MALICIOUS

Classifications: Downloader | Injector | Spyware

Threat Names: SmokeLoader | Gen:Variant.Babar.29261

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**8696a4269e30ddb34a7e0e84629ede03.virus.exe**
ID	#3014847
MD5	8696a4269e30ddb34a7e0e84629ede03
SHA1	125198e1f636ef118e468145d02e801a3ffe2a97
SHA256	47ec411eab0aa15619f24caa6256ed4ca5cfc695a26f5b71830b53b07c22b05b
File Size	278.50 KB
Report Created	2021-11-18 13:28 (UTC+1)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (26 rules, 171 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	2	Downloader
	• Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #1) 8696a4269e30ddb34a7e0e84629ede03.virus.exe. • Rule "SmokeLoaderStrings" from ruleset "Malware" has matched on the function strings for (process #2) explorer.exe.			
5/5	Browser	Adds a hook to a web browser	7	Spyware
	• A hook was added to Internet Explorer for wininet.dll:HttpSendRequestA+0x0. • A hook was added to Internet Explorer for wininet.dll:HttpSendRequestW+0x0. • A hook was added to Internet Explorer for wininet.dll:InternetWriteFile+0x0. • A hook was added to Internet Explorer for ws2_32.dll:send+0x0. • A hook was added to Internet Explorer for ws2_32.dll:WSASend+0x0. • A hook was added to Internet Explorer for ws2_32.dll:GetAddrInfoW+0x0. • A hook was added to Internet Explorer for ws2_32.dll:GetAddrInfoExW+0x0.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: AbleFTP, FileZilla, Total Commander, Microsoft Outlook, Internet Explorer, git.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #2) explorer.exe tries to delete zone identifier of file "C:\Users\kEecfMwgj\AppData\Roaming\ahieedr".			
4/5	Injection	Writes into the memory of another process	26	Injector

Score	Category	Operation	Count	Classification
	• (Process #1) 8696a4269e30ddb34a7e0e84629ede03.virus.exe modifies memory of (process #2) explorer.exe. • (Process #2) explorer.exe modifies memory of (process #3) explorer.exe. • (Process #2) explorer.exe modifies memory of (process #4) explorer.exe. • (Process #2) explorer.exe modifies memory of (process #5) explorer.exe. • (Process #2) explorer.exe modifies memory of (process #6) explorer.exe. • (Process #6) explorer.exe modifies memory of (process #7) iexplore.exe. • (Process #16) explorer.exe modifies memory of (process #7) iexplore.exe. • (Process #2) explorer.exe modifies memory of (process #8) explorer.exe. • (Process #6) explorer.exe modifies memory of (process #9) iexplore.exe. • (Process #11) explorer.exe modifies memory of (process #9) iexplore.exe. • (Process #16) explorer.exe modifies memory of (process #9) iexplore.exe. • (Process #2) explorer.exe modifies memory of (process #11) explorer.exe. • (Process #2) explorer.exe modifies memory of (process #12) explorer.exe. • (Process #11) explorer.exe modifies memory of (process #13) flashfxp.exe. • (Process #11) explorer.exe modifies memory of (process #14) filezilla.exe. • (Process #24) explorer.exe modifies memory of (process #14) filezilla.exe. • (Process #2) explorer.exe modifies memory of (process #16) explorer.exe. • (Process #11) explorer.exe modifies memory of (process #17) winscp.exe. • (Process #11) explorer.exe modifies memory of (process #19) outlook.exe. • (Process #2) explorer.exe modifies memory of (process #20) explorer.exe. • (Process #11) explorer.exe modifies memory of (process #21) smartftp.exe. • (Process #11) explorer.exe modifies memory of (process #22) thunderbird.exe. • (Process #2) explorer.exe modifies memory of (process #23) explorer.exe. • (Process #2) explorer.exe modifies memory of (process #24) explorer.exe. • (Process #2) explorer.exe modifies memory of (process #25) explorer.exe. • (Process #2) explorer.exe modifies memory of (process #26) explorer.exe.			
4/5	Injection	Modifies control flow of another process	14	Injector
	• (Process #1) 8696a4269e30ddb34a7e0e84629ede03.virus.exe creates thread in (process #2) explorer.exe. • (Process #6) explorer.exe creates thread in (process #7) iexplore.exe. • (Process #11) explorer.exe creates thread in (process #7) iexplore.exe. • (Process #16) explorer.exe creates thread in (process #7) iexplore.exe. • (Process #6) explorer.exe creates thread in (process #9) iexplore.exe. • (Process #11) explorer.exe creates thread in (process #9) iexplore.exe. • (Process #16) explorer.exe creates thread in (process #9) iexplore.exe. • (Process #11) explorer.exe creates thread in (process #13) flashfxp.exe. • (Process #11) explorer.exe creates thread in (process #14) filezilla.exe. • (Process #24) explorer.exe creates thread in (process #14) filezilla.exe. • (Process #11) explorer.exe creates thread in (process #17) winscp.exe. • (Process #11) explorer.exe creates thread in (process #19) outlook.exe. • (Process #11) explorer.exe creates thread in (process #21) smartftp.exe. • (Process #11) explorer.exe creates thread in (process #22) thunderbird.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected the sample itself as "Gen:Variant.Babar.29261".			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
3/5	Data Collection	Reads memory of user process	6	-

Score	Category	Operation	Count	Classification
	• (Process #11) explorer.exe reads memory of process (process #13) flashfxp.exe. • (Process #11) explorer.exe reads memory of process (process #14) filezilla.exe. • (Process #11) explorer.exe reads memory of process (process #17) winscp.exe. • (Process #11) explorer.exe reads memory of process (process #21) smartftp.exe. • (Process #11) explorer.exe reads memory of process (process #22) thunderbird.exe. • (Process #24) explorer.exe reads memory of process (process #14) filezilla.exe.			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #1) 8696a4269e30ddb34a7e0e84629ede03.virus.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Hide Tracks	Deletes file after execution	2	-
	• (Process #2) explorer.exe deletes executed executable "c:\users\keecfmwgj\appdata\roaming\ahieedr". • (Process #2) explorer.exe deletes executed executable "c:\users\keecfmwgj\desktop\8696a4269e30ddb34a7e0e84629ede03.virus.exe".			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #3) explorer.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #3) explorer.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	Data Collection	Reads sensitive ftp data	3	-
	• (Process #3) explorer.exe tries to read sensitive data of ftp application "FileZilla" by file. • (Process #23) explorer.exe tries to read sensitive data of ftp application "AbleFTP" by file. • (Process #23) explorer.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	Anti Analysis	Delays execution	3	-
	• (Process #14) filezilla.exe has a thread which sleeps more than 5 minutes. • (Process #2) explorer.exe has a thread which sleeps more than 5 minutes. • (Process #26) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #23) explorer.exe tries to read sensitive data of application "git" by file.			
2/5	Masquerade	Creates a new process from a system binary	1	-
	• (Process #2) explorer.exe creates a new explorer.exe process.			
2/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\ahieedr", to be triggered by Logon. • Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\ahieedr", to be triggered by Time. Task has been rescheduled by the analyzer.			
1/5	Discovery	Enumerates running processes	9	-

Score	Category	Operation	Count	Classification
	• (Process #2) explorer.exe enumerates running processes. • (Process #6) explorer.exe enumerates running processes. • (Process #8) explorer.exe enumerates running processes. • (Process #11) explorer.exe enumerates running processes. • (Process #12) explorer.exe enumerates running processes. • (Process #16) explorer.exe enumerates running processes. • (Process #20) explorer.exe enumerates running processes. • (Process #24) explorer.exe enumerates running processes. • (Process #25) explorer.exe enumerates running processes.			
1/5	Mutex	Creates mutex	18	-
	• (Process #2) explorer.exe creates mutex with name "7C2D5ED2D6B71DDF065E08EDB38519078443A5AF". • (Process #6) explorer.exe creates mutex with name "opera_shared_counter". • (Process #7) iexplore.exe creates mutex with name "A51BEC40CF6D8BD76CA31608E39B8662". • (Process #9) iexplore.exe creates mutex with name "3614EE7DCF67EA55E5FA4BF08892DDA7". • (Process #11) explorer.exe creates mutex with name "opera_shared_counter". • (Process #7) iexplore.exe creates mutex with name "79FF8A9E04191F68E84F55B788C3DB95". • (Process #9) iexplore.exe creates mutex with name "5C7B8ACCFA112F039BCB37749FCB206B". • (Process #13) flashfxp.exe creates mutex with name "093E748EDFA3BC8C486A602DB4AE042E". • (Process #14) filezilla.exe creates mutex with name "F086C931E57676B770EA8825FF5EE63F". • (Process #17) winscp.exe creates mutex with name "9A13379D174D40744C105A1B640A414C". • (Process #19) outlook.exe creates mutex with name "DD9336F98CA7F483A811DFD312803FE9". • (Process #21) smartftp.exe creates mutex with name "89CC2A001C7D1D32AEC982DE2C008933". • (Process #16) explorer.exe creates mutex with name "opera_shared_counter". • (Process #22) thunderbird.exe creates mutex with name "0CD685E8677D85A7CBD4766477F43A23". • (Process #7) iexplore.exe creates mutex with name "84CFF8068531CDBB2CA4C9A315CFD60F". • (Process #9) iexplore.exe creates mutex with name "2EFA102D67FBFA95AE7895A49D7EA40D". • (Process #24) explorer.exe creates mutex with name "opera_shared_counter". • (Process #14) filezilla.exe creates mutex with name "E5AED93F4D1BFA97BD58091959CE09A1".			
1/5	Hide Tracks	Creates process with hidden window	13	-
	• (Process #2) explorer.exe starts (process #3) explorer.exe with a hidden window. • (Process #2) explorer.exe starts (process #4) explorer.exe with a hidden window. • (Process #2) explorer.exe starts (process #5) explorer.exe with a hidden window. • (Process #2) explorer.exe starts (process #6) explorer.exe with a hidden window. • (Process #2) explorer.exe starts (process #8) explorer.exe with a hidden window. • (Process #2) explorer.exe starts (process #11) explorer.exe with a hidden window. • (Process #2) explorer.exe starts (process #12) explorer.exe with a hidden window. • (Process #2) explorer.exe starts (process #16) explorer.exe with a hidden window. • (Process #2) explorer.exe starts (process #20) explorer.exe with a hidden window. • (Process #2) explorer.exe starts (process #23) explorer.exe with a hidden window. • (Process #2) explorer.exe starts (process #24) explorer.exe with a hidden window. • (Process #2) explorer.exe starts (process #25) explorer.exe with a hidden window. • (Process #2) explorer.exe starts (process #26) explorer.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	24	-

Score	Category	Operation	Count	Classification
	• (Process #2) explorer.exe reads from (process #3) explorer.exe. • (Process #2) explorer.exe reads from (process #4) explorer.exe. • (Process #2) explorer.exe reads from (process #5) explorer.exe. • (Process #2) explorer.exe reads from (process #6) explorer.exe. • (Process #6) explorer.exe reads from (process #7) iexplore.exe. • (Process #6) explorer.exe reads from taskeng.exe. • (Process #2) explorer.exe reads from (process #8) explorer.exe. • (Process #2) explorer.exe reads from (process #11) explorer.exe. • (Process #11) explorer.exe reads from taskeng.exe. • (Process #11) explorer.exe reads from (process #13) flashfxp.exe. • (Process #2) explorer.exe reads from (process #12) explorer.exe. • (Process #11) explorer.exe reads from (process #14) filezilla.exe. • (Process #11) explorer.exe reads from (process #17) winscp.exe. • (Process #2) explorer.exe reads from (process #16) explorer.exe. • (Process #11) explorer.exe reads from (process #21) smartftp.exe. • (Process #11) explorer.exe reads from (process #22) thunderbird.exe. • (Process #2) explorer.exe reads from (process #20) explorer.exe. • (Process #16) explorer.exe reads from (process #7) iexplore.exe. • (Process #16) explorer.exe reads from taskeng.exe. • (Process #2) explorer.exe reads from (process #23) explorer.exe. • (Process #2) explorer.exe reads from (process #24) explorer.exe. • (Process #2) explorer.exe reads from (process #25) explorer.exe. • (Process #2) explorer.exe reads from (process #26) explorer.exe. • (Process #24) explorer.exe reads from (process #14) filezilla.exe.		
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #4) explorer.exe tries to gather information about application "Mozilla" by registry. • (Process #3) explorer.exe tries to gather information about application "Mozilla" by registry.			
1/5	Execution	Executes itself	1	-
	• (Process #10) taskeng.exe executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\8696a4269e30ddb34a7e0e84629ede03.virus.exe.			
1/5	Obfuscation	Overwrites code	8	-
	• (Process #7) iexplore.exe overwrites code to possibly hide behavior. • (Process #9) iexplore.exe overwrites code to possibly hide behavior. • (Process #13) flashfxp.exe overwrites code to possibly hide behavior. • (Process #14) filezilla.exe overwrites code to possibly hide behavior. • (Process #17) winscp.exe overwrites code to possibly hide behavior. • (Process #19) outlook.exe overwrites code to possibly hide behavior. • (Process #21) smartftp.exe overwrites code to possibly hide behavior. • (Process #22) thunderbird.exe overwrites code to possibly hide behavior.			
1/5	Obfuscation	Resolves API functions dynamically	22	-

Score	Category	Operation	Count	Classification
		• (Process #2) explorer.exe resolves 24 API functions by name. • (Process #3) explorer.exe resolves 156 API functions by name. • (Process #4) explorer.exe resolves 68 API functions by name. • (Process #5) explorer.exe resolves 56 API functions by name. • (Process #6) explorer.exe resolves 91 API functions by name. • (Process #7) iexplore.exe resolves 105 API functions by name. • (Process #9) iexplore.exe resolves 105 API functions by name. • (Process #8) explorer.exe resolves 90 API functions by name. • (Process #11) explorer.exe resolves 72 API functions by name. • (Process #13) flashfxp.exe resolves 71 API functions by name. • (Process #14) filezilla.exe resolves 93 API functions by name. • (Process #12) explorer.exe resolves 70 API functions by name. • (Process #17) winscp.exe resolves 72 API functions by name. • (Process #19) outlook.exe resolves 72 API functions by name. • (Process #21) smartftp.exe resolves 72 API functions by name. • (Process #16) explorer.exe resolves 54 API functions by name. • (Process #22) thunderbird.exe resolves 72 API functions by name. • (Process #20) explorer.exe resolves 52 API functions by name. • (Process #23) explorer.exe resolves 159 API functions by name. • (Process #24) explorer.exe resolves 91 API functions by name. • (Process #25) explorer.exe resolves 89 API functions by name. • (Process #26) explorer.exe resolves 83 API functions by name.		

Mitre ATT&CK Matrix

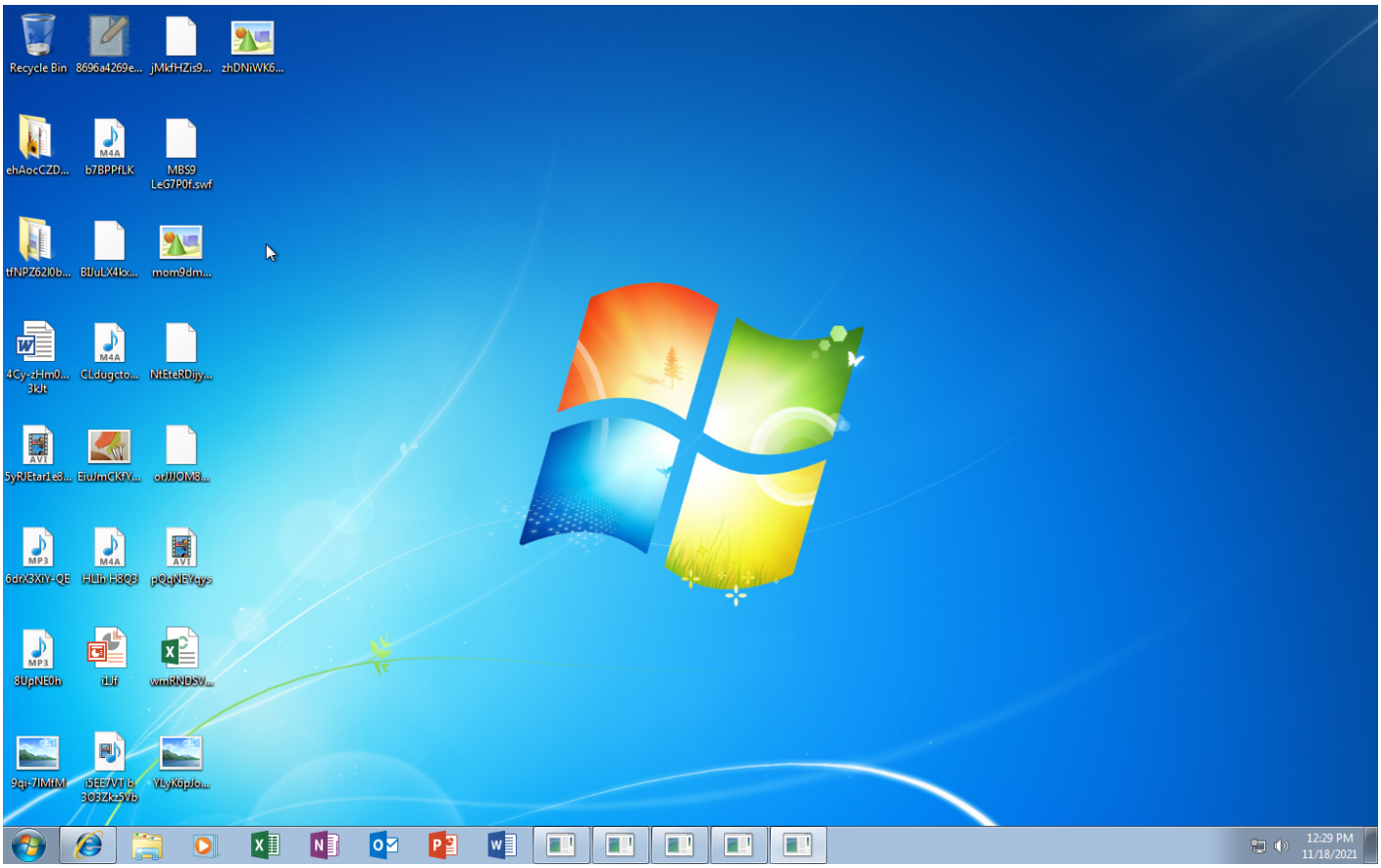
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1179 Hooking	#T1179 Hooking	#T1096 NTFS File Attributes	#T1003 Credential Dumping	#T1057 Process Discovery		#T1119 Automated Collection			
		#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window	#T1214 Credentials in Registry	#T1012 Query Registry		#T1005 Data from Local System			
				#T1045 Software Packing	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1185 Man in the Browser			
					#T1179 Hooking						

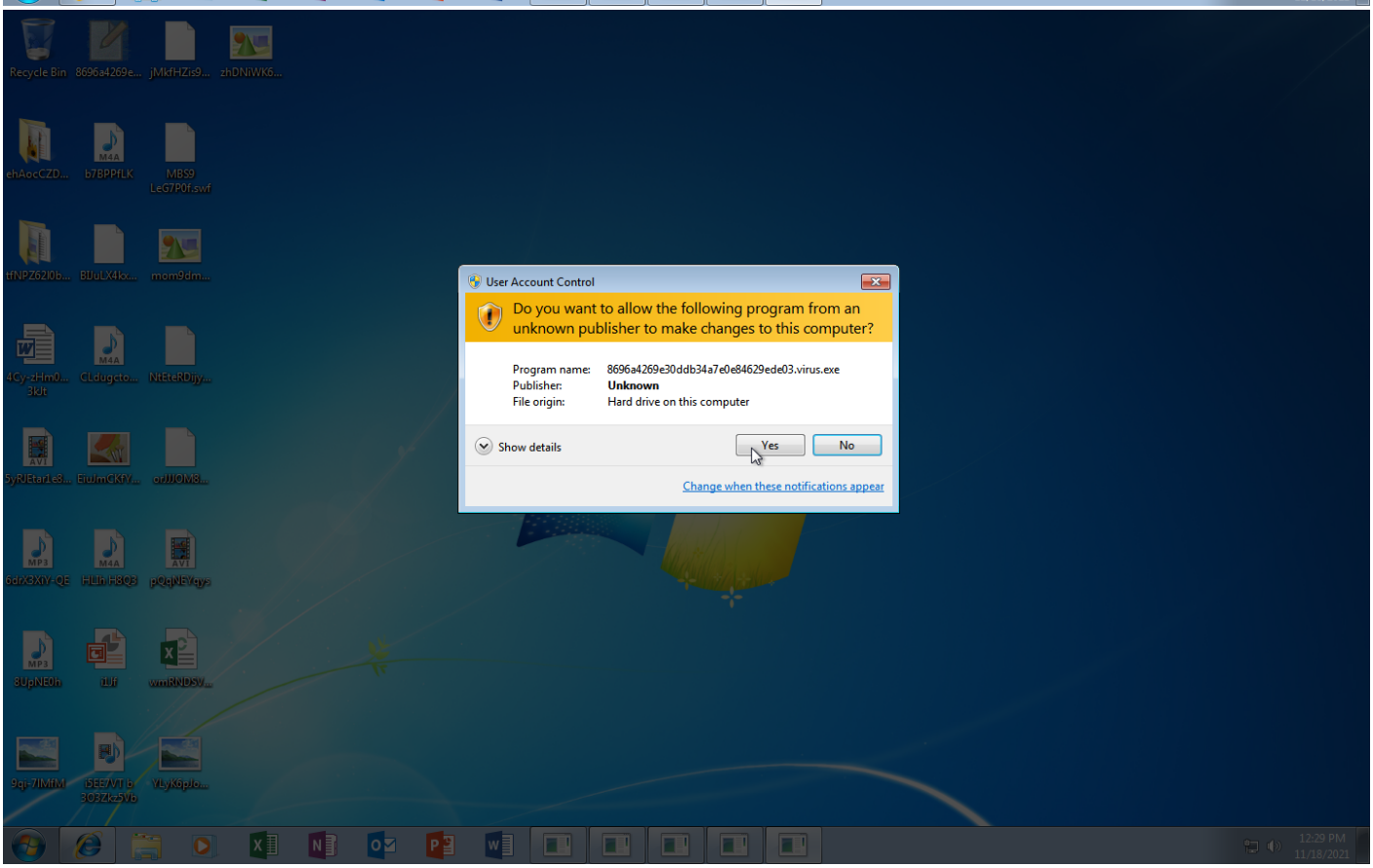
Sample Information

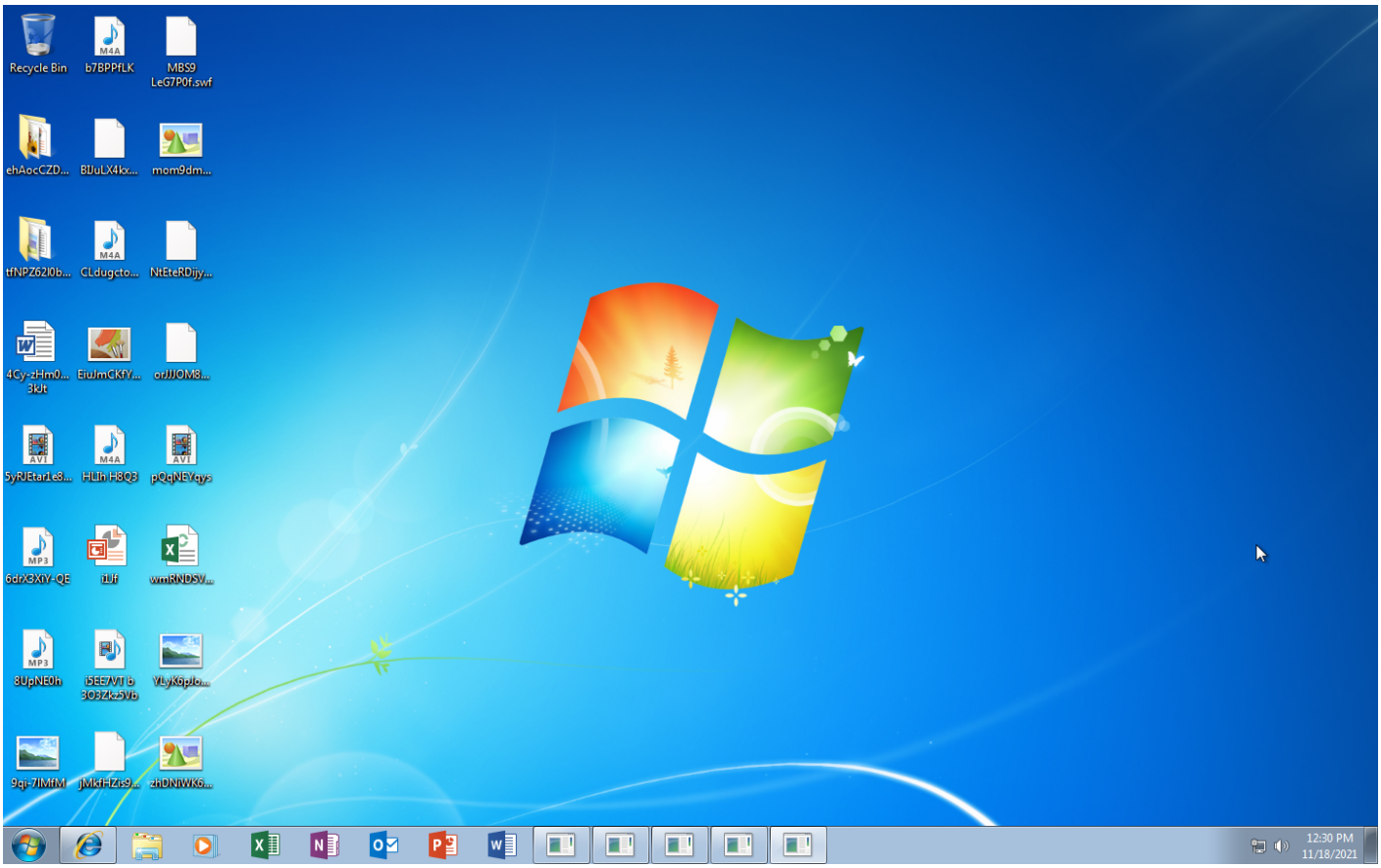
ID	#3014847
MD5	8696a4269e30ddb34a7e0e84629ede03
SHA1	125198e1f636ef118e468145d02e801a3ffe2a97
SHA256	47ec411eab0aa15619f24caa6256ed4ca5cfc695a26f5b71830b53b07c22b05b
SSDeep	3072:80Zpf7ywrLoWHdAucQoHnSzG+dWpvgne52lPxsBvBPoeg8MRkY34R3R8UJPb9wy:RIUJcQk3+WvgnJla7oe0RdIdRzYy
ImpHash	ff6439958bc7d1b926a3ea41188420fe
File Name	8696a4269e30ddb34a7e0e84629ede03.virus.exe
File Size	278.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

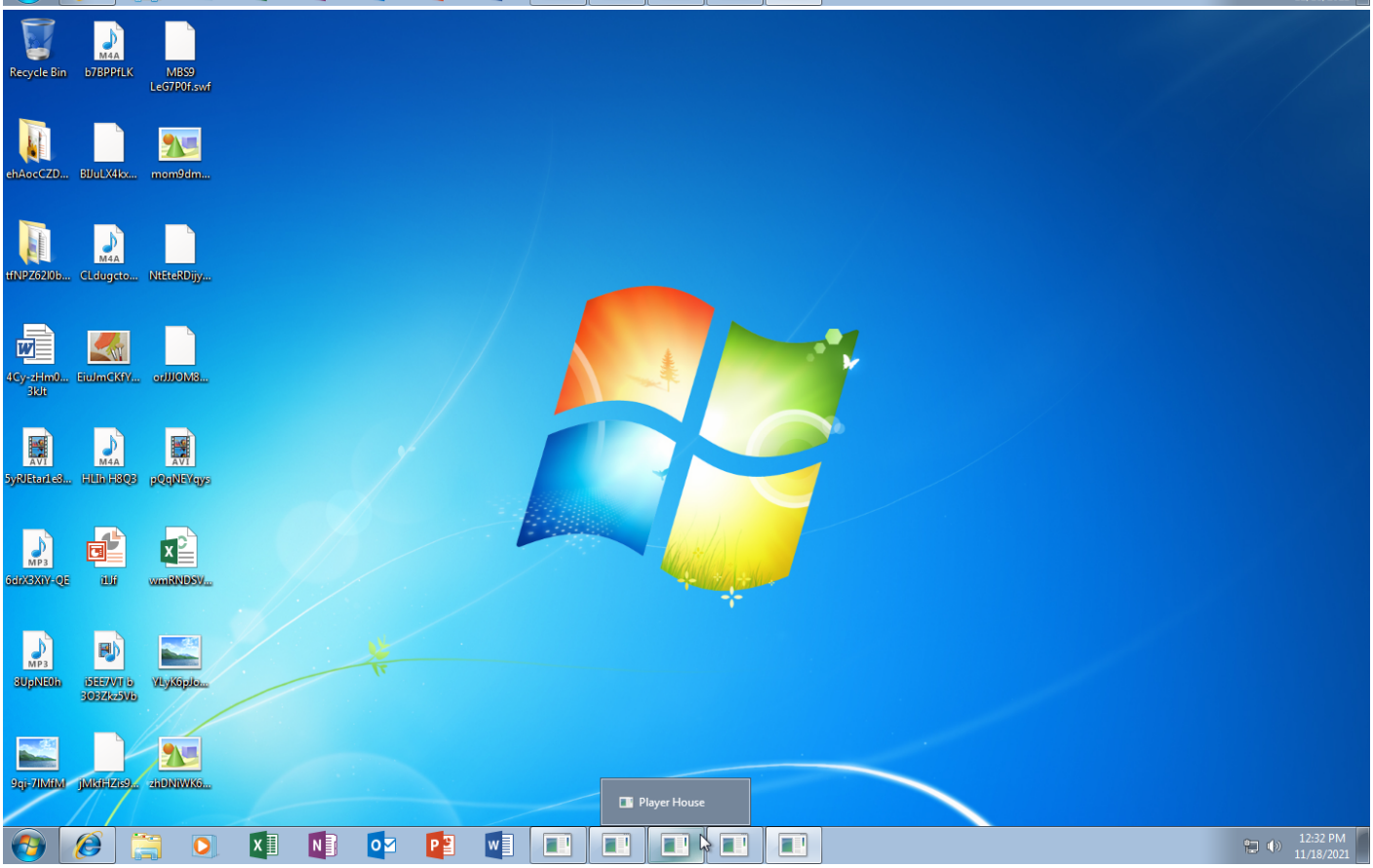
Analysis Information

Creation Time	2021-11-18 13:28 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	25
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✓
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	1
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	2


Recycle Bin
8696a4269e...
jMkfHZis9...
zhDNiWK6...
ehAocCZD...
b7BPPfLK
MBS9 LeG7P0f.swf
tfNPZ62l0b...
BUuLX4lx...
mom9dm...
4Cy-zHm0... 3kJt
CLdugcto...
NtEteRDijy...
5yRJEtar1e8...
EiuJmCKfY...
orJJOM8...
6drX3XtY-QE
HLIh H8Q3
pQqNEYqys
8UpNE0h
1.jf
wmRNDSV...
9qi-7IMfM
YLyK6plo...
12:29 PM
11/18/2021


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 8696a4269e30ddb34a7e0e84629ede03.virus.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

1.57 KB total sent

425.09 KB total received

1 ports 80

1 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

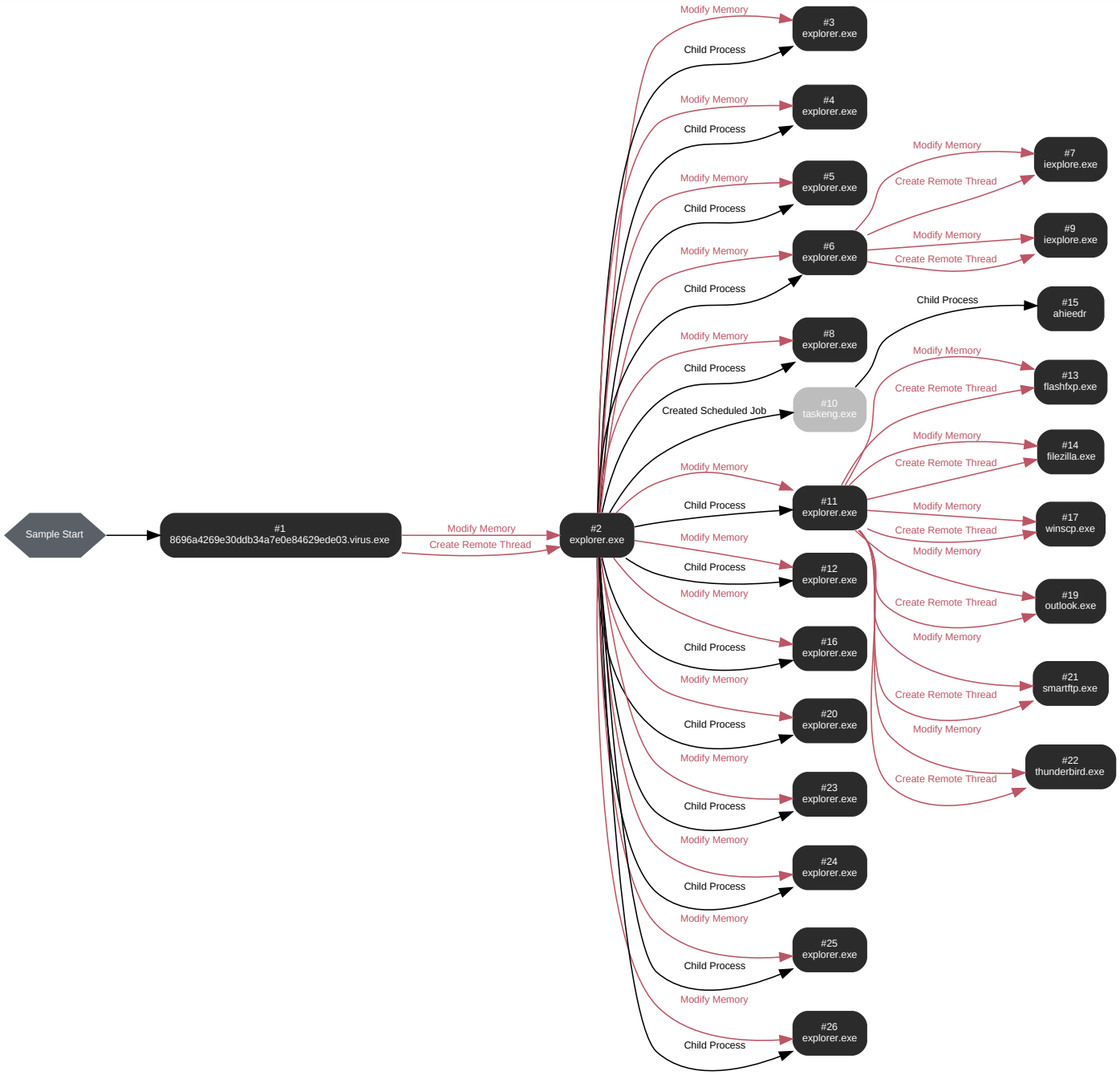
2 sessions, 1.57 KB sent, 425.09 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	rsuehfidvdkfvk.top/	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: 8696a4269e30ddb34a7e0e84629ede03.virus.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\8696a4269e30ddb34a7e0e84629ede03.virus.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\8696a4269e30ddb34a7e0e84629ede03.virus.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 62446, Reason: Analysis Target
Unmonitor End Time	End Time: 95904, Reason: Terminated
Monitor duration	33.46s
Return Code	0
PID	3460
Parent PID	1116
Bitness	32 Bit

Host Behavior

Type	Count
System	10
Module	44
File	4
Environment	1
Keyboard	2
Process	1
-	1
Registry	18
-	1

Process #2: explorer.exe

ID	2
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 89180, Reason: Injection
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	214.05s
Return Code	Unknown
PID	1116
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\keecfmwgj\desktop\8696a4269e30ddb34a7e0e84629ede03.virus.exe	0xd88	0x2400000(37748736)	0x5000	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\8696a4269e30ddb34a7e0e84629ede03.virus.exe	0xd88	0x37c0000(58458112)	0x16000	✓	1
Create Remote Thread	#1: c:\users\keecfmwgj\desktop\8696a4269e30ddb34a7e0e84629ede03.virus.exe	0xd88	0x37c1930(58464560)	-	✓	1

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Roaming\ahieedr	278.50 KB	47ec411eab0aa15619f24caa6256ed4ca5cfc695a26f5b71830b53b07c22b05b	✗
C:\Users\kEecfMwgj\AppData\Roaming\htcufvu	412.28 KB	6b2757598d730ac5f2c56a1be845369ba88384f034b255ee6bc6a2c34ca086ac	✗

Host Behavior

Type	Count
Module	213
System	1742
Process	286
Mutex	1
Registry	3
File	20
User	1
COM	1
-	39
-	13

Network Behavior

Type	Count
HTTP	1
TCP	1

Process #3: explorer.exe

ID	3
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 119819, Reason: Child Process
Unmonitor End Time	End Time: 140216, Reason: Terminated
Monitor duration	20.40s
Return Code	0
PID	3544
Parent PID	1116
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0xc0000(786432)	0x6b000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x130000(1245184)	0x74000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x3e0efa(4067066)	0x7	✓	1

Host Behavior

Type	Count
Module	197
Registry	66
System	3
File	57

Network Behavior

Type	Count
HTTP	1
TCP	1

Process #4: explorer.exe

ID	4
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\explorer.exe
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 129800, Reason: Child Process
Unmonitor End Time	End Time: 135257, Reason: Terminated
Monitor duration	5.46s
Return Code	0
PID	3552
Parent PID	1116
Bitness	64 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x50000(327680)	0xc000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x60000(393216)	0x7000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0xff64b790(4284790672)	0x10	✓	1

Host Behavior

Type	Count
Module	80
Registry	5

Process #5: explorer.exe

ID	5
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 135258, Reason: Child Process
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	167.98s
Return Code	Unknown
PID	3564
Parent PID	1116
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x70000(458752)	0x9000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x80000(524288)	0x4000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x3e0efa(4067066)	0x7	✓	1

Host Behavior

Type	Count
Module	578
File	251
System	250

Process #6: explorer.exe

ID	6
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 138694, Reason: Child Process
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	164.54s
Return Code	Unknown
PID	3584
Parent PID	1116
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x70000(458752)	0xb000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x80000(524288)	0x7000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x3e0efa(4067066)	0x7	✓	1

Host Behavior

Type	Count
Module	188
File	1
Process	17407
Mutex	2
-	6
-	2
System	157

Process #7: iexplore.exe

ID	7
File Name	c:\program files (x86)\internet explorer\iexplore.exe
Command Line	"C:\Program Files (x86)\Internet Explorer\iexplore.exe" about:blank
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 139378, Reason: Injection
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	163.86s
Return Code	Unknown
PID	1432
Parent PID	1116
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\windows\syswow64\explorer.exe	0xe04	0x2900000(42991616)	0xb000	✓	1
Modify Memory	#6: c:\windows\syswow64\explorer.exe	0xe04	0x2910000(43057152)	0x1000	✓	1
Modify Memory	#6: c:\windows\syswow64\explorer.exe	0xe04	0x7793bee0(2006171360)	0x5	✓	2
Create Remote Thread	#6: c:\windows\syswow64\explorer.exe	0xe04	0x7793bee0(2006171360)	-	✓	1
Create Remote Thread	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	-	✓	1
Modify Memory	#16: c:\windows\syswow64\explorer.exe	0xe6c	0x30e0000(51249152)	0x9000	✓	1
Modify Memory	#16: c:\windows\syswow64\explorer.exe	0xe6c	0x30f0000(51314688)	0x1000	✓	1
Create Remote Thread	#16: c:\windows\syswow64\explorer.exe	0xe6c	0x7793bee0(2006171360)	-	✓	1

Host Behavior

Type	Count
Module	261
Mutex	3
System	3

Process #8: explorer.exe

ID	8
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\explorer.exe
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 140421, Reason: Child Process
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	162.81s
Return Code	Unknown
PID	3600
Parent PID	1116
Bitness	64 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x50000(327680)	0xf000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x60000(393216)	0x9000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0xff64b790(4284790672)	0x10	✓	1

Host Behavior

Type	Count
Module	103
File	1
Process	270

Process #9: iexplore.exe

ID	9
File Name	c:\program files (x86)\internet explorer\iexplore.exe
Command Line	"C:\Program Files (x86)\Internet Explorer\iexplore.exe" SCODEF:1432 CREDAT:14337
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 140469, Reason: Injection
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	162.76s
Return Code	Unknown
PID	1352
Parent PID	1432
Bitness	32 Bit

Injection Information (11)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\windows\syswow64\explorer.exe	0xe04	0x2350000(37027840)	0xb000	✓	1
Modify Memory	#6: c:\windows\syswow64\explorer.exe	0xe04	0x2360000(37093376)	0x1000	✓	1
Modify Memory	#6: c:\windows\syswow64\explorer.exe	0xe04	0x7793bee0(2006171360)	0x5	✓	4
Create Remote Thread	#6: c:\windows\syswow64\explorer.exe	0xe04	0x7793bee0(2006171360)	-	✓	1
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x25a0000(39452672)	0x9000	✓	1
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x25b0000(39518208)	0x1000	✓	1
Create Remote Thread	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	-	✓	1
Modify Memory	#16: c:\windows\syswow64\explorer.exe	0xe6c	0x25e0000(39714816)	0x9000	✓	1
Modify Memory	#16: c:\windows\syswow64\explorer.exe	0xe6c	0x25f0000(39780352)	0x1000	✓	1
Modify Memory	#16: c:\windows\syswow64\explorer.exe	0xe6c	0x7793bee0(2006171360)	0x5	✓	1
Create Remote Thread	#16: c:\windows\syswow64\explorer.exe	0xe6c	0x7793bee0(2006171360)	-	✓	1

Host Behavior

Type	Count
Module	259
Mutex	3
System	3

Process #10: taskeng.exe

ID	10
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {82661305-AA2B-4094-A01F-EC817837FE6B} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 142118, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	161.12s
Return Code	Unknown
PID	3612
Parent PID	868
Bitness	64 Bit

Process #11: explorer.exe

ID	11
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 143074, Reason: Child Process
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	160.16s
Return Code	Unknown
PID	3620
Parent PID	1116
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0xb0000(720896)	0x9000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0xc0000(786432)	0x5000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x3e0efa(4067066)	0x7	✓	1

Host Behavior

Type	Count
Module	311
Process	16794
Mutex	8
-	8
System	158
-	21

Process #12: explorer.exe

ID	12
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\explorer.exe
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 145995, Reason: Child Process
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	157.24s
Return Code	Unknown
PID	3648
Parent PID	1116
Bitness	64 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x50000(327680)	0xc000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x60000(393216)	0x6000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0xff64b790(4284790672)	0x10	✓	1

Host Behavior

Type	Count
Module	79
Process	733

Process #13: flashfxp.exe

ID	13
File Name	c:\program files (x86)\msbuild\flashfxp.exe
Command Line	"C:\Program Files (x86)\MSBuild\flashfxp.exe"
Initial Working Directory	C:\Program Files (x86)\MSBuild\
Monitor Start Time	Start Time: 147050, Reason: Injection
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	156.18s
Return Code	Unknown
PID	2868
Parent PID	1116
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x200000(2097152)	0x9000	✓	1
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x210000(2162688)	0x1000	✓	1
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	0x5	✓	2
Create Remote Thread	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	-	✓	1

Host Behavior

Type	Count
Module	82
Mutex	1
System	1

Process #14: filezilla.exe

ID	14
File Name	c:\program files (x86)\microsoft onedrive\filezilla.exe
Command Line	"C:\Program Files (x86)\Microsoft OneDrive\filezilla.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft OneDrive\
Monitor Start Time	Start Time: 148158, Reason: Injection
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	155.08s
Return Code	Unknown
PID	2932
Parent PID	1116
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x70000(458752)	0x9000	✓	1
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x80000(524288)	0x1000	✓	1
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	0x5	✓	2
Create Remote Thread	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	-	✓	1
Modify Memory	#24: c:\windows\syswow64\explorer.exe	0xea4	0xa0000(655360)	0xb000	✓	1
Modify Memory	#24: c:\windows\syswow64\explorer.exe	0xea4	0xb0000(720896)	0x1000	✓	1
Modify Memory	#24: c:\windows\syswow64\explorer.exe	0xea4	0x7793bee0(2006171360)	0x5	✓	2
Create Remote Thread	#24: c:\windows\syswow64\explorer.exe	0xea4	0x7793bee0(2006171360)	-	✓	1

Host Behavior

Type	Count
Module	182
Mutex	2
System	474

Process #15: ahieedr

ID	15
File Name	c:\users\keecfmwgj\appdata\roaming\ahieedr
Command Line	C:\Users\kEecfMwgj\AppData\Roaming\ahieedr
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 148751, Reason: Child Process
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	154.48s
Return Code	Unknown
PID	3680
Parent PID	3612
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	7
File	3
Environment	1

Process #16: explorer.exe

ID	16
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 149182, Reason: Child Process
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	154.05s
Return Code	Unknown
PID	3688
Parent PID	1116
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x70000(458752)	0x9000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x80000(524288)	0x4000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x3e0efa(4067066)	0x7	✓	1

Host Behavior

Type	Count
Module	114
Process	16115
Mutex	3
System	146
-	6
-	2

Process #17: winscp.exe

ID	17
File Name	c:\program files (x86)\windows nt\winscp.exe
Command Line	"C:\Program Files (x86)\Windows NT\winscp.exe"
Initial Working Directory	C:\Program Files (x86)\Windows NT\
Monitor Start Time	Start Time: 149337, Reason: Injection
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	153.90s
Return Code	Unknown
PID	3012
Parent PID	1116
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x70000(458752)	0x9000	✓	1
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x80000(524288)	0x1000	✓	1
Create Remote Thread	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	-	✓	1
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	0x5	✓	1

Host Behavior

Type	Count
Module	84
Mutex	1
System	1

Process #19: outlook.exe

ID	19
File Name	c:\program files (x86)\windows sidebar\outlook.exe
Command Line	"C:\Program Files (x86)\Windows Sidebar\outlook.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Sidebar\
Monitor Start Time	Start Time: 151402, Reason: Injection
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	151.83s
Return Code	Unknown
PID	2276
Parent PID	1116
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	0x5	✓	2
Create Remote Thread	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	-	✓	1

Host Behavior

Type	Count
Module	84
Mutex	1
System	1

Process #20: explorer.exe

ID	20
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\explorer.exe
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 152121, Reason: Child Process
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	151.11s
Return Code	Unknown
PID	3704
Parent PID	1116
Bitness	64 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x50000(327680)	0x9000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0xe0000(917504)	0x5000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0xff64b790(4284790672)	0x10	✓	1

Host Behavior

Type	Count
Module	58
Process	228

Process #21: smartftp.exe

ID	21
File Name	c:\program files\windows nt\smartftp.exe
Command Line	"C:\Program Files\Windows NT\smartftp.exe"
Initial Working Directory	C:\Program Files\Windows NT\
Monitor Start Time	Start Time: 152133, Reason: Injection
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	151.10s
Return Code	Unknown
PID	2640
Parent PID	1116
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0xe0000(917504)	0x9000	✓	1
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0xf0000(983040)	0x1000	✓	1
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	0x5	✓	1
Create Remote Thread	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	-	✓	1

Host Behavior

Type	Count
Module	84
Mutex	1
System	1

Process #22: thunderbird.exe

ID	22
File Name	c:\program files (x86)\windows defender\thunderbird.exe
Command Line	"C:\Program Files (x86)\Windows Defender\thunderbird.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Defender\
Monitor Start Time	Start Time: 153775, Reason: Injection
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	149.46s
Return Code	Unknown
PID	2648
Parent PID	1116
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0xe0000(917504)	0x9000	✓	1
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0xf0000(983040)	0x1000	✓	1
Modify Memory	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	0x5	✓	2
Create Remote Thread	#11: c:\windows\syswow64\explorer.exe	0xe28	0x7793bee0(2006171360)	-	✓	1

Host Behavior

Type	Count
Module	84
Mutex	1
System	1

Process #23: explorer.exe

ID	23
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 156920, Reason: Child Process
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	146.31s
Return Code	Unknown
PID	3724
Parent PID	1116
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x70000(458752)	0x27000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0xe0000(917504)	0x22000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x3e0efa(4067066)	0x7	✓	1

Host Behavior

Type	Count
Module	189
System	3
Environment	1
File	1610

Process #24: explorer.exe

ID	24
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 161089, Reason: Child Process
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	142.15s
Return Code	Unknown
PID	3744
Parent PID	1116
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x70000(458752)	0xb000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x80000(524288)	0x6000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x3e0efa(4067066)	0x7	✓	1

Host Behavior

Type	Count
Module	342
File	97
Process	10795
Mutex	1
-	3
-	1
System	97

Process #25: explorer.exe

ID	25
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\explorer.exe
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 164274, Reason: Child Process
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	138.96s
Return Code	Unknown
PID	3776
Parent PID	1116
Bitness	64 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x50000(327680)	0xd000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x60000(393216)	0x7000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0xff64b790(4284790672)	0x10	✓	1

Host Behavior

Type	Count
Module	104
File	3
Process	345
System	2

Process #26: explorer.exe

ID	26
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 166176, Reason: Child Process
Unmonitor End Time	End Time: 303234, Reason: Terminated by Timeout
Monitor duration	137.06s
Return Code	Unknown
PID	3792
Parent PID	1116
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x70000(458752)	0xb000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x80000(524288)	0x8000	✓	1
Modify Memory	#2: c:\windows\explorer.exe	0xda8	0x3e0efa(4067066)	0x7	✓	1

Host Behavior

Type	Count
Module	1054
File	471
System	471

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
47ec411eab0aa15619f24caa6256ed4ca5cfc695a26f5b71830b53b07c22b05b	C:\Users\kEecfMwgj\Desktop\8696a4269e30ddb34a7e0e84629ede03.virus.exe, C:\Users\kEecfMwgj\AppData\Roaming\ahieedr	Sample File	278.50 KB	application/vnd.microsoft.portable-executable	Create, Delete, Access, Write	MALICIOUS
6b2757598d730ac5f2c56a1be845369ba88384f034b255ee6bc6a2c34ca086ac	C:\Users\kEecfMwgj\AppData\Roaming\htcufvu	Dropped File	412.28 KB	application/octet-stream	Read, Create, Write, Delete, Access	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\8696a4269e30ddb34a7e0e84629ede03.virus.exe	Sample File	Delete, Access	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\ahieedr	Sample File	Create, Delete, Access, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\ahieedr:Zone.Identifier	Accessed File	Delete, Access	CLEAN
C:\Windows\system32\advapi32.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\htcufvu	Dropped File	Read, Create, Write, Delete, Access	CLEAN
C:\Program Files (x86)\Internet Explorer\iexplore.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\MSBuild\flashfxp.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft OneDrive\filezilla.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows NT\winscp.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Sidebar\outlook.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows NT\smartftp.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Defender\thunderbird.exe	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\explorer.exe	Accessed File	Access	CLEAN
0	Accessed File	Delete, Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\A5AF	Accessed File	Create, Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://rsuehfidvdkfvk.top	-	5.188.88.118	-	POST	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
rsuehfidvdkfvk.top	5.188.88.118	-	HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
5.188.88.118	rsuehfidvdkfvk.top	Russia	DNS, HTTP, TCP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
7C2D5ED2D6B71DDF065E08EDB38519078443A5AF	access	explorer.exe	CLEAN
opera_shared_counter	access	explorer.exe	CLEAN
A51BEC40CF6D8BD76CA31608E39B8662	access	iexplore.exe	CLEAN
3614EE7DCF67EA55E5FA4BF08892DDA7	access	iexplore.exe	CLEAN
79FF8A9E04191F68E84F55B788C3DB95	access	iexplore.exe	CLEAN
5C7B8ACCFA112F039BCB37749FCB206B	access	iexplore.exe	CLEAN
093E748EDFA3BC8C486A602DB4AE042E	access	flashfxp.exe	CLEAN
F086C931E57676B770EA8825FF5EE63F	access	filezilla.exe	CLEAN
9A13379D174D40744C105A1B640A414C	access	winscp.exe	CLEAN
DD9336F98CA7F483A811DFD312803FE9	access	outlook.exe	CLEAN
89CC2A001C7D1D32AEC982DE2C008933	access	smartftp.exe	CLEAN
0CD685E8677D85A7CBD4766477F43A23	access	thunderbird.exe	CLEAN
84CFF8068531CDBB2CA4C9A315CFD60F	access	iexplore.exe	CLEAN
2EFA102D67FBFA95AE7895A49D7EA40D	access	iexplore.exe	CLEAN
E5AED93F4D1BFA97BD58091959CE09A1	access	filezilla.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\IDE	access	8696a4269e30ddb34a7e0e84629ede03.virus.exe	CLEAN
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\SCSI	access	8696a4269e30ddb34a7e0e84629ede03.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\557014fe	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\634642a8	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Mozilla	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Mozilla	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Server	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Server	read, access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Server	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Server	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Port	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Port	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Server	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Server	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Server	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Server	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Martin Prikryl	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Martin Prikryl	access	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
8696a4269e30ddb34a7e0e84629ede03.virus.exe	"C:\Users\kEecfMwgj\Desktop\8696a4269e30ddb34a7e0e84629ede03.virus.exe"	MALICIOUS
ahieedr	C:\Users\kEecfMwgj\AppData\Roaming\ahieedr	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
explorer.exe	C:\Windows\SysWOW64\explorer.exe	SUSPICIOUS
filezilla.exe	"C:\Program Files (x86)\Microsoft OneDrive\filezilla.exe"	SUSPICIOUS
explorer.exe	C:\Windows\explorer.exe	CLEAN
iexplore.exe	"C:\Program Files (x86)\Internet Explorer\iexplore.exe" about:blank	CLEAN
iexplore.exe	"C:\Program Files (x86)\Internet Explorer\iexplore.exe" SCODEF:1432 CREDAT:14337	CLEAN
taskeng.exe	taskeng.exe {82661305-AA2B-4094-A01F-EC817837FE6B} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]	CLEAN
flashfxp.exe	"C:\Program Files (x86)\MSBuild\flashfxp.exe"	CLEAN

Process Name	Commandline	Verdict
winscp.exe	"C:\Program Files (x86)\Windows NT\winscp.exe"	CLEAN
outlook.exe	"C:\Program Files (x86)\Windows Sidebar\outlook.exe"	CLEAN
smartftp.exe	"C:\Program Files\Windows NT\smartftp.exe"	CLEAN
thunderbird.exe	"C:\Program Files (x86)\Windows Defender\thunderbird.exe"	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Malware	SmokeLoaderStrings	SmokeLoader strings	Function Strings	function_strings_process_2.txt	Downloader	5/5

Antivirus (1)

File Type	Threat Name	File Name	Verdict
Sample File	Gen:Variant.Babar.29261	C:\Users\kEecfMwgj\Desktop\8696a4269e30ddb34a7e0e84629ede03.virus.exe	MALICIOUS

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	4.3.1
Dynamic Engine Version	4.3.1 / 11/09/2021 04:55
Static Engine Version	4.3.1.0 / 2021-11-09 04:00:13
AV Exceptions Version	4.3.1.6 / 2021-09-21 13:25:28
Link Detonation Heuristics Version	4.3.1.23 / 2021-11-15 15:11:35
Signature Trust Store Version	4.3.1.6 / 2021-09-21 13:25:28
VMRay Threat Identifiers Version	4.3.1.22 / 2021-11-15 15:04:23
YARA Built-in Ruleset Version	4.3.1.20

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-11-18 10:22:36+00:00
Built-in AV Database Records	10503561

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