuscated Files or Information		#T1012 Query Registry					
						#T1063 Security Software Discovery					
						#T1497 Virtualization/ Sandbox Evasion					
						#T1124 System Time Discovery					

Sample Information

ID	#3266311
MD5	d609a21245d77dccd6d4a659cbd9466a
SHA1	a8775ccb1d6b7b941e5b37d59db5d25f4b736cf9
SHA256	a0f70f88c9a376e7c0f7e508c796bf1dbbf58ff8b172b9aff3421be63e2d7f78
SSDeep	3072:WulvZ9KEbLnAALxvRs7uCoorI90O3manWxULkIFueWrxpzbgqru:WrPKOnvA7ulrUJY0kIFueuzbgwu
ImpHash	6aeb06b4ccc41eb437631c770949cf13
File Name	d609a21245d77dccd6d4a659cbd9466a.virus.exe
File Size	278.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-01-11 19:49 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	9
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	3


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: d609a21245d77dccd6d4a659cbd9466a.virus.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

Screenshots truncated

NETWORK

General

4426.55 KB total sent

7361.58 KB total received

3 ports 80, 81, 443

5 contacted IP addresses

0 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

7 DNS requests for 3 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

4 URLs contacted, 3 servers

12 sessions, 8.80 KB sent, 7335.33 KB received

HTTP Requests

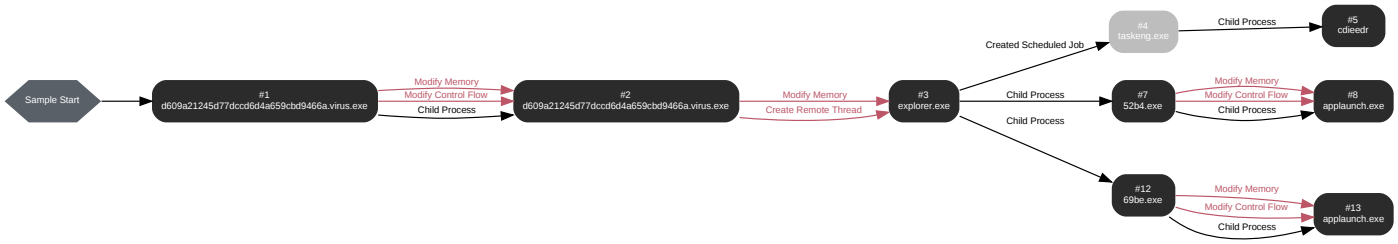
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	host-data-coin-11.com/	-	-		0 bytes	NA
GET	data-host-coin-8.com/files/9718_1641769402_1919.exe	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/917178535238586432/922560115226312704/StopScam.vmp.exe	-	-		0 bytes	NA
GET	https://api.ip.sb/ip	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	yabynennet.xyz	NoError	185.82.202.246		NA
A	api.ip.sb, api.ip.sb.cdn.cloudflare.net	NoError	104.26.13.31, 172.67.75.172, 104.26.12.31	api.ip.sb.cdn.cloudflare.net	NA
A	cdn.discordapp.com	NoError	162.159.129.233, 162.159.130.233, 162.159.133.233, 162.159.134.233, 162.159.135.233		NA
-	api.ip.sb	-	104.26.13.31, 172.67.75.172, 104.26.12.31		NA

BEHAVIOR

Process Graph



Process #1: d609a21245d77dccd6d4a659cbd9466a.virus.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 47852, Reason: Analysis Target
Unmonitor End Time	End Time: 83848, Reason: Terminated
Monitor duration	36.00s
Return Code	0
PID	3676
Parent PID	912
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	72
File	6
Environment	1
Window	1
Process	1
-	3
-	5

Process #2: d609a21245d77dccd6d4a659cbd9466a.virus.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 80921, Reason: Child Process
Unmonitor End Time	End Time: 97266, Reason: Terminated
Monitor duration	16.34s
Return Code	0
PID	3720
Parent PID	3676
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\keecfmwgj\desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe	0xe60	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe	0xe60	0x401000(4198400)	0x7200	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe	0xe60	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe	0xe60 / 0xe8c	0x779f01c4(2006909380)	-	✓	1

Host Behavior

Type	Count
Module	17
Keyboard	2
Process	1
File	1
System	6
-	1
Registry	18
-	1

Process #3: explorer.exe

ID	3
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 90510, Reason: Injection
Unmonitor End Time	End Time: 289093, Reason: Terminated by Timeout
Monitor duration	198.58s
Return Code	Unknown
PID	912
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\keecfmwgj\desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe	0xe8c	0x27a0000(41549824)	0x5000	✓	1
Modify Memory	#2: c:\users\keecfmwgj\desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe	0xe8c	0x3a10000(60882944)	0x16000	✓	1
Create Remote Thread	#2: c:\users\keecfmwgj\desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe	0xe8c	0x3a11930(60889392)	-	✓	1

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Roaming\cdieedr	278.00 KB	a0f70f88c9a376e7c0f7e508c796bf1dbbf58ff8b172b9aff3421be63e2d7f78	✗
C:\Users\KEECFM~1\AppData\Local\Temp\69BE.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\KEECFM~1\AppData\Local\Temp\52B4.exe	3557.41 KB	e785bcea30bd913df48c9339dca2ed97c087b4f174f9a9da820001dbe1233c54	✗

Host Behavior

Type	Count
Module	17
System	3527
Process	276
Mutex	1
Registry	3
File	23
User	1
COM	1

Network Behavior

Type	Count
HTTP	9

Type	Count
TCP	9

Process #4: taskeng.exe

ID	4
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {312A59F4-5D1B-45EE-A1BE-19E5671C0331} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 128789, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 289093, Reason: Terminated by Timeout
Monitor duration	160.30s
Return Code	Unknown
PID	3768
Parent PID	864
Bitness	64 Bit

Process #5: cdieedr

ID	5
File Name	c:\users\keecfmwgj\appdata\roaming\cdieedr
Command Line	C:\Users\kEecfMwgj\AppData\Roaming\cdieedr
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 135295, Reason: Child Process
Unmonitor End Time	End Time: 289093, Reason: Terminated by Timeout
Monitor duration	153.80s
Return Code	Unknown
PID	3808
Parent PID	3768
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	29
File	3
Environment	1

Process #7: 52b4.exe

ID	7
File Name	c:\users\keecfmwgj\appdata\local\temp\52b4.exe
Command Line	C:\Users\KEECFM~1\AppData\Local\Temp\52B4.exe
Initial Working Directory	C:\Users\KEECFM~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 144823, Reason: Child Process
Unmonitor End Time	End Time: 164804, Reason: Terminated
Monitor duration	19.98s
Return Code	0
PID	3820
Parent PID	912
Bitness	32 Bit

Host Behavior

Type	Count
Module	482
Registry	2
Keyboard	1
System	10
-	1
File	5
Environment	1
Process	1
-	3
-	8

Process #8: applaunch.exe

ID	8
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\KEECFM~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 160646, Reason: Child Process
Unmonitor End Time	End Time: 241412, Reason: Terminated
Monitor duration	80.77s
Return Code	0
PID	3868
Parent PID	3820
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#7: c:\users\keecfmwgj\appdata\local\temp\52b4.exe	0xef0	0x400000(4194304)	0x20000	✓	1
Modify Memory	#7: c:\users\keecfmwgj\appdata\local\temp\52b4.exe	0xef0	0xfffde008(4294828040)	0x4	✓	1
Modify Control Flow	#7: c:\users\keecfmwgj\appdata\local\temp\52b4.exe	0xef0 / 0xf20	0x779f01c4(2006909380)	-	✓	1

Host Behavior

Type	Count
Registry	279
File	351
System	163
-	13
User	3
Module	74
Environment	8
COM	108
-	11
Window	2
Keyboard	3

Network Behavior

Type	Count
HTTPS	2
DNS	4
TCP	3

Process #12: 69be.exe

ID	12
File Name	c:\users\keecfmwgj\appdata\local\temp\69be.exe
Command Line	C:\Users\KEECFM~1\AppData\Local\Temp\69BE.exe
Initial Working Directory	C:\Users\KEECFM~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 239631, Reason: Child Process
Unmonitor End Time	End Time: 247729, Reason: Terminated
Monitor duration	8.10s
Return Code	0
PID	4016
Parent PID	912
Bitness	32 Bit

Host Behavior

Type	Count
Module	482
Registry	2
Keyboard	1
System	10
-	1
File	5
Environment	1
Process	1
-	3
-	9

Process #13: applaunch.exe

ID	13
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\KEECFM~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 245819, Reason: Child Process
Unmonitor End Time	End Time: 289093, Reason: Terminated by Timeout
Monitor duration	43.27s
Return Code	Unknown
PID	4040
Parent PID	4016
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\temp\69be.exe	0xfb4	0x70000(458752)	0x20000	✓	1
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\temp\69be.exe	0xfb4	0xfffde008(4294828040)	0x4	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\appdata\local\temp\69be.exe	0xfb4 / 0xfcc	0x779f01c4(2006909380)	-	✓	1

Host Behavior

Type	Count
Registry	269
File	337
System	69
-	12
User	3
Module	39
Environment	4
Window	1
COM	79
-	2
Keyboard	3

Network Behavior

Type	Count
DNS	3
TCP	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a0f70f88c9a376e7c0f7e508c796bf1dbbf58ff8b172b9aff3421be63e2d7f78	C:\Users\kEecfMwgj\Desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe, C:\Users\kEecfMwgj\AppData\Roaming\cdieedr	Sample File	278.00 KB	application/vnd.microsoft.portable-executable	Write, Delete, Create, Access	MALICIOUS
e785bcea30bd913df48c9339dca2ed97c087b4f174f9a9da820001dbe1233c54	C:\Users\KEECFM~1\AppData\Local\Temp\69BE.exe, C:\Users\KEECFM~1\AppData\Local\Temp\52B4.exe	Downloaded File	3557.41 KB	application/vnd.microsoft.portable-executable	Write, Create, Access	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe	Sample File	Delete, Access	CLEAN
apfHQ	Accessed File	Access	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\cdieedr	Sample File	Write, Delete, Create, Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\cdieedr:Zone.Identifier	Accessed File	Delete, Access	CLEAN
C:\Windows\system32\advapi32.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\estugfj	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\52B4.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\52B4.exe	Downloaded File	Write, Create, Access	CLEAN
	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Read, Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe.Config	Accessed File	Read, Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Yandex\YaAddon	Accessed File	Create, Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Yandex	Accessed File	Create, Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\NordVPN	Accessed File	Access	CLEAN
C:\Program Files (x86)\Internet Explorer\iexplore.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\1BY5mTkcZANR.docx	Accessed File	Read, Access	CLEAN
C:\Users\kEecfMwgj\Desktop\CduSDavY.doc	Accessed File	Read, Access	CLEAN
C:\Users\kEecfMwgj\Documents\7VZCVQe.docx	Accessed File	Read, Access	CLEAN
C:\Users\kEecfMwgj\Documents\IvDexdy_r Oq.docx	Accessed File	Read, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Documents\KangmawL.docx	Accessed File	Read, Access	CLEAN
C:\Users\kEecfMwgj\Documents\t6GW4d_MTgVoESu.docx	Accessed File	Read, Access	CLEAN
C:\Users\kEecfMwgj\Documents\W0TV7ENECKo 9vK.docx	Accessed File	Read, Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\FileZilla\sitemanager.xml	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\fl.exe	Accessed File	Create, Delete, Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\69BE.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\69BE.exe	Downloaded File	Write, Create, Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://host-data-coin-11.com	-	5.188.88.184	-	POST	MALICIOUS
http://data-host-coin-8.com/files/9718_1641769402_1919.exe	-	5.188.88.184	-	GET	MALICIOUS
https://cdn.discordapp.com/attachments/917178535238586432/922560115226312704/StopScam.vmp.exe	-	162.159.129.233	-	GET	MALICIOUS
https://api.ip.sb/ip	-	104.26.13.31	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
yabynennet.xyz	185.82.202.246	-	DNS	MALICIOUS
host-data-coin-11.com	5.188.88.184	-	HTTP	CLEAN
data-host-coin-8.com	5.188.88.184	-	HTTP	CLEAN
api.ip.sb	104.26.12.31, 172.67.75.172, 104.26.13.31	-	HTTPS, DNS	CLEAN
api.ip.sb.cdn.cloudflare.net	104.26.12.31, 172.67.75.172, 104.26.13.31	-	DNS	CLEAN
cdn.discordapp.com	162.159.130.233, 162.159.133.233, 162.159.134.233, 162.159.135.233, 162.159.129.233	-	HTTPS, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
5.188.88.184	host-data-coin-11.com, data-host-coin-8.com	Russia	TCP, DNS, HTTP	CLEAN
192.168.0.1	-	-	UDP, DNS	CLEAN
162.159.129.233	cdn.discordapp.com	-	TCP, HTTPS, DNS	CLEAN
185.82.202.246	yabynennet.xyz	Netherlands	TCP, DNS	CLEAN
104.26.13.31	api.ip.sb, api.ip.sb.cdn.cloudflare.net	United States	TCP, HTTPS, DNS, TLS	CLEAN
172.67.75.172	api.ip.sb, api.ip.sb.cdn.cloudflare.net	United States	DNS	CLEAN
104.26.12.31	api.ip.sb, api.ip.sb.cdn.cloudflare.net	United States	DNS	CLEAN
162.159.130.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.133.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.134.233	cdn.discordapp.com	-	DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
162.159.135.233	cdn.discordapp.com	-	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
4BCD659AD8F347B5B451918CD891C8238443A5AF	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\IDE	access	d609a21245d77dccd6d4a659cbd9466a.virus.exe	CLEAN
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\SCSI	access	d609a21245d77dccd6d4a659cbd9466a.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\svcVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Version	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Borland\Locales	access	52b4.exe, 69be.exe	CLEAN
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales	access	52b4.exe, 69be.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseHttpPipeliningAndBufferPooling	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseHttpPipeliningAndBufferPooling	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseSafeSynchronousClose	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseSafeSynchronousClose	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseStrictRfcInterimResponseHandling	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictRfcInterimResponseHandling	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowDangerousUnicodeDecompositions	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowDangerousUnicodeDecompositions	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.UseStrictIPv6AddressParsing	access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictIPv6AddressParsing	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowAllUriEncodingExpansion	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowAllUriEncodingExpansion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SystemDefaultTlsVersions	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.RequireCertificateEKUs	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\RequireCertificateEKUs	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\WMIDisableCOMSecurity	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CSDVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Clients\StartMenuInternet	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Clients\StartMenuInternet\IEXPLORE.EXE	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Clients\StartMenuInternet\IEXPLORE.EXE\shell\open\command	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Valve\Steam	access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743	access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132}.KB4503575	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132}.KB4503575\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132}.KB4503575\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	read, access	applaunch.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
d609a21245d77dccd6d4a659cbd9466a.virus.exe	"C:\Users\kEecfMwgj\Desktop\d609a21245d77dccd6d4a659cbd9466a.virus.exe"	MALICIOUS
52b4.exe	C:\Users\KEECFM~1\AppData\Local\Temp\52B4.exe	MALICIOUS

Process Name	Commandline	Verdict
69be.exe	C:\Users\KEECFM~1\AppData\Local\Temp\69BE.exe	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
applaunch.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe"	SUSPICIOUS
taskeng.exe	taskeng.exe {312A59F4-5D1B-45EE-A1BE-19E5671C0331} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]	CLEAN
cdieedr	C:\Users\kEecfMwgj\AppData\Roaming\cdieedr	CLEAN

YARA / AV

YARA (3)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Malware	SmokeLoaderStrings	SmokeLoader strings	Function Strings	function_strings_process_3.txt	Downloader	5/5

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.4.0
Dynamic Engine Version	4.4.0 / 12/08/2021 19:04
Static Engine Version	4.4.0.0 / 2021-12-08 18:00:20
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.0.0 / 2021-12-08 18:00:20
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.7 / 2021-12-15 19:11:26
YARA Built-in Ruleset Version	4.4.1.7

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	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH
User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp
System Root	C:\Windows