MALICIOUS

Classifications: Spyware

Threat Names: Agent Tesla v3 | Mal/Generic-S | Trojan.GenericKD.37609257

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe**
ID	#969380
MD5	93445df2c96362810e0395c5c867700e
SHA1	645f936406b04fbfb737bbffb5678d5255c6ec34
SHA256	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa
File Size	384.00 KB
Report Created	2021-09-28 15:00 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (21 rules, 46 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
	• Rule "AgentTesla_StringDecryption_v3" from ruleset "Malware" has matched on a memory dump for (process #28) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe.			
4/5	Defense Evasion	Tries to disable antivirus software	2	-
	• (Process #25) sc.exe stops a service related to Windows Defender via ControlService (API). • (Process #9) advancedrun.exe stops a service related to Windows Defender via the sc.exe utility.			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected the sample itself as "Trojan.GenericKD.37609257".			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
2/5	Discovery	Executes WMI query	4	-
	• (Process #3) powershell.exe executes WMI query: Select * from Win32_PingStatus where ((Address='www.bing.com') And TimeToLive=80 And BufferSize=32). • (Process #4) powershell.exe executes WMI query: Select * from Win32_PingStatus where ((Address='www.facebook.com') And TimeToLive=80 And BufferSize=32). • (Process #2) powershell.exe executes WMI query: Select * from Win32_PingStatus where ((Address='www.google.com') And TimeToLive=80 And BufferSize=32). • (Process #8) powershell.exe executes WMI query: Select * from Win32_PingStatus where ((Address='www.twitter.com') And TimeToLive=80 And BufferSize=32).			
2/5	Privilege Escalation	Enables critical process privilege	2	-
	• (Process #9) advancedrun.exe enables critical process privilege "SeImpersonatePrivilege". • (Process #26) advancedrun.exe enables critical process privilege "SeImpersonatePrivilege".			
2/5	Hide Tracks	Deletes file after execution	1	-
	• (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe deletes executed executable "c:\users\keecfmwgj\appdata\local\temp\advancedrun.exe".			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe modifies memory of (process #28) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe alters context of (process #28) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe.			
1/5	Hide Tracks	Creates process with hidden window	8	-
	• (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe starts (process #3) powershell.exe with a hidden window. • (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe starts (process #4) powershell.exe with a hidden window. • (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe starts (process #8) powershell.exe with a hidden window. • (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe starts (process #9) advancedrun.exe with a hidden window. • (Process #9) advancedrun.exe starts (process #25) sc.exe with a hidden window. • (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe starts (process #26) advancedrun.exe with a hidden window. • (Process #26) advancedrun.exe starts (process #27) powershell.exe with a hidden window. • (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe starts (process #28) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe with a hidden window.			

Score	Category	Operation	Count	Classification
1/5	Privilege Escalation	Enables process privilege	4	-
	• (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe enables process privilege "SeDebugPrivilege". • (Process #9) advancedrun.exe enables process privilege "SeDebugPrivilege". • (Process #26) advancedrun.exe enables process privilege "SeDebugPrivilege". • (Process #28) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Enumerates running processes	3	-
	• (Process #9) advancedrun.exe enumerates running processes. • (Process #26) advancedrun.exe enumerates running processes. • (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe enumerates running processes.			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe creates mutex with name "Thcyqfmzh".			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe reads from (process #28) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Network Connection	Performs DNS request	5	-
	• (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe resolves host name "store2.gofile.io" to IP "31.14.69.10". • (Process #4) powershell.exe resolves host name "www.facebook.com" to IP "69.171.250.35". • (Process #2) powershell.exe resolves host name "www.google.com" to IP "172.217.18.100". • (Process #3) powershell.exe resolves host name "www.bing.com" to IP "131.253.33.200". • (Process #8) powershell.exe resolves host name "www.twitter.com" to IP "104.244.42.129".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe opens an outgoing TCP connection to host "31.14.69.10:443".			
1/5	Execution	Drops PE file	1	-
	• (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe drops file "C:\Users\kEecfMwgj\AppData\Local\Temp\AdvancedRun.exe".			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\Users\kEecfMwgj\AppData\Local\Temp\AdvancedRun.exe".			
1/5	Execution	Executes itself	1	-
	• (Process #1) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe.			
1/5	Obfuscation	Resolves API functions dynamically	5	-
	• (Process #4) powershell.exe resolves 50 API functions by name. • (Process #3) powershell.exe resolves 50 API functions by name. • (Process #2) powershell.exe resolves 50 API functions by name. • (Process #8) powershell.exe resolves 50 API functions by name. • (Process #28) ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe resolves 49 API functions by name.			

Score	Category	Operation	Count	Classification
-	Trusted	Known clean file	1	-
	• File "C:\Users\kEecfMwgj\AppData\Local\Temp\AdvancedRun.exe" is a known clean file.			

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			#T1143 Hidden Window		#T1057 Process Discovery					#T1489 Service Stop
				#T1089 Disabling Security Tools							
				#T1045 Software Packing							

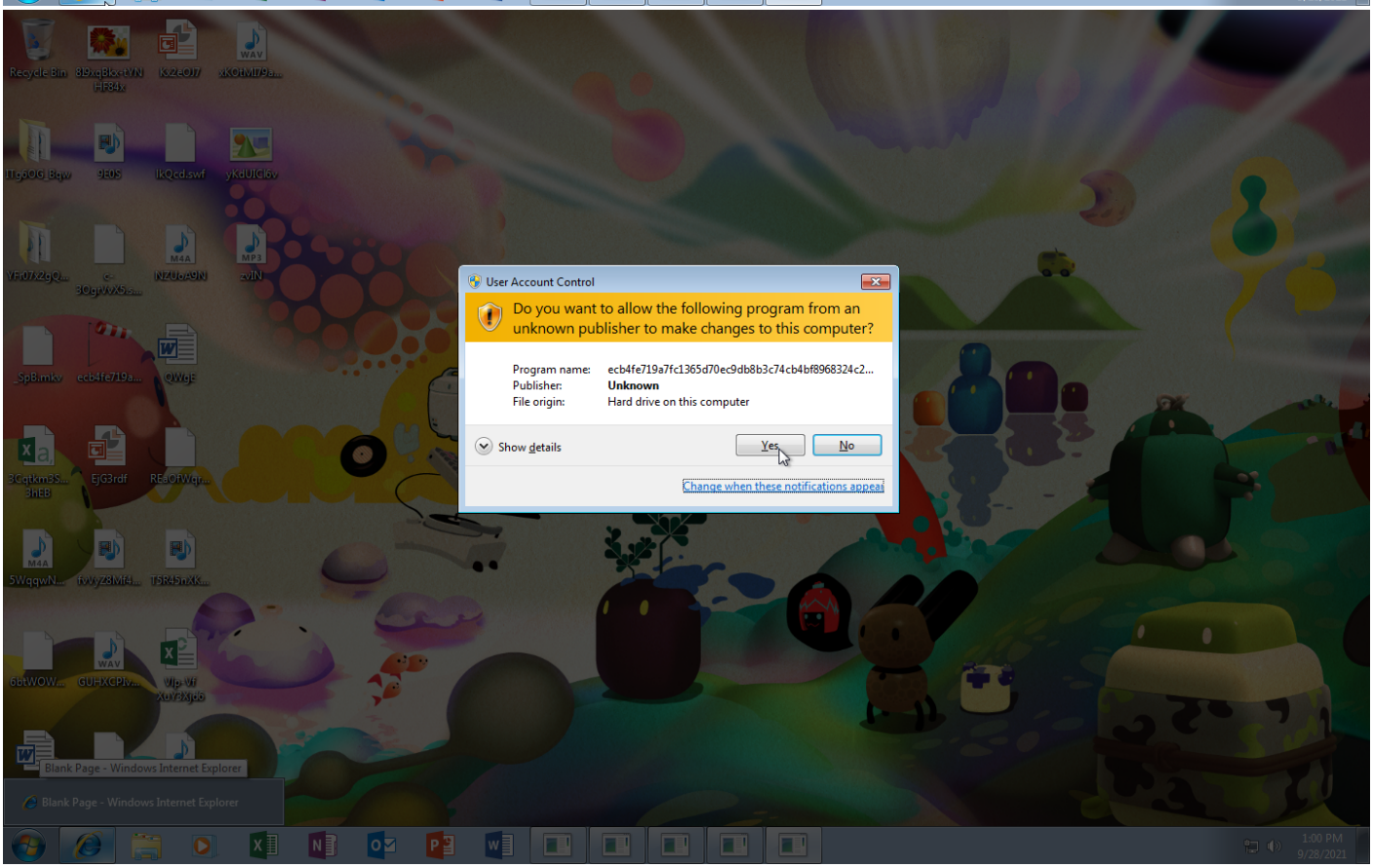
Sample Information

ID	#969380
MD5	93445df2c96362810e0395c5c867700e
SHA1	645f936406b04fbfb737bbffb5678d5255c6ec34
SHA256	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa
SSDeep	3072:qx4Jmb4+WHRWm+3TkQ/b62tN+mbjOKC1g2L4o:qvb4+WZQJ0
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe
File Size	384.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 15:00 (UTC+2)
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	1


Blank Page - Windows Internet Explorer
1:00 PM
9/28/2021


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c2...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear
Blank Page - Windows Internet Explorer

Screenshots truncated

NETWORK

General

3.08 KB total sent

500.74 KB total received

1 ports 443

2 contacted IP addresses

4 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

33 DNS requests for 5 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

1 sessions, 3.08 KB sent, 500.74 KB received

HTTP Requests

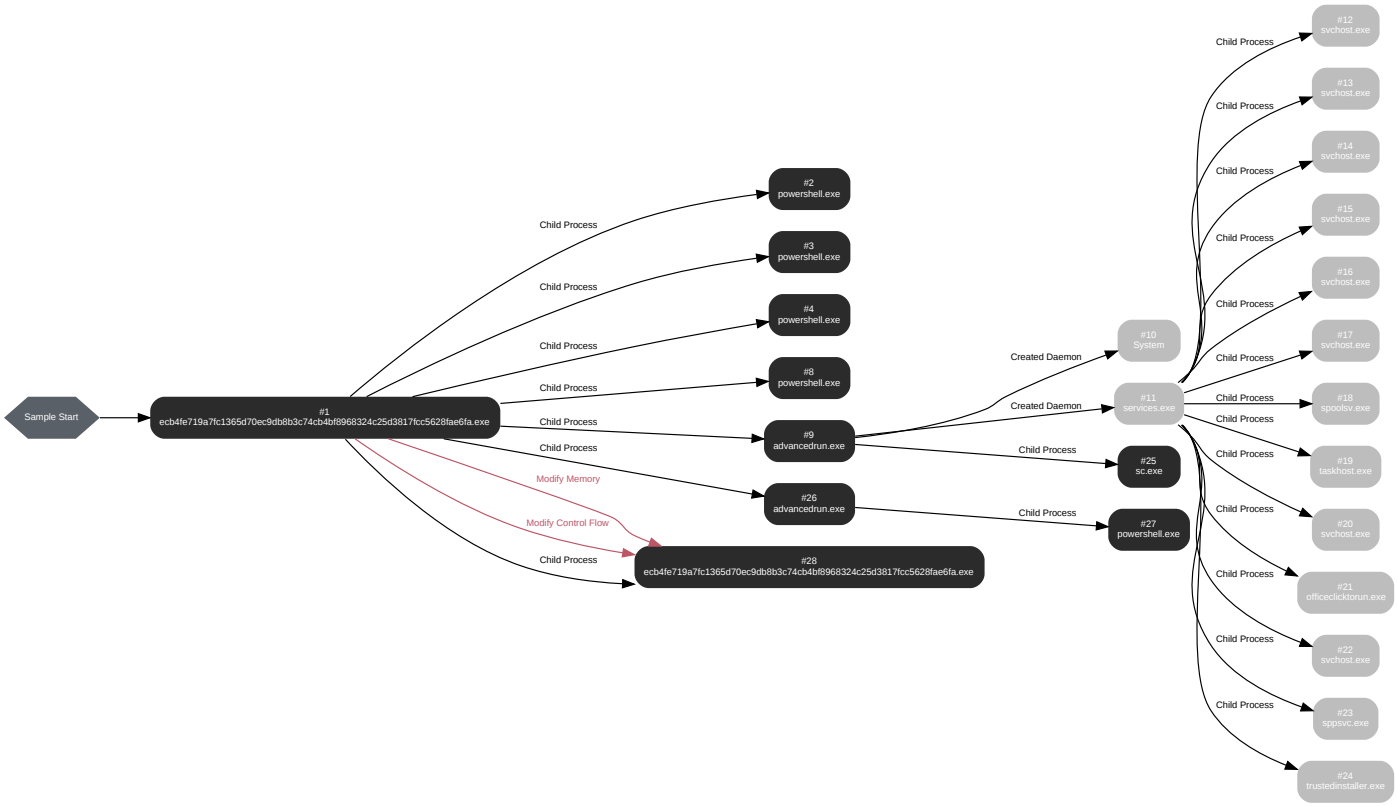
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
	www.google.com	-	-		0 bytes	NA
	www.bing.com	-	-		0 bytes	NA
	www.facebook.com	-	-		0 bytes	NA
	www.twitter.com	-	-		0 bytes	NA
GET	https://store2.gofile.io/download/956f4086-c03d-4dbb-9647-f6db09f6a8b5/lyybawggybiqbtxofebfdynt.dll	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	store2.gofile.io	NoError	31.14.69.10		NA
-	www.facebook.com	-	69.171.250.35		NA
-	www.google.com	-	172.217.18.100		NA
-	www.bing.com	-	131.253.33.200, 13.107.22.200		NA
-	www.twitter.com	-	104.244.42.129, 104.244.42.65		NA

BEHAVIOR

Process Graph



Process #1: ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 40856, Reason: Analysis Target
Unmonitor End Time	End Time: 254951, Reason: Terminated
Monitor duration	214.09s
Return Code	0
PID	3792
Parent PID	1096
Bitness	32 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\Temp\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	384.00 KB	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa	✕
-	8.03 KB	790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	✕
C:\Users\kEecfMwgj\AppData\Local\Temp\AdvancedRun.exe	88.87 KB	29ae7b30ed8394c509c561f6117ea671ec412da50d435099756bbb257fafb10b	✕
-	108.45 KB	f8214daf0e6176a9b7ee15ca3588130e41313abb6cd0bc10b55c0d4509790a72	✕

Host Behavior

Type	Count
Registry	53
Process	107
File	29
Module	48
System	114
Window	13
-	10
User	1
Environment	8
Mutex	1
-	3
-	7

Network Behavior

Type	Count
HTTPS	1
DNS	1
TCP	1

Process #2: powershell.exe

ID	2
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Test-Connection www.google.com
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81658, Reason: Child Process
Unmonitor End Time	End Time: 144445, Reason: Terminated
Monitor duration	62.79s
Return Code	0
PID	3860
Parent PID	3792
Bitness	32 Bit

Host Behavior

Type	Count
System	30
Module	56
File	558
Environment	50
Registry	65
-	62
COM	53
-	4

Network Behavior

Type	Count
DNS	8

Process #3: powershell.exe

ID	3
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Test-Connection www.bing.com
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81667, Reason: Child Process
Unmonitor End Time	End Time: 143769, Reason: Terminated
Monitor duration	62.10s
Return Code	0
PID	3868
Parent PID	3792
Bitness	32 Bit

Host Behavior

Type	Count
System	30
Module	56
File	542
Environment	49
Registry	65
-	62
COM	53
-	4

Network Behavior

Type	Count
DNS	8

Process #4: powershell.exe

ID	4
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Test-Connection www.facebook.com
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81971, Reason: Child Process
Unmonitor End Time	End Time: 144694, Reason: Terminated
Monitor duration	62.72s
Return Code	0
PID	3896
Parent PID	3792
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	13.51 KB	966575dd0852d7b23ba7523b8d158631fe4581af6212858e24122e9ea50cfbbc	✕

Host Behavior

Type	Count
System	30
Module	56
File	548
Environment	49
Registry	65
-	62
COM	53
-	4

Network Behavior

Type	Count
DNS	8

Process #8: powershell.exe

ID	8
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Test-Connection www.twitter.com
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 143738, Reason: Child Process
Unmonitor End Time	End Time: 164453, Reason: Terminated
Monitor duration	20.71s
Return Code	0
PID	2704
Parent PID	3792
Bitness	32 Bit

Host Behavior

Type	Count
System	25
Module	56
File	315
Environment	49
Registry	55
-	57
COM	53
-	4

Network Behavior

Type	Count
DNS	8

Process #9: advancedrun.exe

ID	9
File Name	c:\users\keecfmwgj\appdata\local\temp\advancedrun.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\Temp\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\sc.exe" /WindowState 0 /CommandLine "stop WinDefend" /StartDirectory "" /RunAs 8 /Run
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 236432, Reason: Child Process
Unmonitor End Time	End Time: 245192, Reason: Terminated
Monitor duration	8.76s
Return Code	0
PID	3536
Parent PID	3792
Bitness	32 Bit

Host Behavior

Type	Count
Module	233
System	2
Process	457
User	2
-	28
Environment	1
-	4

Process #10: System

ID	10
File Name	System
Command Line	-
Initial Working Directory	-
Monitor Start Time	Start Time: 237313, Reason: Created Daemon
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	4
Parent PID	18446744073709551615
Bitness	64 Bit

Process #11: services.exe

ID	11
File Name	c:\windows\system32\services.exe
Command Line	C:\Windows\system32\services.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237313, Reason: Created Daemon
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	464
Parent PID	368
Bitness	64 Bit

Process #12: svchost.exe

ID	12
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k DcomLaunch
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237313, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	584
Parent PID	464
Bitness	64 Bit

Process #13: svchost.exe

ID	13
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k RPCSS
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237313, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	648
Parent PID	464
Bitness	64 Bit

Process #14: svchost.exe

ID	14
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237313, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	696
Parent PID	464
Bitness	64 Bit

Process #15: svchost.exe

ID	15
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237313, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	776
Parent PID	464
Bitness	64 Bit

Process #16: svchost.exe

ID	16
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalService
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237313, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	1004
Parent PID	464
Bitness	64 Bit

Process #17: svchost.exe

ID	17
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k NetworkService
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237313, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	816
Parent PID	464
Bitness	64 Bit

Process #18: spoolsv.exe

ID	18
File Name	c:\windows\system32\spoolsv.exe
Command Line	C:\Windows\System32\spoolsv.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237313, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	1164
Parent PID	464
Bitness	64 Bit

Process #19: taskhost.exe

ID	19
File Name	c:\windows\system32\taskhost.exe
Command Line	"taskhost.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237313, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	1200
Parent PID	464
Bitness	64 Bit

Process #20: svchost.exe

ID	20
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237313, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	1224
Parent PID	464
Bitness	64 Bit

Process #21: officeclicktorun.exe

ID	21
File Name	c:\program files\common files\microsoft shared\clicktorun\officeclicktorun.exe
Command Line	"C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe" /service
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237313, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	1476
Parent PID	464
Bitness	64 Bit

Process #22: svchost.exe

ID	22
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237313, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	556
Parent PID	464
Bitness	64 Bit

Process #23: sppsvc.exe

ID	23
File Name	c:\windows\system32\sppsvc.exe
Command Line	C:\Windows\system32\sppsvc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237313, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.93s
Return Code	Unknown
PID	2184
Parent PID	464
Bitness	64 Bit

Process #24: trustedinstaller.exe

ID	24
File Name	c:\windows\servicing\trustedinstaller.exe
Command Line	C:\Windows\servicing\TrustedInstaller.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237420, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	51.83s
Return Code	Unknown
PID	3452
Parent PID	464
Bitness	64 Bit

Process #25: sc.exe

ID	25
File Name	c:\windows\system32\sc.exe
Command Line	"C:\Windows\System32\sc.exe" stop WinDefend
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 243797, Reason: Child Process
Unmonitor End Time	End Time: 246379, Reason: Terminated
Monitor duration	2.58s
Return Code	1062
PID	3576
Parent PID	3536
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	1
File	3
-	3

Process #26: advancedrun.exe

ID	26
File Name	c:\users\keecfmwgj\appdata\local\temp\advancedrun.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\Temp\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" /WindowState 0 /CommandLine "rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse" /StartDirectory "" /RunAs 8 /Run
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 244294, Reason: Child Process
Unmonitor End Time	End Time: 247426, Reason: Terminated
Monitor duration	3.13s
Return Code	0
PID	3596
Parent PID	3792
Bitness	32 Bit

Host Behavior

Type	Count
Module	235
System	2
Process	463
User	2
-	28
Environment	1
-	4

Process #27: powershell.exe

ID	27
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse
Initial Working Directory	C:\Windows\System32\WindowsPowerShell\v1.0\
Monitor Start Time	Start Time: 245853, Reason: Child Process
Unmonitor End Time	End Time: 280180, Reason: Terminated
Monitor duration	34.33s
Return Code	0
PID	2040
Parent PID	3596
Bitness	64 Bit

Host Behavior

Type	Count
System	14
Module	4
File	412
Environment	19
Registry	31
-	23

Process #28: ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe

ID	28
File Name	c:\users\keecfmwgj\appdata\local\temp\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe
Command Line	C:\Users\kEecfMwgj\AppData\Local\Temp\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 252730, Reason: Child Process
Unmonitor End Time	End Time: 289247, Reason: Terminated by Timeout
Monitor duration	36.52s
Return Code	Unknown
PID	3720
Parent PID	3792
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\keecfmwgj\desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	0xed4	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	0xed4	0x402000(4202496)	0x34c00	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	0xed4	0x438000(4423680)	0x600	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	0xed4	0x43a000(4431872)	0x200	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	0xed4	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	0xed4 / 0xe44		-	✓	1

Host Behavior

Type	Count
Registry	44
File	19
Module	63
Window	3
System	5
User	2
-	25
COM	34

Type	Count
Environment	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa	C:\Users\kEecfMwgj\AppData\Local\Temp\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe, C:\Users\kEecfMwgj\Desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	Sample File	384.00 KB	application/vnd.microsoft.portable-executable	Write, Create, Access	MALICIOUS
29ae7b30ed8394c509c561f6117ea671ec412da50d435099756bbb257fafb10b	C:\Users\kEecfMwgj\AppData\Local\Temp\AdvancedRun.exe	Dropped File	88.87 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	SUSPICIOUS
966575dd0852d7b23ba7523b8d158631fe4581af6212858e24122e9ea50cfbbc	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	Dropped File	13.51 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	8.03 KB	application/octet-stream	-	CLEAN
f8214daf0e6176a9b7ee15ca3588130e41313abb6cd0bc10b55c0d4509790a72	c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	108.45 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
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:\Users\kEecfMwgj\Desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe.config	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\%SystemRoot%\system32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Windows	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Read, Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	Dropped File	Write, Read, Create, Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Accessed File	Read, Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.psm1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.cdxml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.ni.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Read, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psm1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.cdxml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.xaml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.ni.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Accessed File	Read, Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	Accessed File	Read, Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Format.ps1xml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Resource.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psm1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.ni.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.psm1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.cdxml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.ni.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\en-US\Microsoft.PowerShell.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\en\Microsoft.PowerShell.Management.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Commands.Management.dll\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSWorkflow\PSWorkflow.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSWorkflowUtility\PSWorkflowUtility.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetworkSwitchManager\NetworkSwitchManager.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\PSDesiredStateConfiguration.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\PSScheduledJob.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.LocalAccounts\1.0.0.0\Microsoft.PowerShell.LocalAccounts.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE\ISE.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\en-US\Microsoft.PowerShell.Utility.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\en\Microsoft.PowerShell.Utility.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Commands.Utility.dll\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Utility	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Utility	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Utility	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	Accessed File	Read, Access	CLEAN
C:\Users\kEecfMwgj\Desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	Sample File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\AdvancedRun.exe	Dropped File	Write, Create, Delete, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Local\Temp\AdvancedRun.cfg	Accessed File	Read, Access	CLEAN
C:\Program Files (x86)\Internet Explorer\iexplore.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Defender\linegood.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Defender\no_nothing.exe	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\form remember evening.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Reference Assemblies\study-reality-mission.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Portable Devices\field.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Defender\apply-wear-benefit.exe	Accessed File	Access	CLEAN
C:\Program Files\Common Files\law-stay.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Media Player\wife_heat.exe	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\interview nothing work.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Journal\your hit sense.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Photo Viewer\leftparticularly.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Mail\must-issue.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows NT\call_order_arrive.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Sidebar\natural_reach_decide.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Reference Assemblies\another great.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Sidebar\bill order.exe	Accessed File	Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.google.com	-	-	-	-	CLEAN
http://www.bing.com	-	-	-	-	CLEAN
http://www.facebook.com	-	-	-	-	CLEAN
http://www.twitter.com	-	-	-	-	CLEAN
https://store2.gofile.io/download/956f4086-c03d-4dbb-9647-f6db09f6a8b5/lyybawggybiqbtxofebfdynt.dll	-	31.14.69.10	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
www.google.com	172.217.18.100	-	DNS, HTTP	CLEAN
www.bing.com	131.253.33.200, 13.107.22.200	-	DNS, HTTP	CLEAN
www.facebook.com	69.171.250.35	-	DNS, HTTP	CLEAN
www.twitter.com	104.244.42.65, 104.244.42.129	-	DNS, HTTP	CLEAN
twitter.com	-	-	HTTP	CLEAN
store2.gofile.io	31.14.69.10	-	DNS, HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
31.14.69.10	store2.gofile.io	France	DNS, HTTPS, TCP	CLEAN
131.253.33.200	www.bing.com, www-bing-com.dual-a-0001.a-msedge.net, dual-a-0001.dc-msedge.net, a-0001.a-afdentry.net.trafficmanager.net	United States	DNS	CLEAN
13.107.22.200	www.bing.com, www-bing-com.dual-a-0001.a-msedge.net, dual-a-0001.dc-msedge.net, a-0001.a-afdentry.net.trafficmanager.net	United States	DNS	CLEAN
172.217.18.100	www.google.com	United States	DNS	CLEAN
69.171.250.35	www.facebook.com, star-mini.c10r.facebook.com	United States	DNS	CLEAN
104.244.42.129	twitter.com, www.twitter.com	United States	DNS	CLEAN
104.244.42.65	twitter.com, www.twitter.com	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Thcyqfmzh	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment__PSLockdownPolicy	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine\ApplicationBase	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe, powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\WMIDisableCOMSecurity	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe, powershell.exe	CLEAN
HKEY_PERFORMANCE_DATA	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe, powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseHttpPipeliningAndBufferPooling	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseHttpPipeliningAndBufferPooling	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseSafeSynchronousClose	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseSafeSynchronousClose	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseStrictRfcInterimResponseHandling	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictRfcInterimResponseHandling	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowDangerousUnicodeDecompositions	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowDangerousUnicodeDecompositions	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.UseStrictIPv6AddressParsing	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictIPv6AddressParsing	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowAllUriEncodingExpansion	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowAllUriEncodingExpansion	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SystemDefaultTlsVersions	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.RequireCertificateEKUs	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\RequireCertificateEKUs	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_CURRENT_USER	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	CLEAN

Process

Process Name	Commandline	Verdict
ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	"C:\Users\kEecfMwgj\Desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe"	MALICIOUS
advancedrun.exe	"C:\Users\kEecfMwgj\AppData\Local\Temp\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\sc.exe" /WindowState 0 /CommandLine "stop WinDefend" /StartDirectory "" /RunAs 8 /Run	MALICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Test-Connection www.google.com	SUSPICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Test-Connection www.bing.com	SUSPICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Test-Connection www.facebook.com	SUSPICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Test-Connection www.twitter.com	SUSPICIOUS
sc.exe	"C:\Windows\System32\sc.exe" stop WinDefend	SUSPICIOUS
advancedrun.exe	"C:\Users\kEecfMwgj\AppData\Local\Temp\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" /WindowState 0 /CommandLine "rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse" /StartDirectory "" /RunAs 8 /Run	SUSPICIOUS
ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	C:\Users\kEecfMwgj\AppData\Local\Temp\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.exe	SUSPICIOUS
System	-	CLEAN
services.exe	C:\Windows\system32\services.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k RPCSS	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalService	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k NetworkService	CLEAN
spoolsv.exe	C:\Windows\System32\spoolsv.exe	CLEAN
taskhost.exe	"taskhost.exe"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork	CLEAN
officeclicktorun.exe	"C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe" /service	CLEAN

Process Name	Commandline	Verdict
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation	CLEAN
sppsvc.exe	C:\Windows\system32\sppsvc.exe	CLEAN
trustedinstaller.exe	C:\Windows\servicing\TrustedInstaller.exe	CLEAN
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	AgentTesla_StringDecryption_v3	Agent Tesla v3 string decryption	Memory Dump	-	Spyware	5/5

Antivirus (1)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKD.37609257	C:\Users\kEecfMwgj\Desktop\ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa.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	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

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

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	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