MALICIOUS

Classifications: Injector

Threat Names: Mal/HTMLGen-A | Gen:Variant.Bulz.604474

Verdict Reason: -

Sample Type	**Windows DLL (x86-32)**
File Name	**b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll**
ID	#2780822
MD5	b9c2828409584dcb2d0a968f1968e00f
SHA1	28f7cdd53a24dd293f4d8233844fe4b609681a82
SHA256	b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969
File Size	378.00 KB
Report Created	2021-09-27 23:15 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (22 rules, 204 matches)

Score	Category	Operation	Count	Classification
4/5	Reputation	Contacts known malicious URL	3	-
	• Reputation analysis labels the URL "https://24.229.150.54/t4" which was contacted by (process #23) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "https://140.82.49.12/t4" which was contacted by (process #49) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "https://96.37.113.36/t4" which was contacted by (process #49) explorer.exe as "Mal/HTMLGen-A".			
4/5	Reputation	Contacts known malicious IP address	1	-
	• Reputation analysis labels the contacted IP address 140.82.49.12 as "Mal/HTMLGen-A".			
4/5	Injection	Writes into the memory of another process	18	Injector
	• (Process #7) dadjtxjf.exe modifies memory of (process #20) explorer.exe. • (Process #17) dadjtxjf.exe modifies memory of (process #21) explorer.exe. • (Process #3) dadjtxjf.exe modifies memory of (process #22) explorer.exe. • (Process #5) dadjtxjf.exe modifies memory of (process #23) explorer.exe. • (Process #12) dadjtxjf.exe modifies memory of (process #24) explorer.exe. • (Process #18) dadjtxjf.exe modifies memory of (process #25) explorer.exe. • (Process #9) dadjtxjf.exe modifies memory of (process #26) explorer.exe. • (Process #4) dadjtxjf.exe modifies memory of (process #27) explorer.exe. • (Process #16) dadjtxjf.exe modifies memory of (process #28) explorer.exe. • (Process #14) dadjtxjf.exe modifies memory of (process #29) explorer.exe. • (Process #15) dadjtxjf.exe modifies memory of (process #30) explorer.exe. • (Process #2) dadjtxjf.exe modifies memory of (process #31) explorer.exe. • (Process #8) dadjtxjf.exe modifies memory of (process #32) explorer.exe. • (Process #19) dadjtxjf.exe modifies memory of (process #33) explorer.exe. • (Process #11) dadjtxjf.exe modifies memory of (process #34) explorer.exe. • (Process #6) dadjtxjf.exe modifies memory of (process #35) explorer.exe. • (Process #13) dadjtxjf.exe modifies memory of (process #36) explorer.exe. • (Process #48) regsvr32.exe modifies memory of (process #49) explorer.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected a memory dump of (process #10) dadjtxjf.exe as "Gen:Variant.Bulz.604474".			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	2	-
	• (Process #23) explorer.exe tries to detect antivirus software via WMI query: "SELECT * FROM AntiVirusProduct". • (Process #49) explorer.exe tries to detect antivirus software via WMI query: "SELECT * FROM AntiVirusProduct".			
3/5	Defense Evasion	Modifies Windows Defender configuration	2	-
	• (Process #50) reg.exe adds exclusion for Windows Defender. • (Process #51) reg.exe adds exclusion for Windows Defender.			
2/5	Anti Analysis	Delays execution	2	-
	• (Process #23) explorer.exe has a thread which sleeps more than 5 minutes. • (Process #49) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Discovery	Queries OS version via WMI	2	-

Score	Category	Operation	Count	Classification
	• (Process #23) explorer.exe queries OS version via WMI. • (Process #49) explorer.exe queries OS version via WMI.			
2/5	Discovery	Executes WMI query	17	-
	• (Process #23) explorer.exe executes WMI query: SELECT * FROM Win32_OperatingSystem. • (Process #23) explorer.exe executes WMI query: SELECT * FROM AntiVirusProduct. • (Process #23) explorer.exe executes WMI query: SELECT * FROM Win32_Processor. • (Process #23) explorer.exe executes WMI query: select * from Win32_ComputerSystem. • (Process #23) explorer.exe executes WMI query: select * from Win32_Bios. • (Process #23) explorer.exe executes WMI query: select * from Win32_DiskDrive. • (Process #23) explorer.exe executes WMI query: select * from Win32_PhysicalMemory. • (Process #23) explorer.exe executes WMI query: select Caption,Description,Vendor,Version,InstallDate,InstallSource,PackageName from Win32_Product. • (Process #23) explorer.exe executes WMI query: select Caption,Description,DeviceID,Manufacturer,Name,PNPDeviceID,Service,Status from Win32_PnPEntity. • (Process #49) explorer.exe executes WMI query: SELECT * FROM Win32_OperatingSystem. • (Process #49) explorer.exe executes WMI query: SELECT * FROM AntiVirusProduct. • (Process #49) explorer.exe executes WMI query: SELECT * FROM Win32_Processor. • (Process #49) explorer.exe executes WMI query: select * from Win32_ComputerSystem. • (Process #49) explorer.exe executes WMI query: select * from Win32_Bios. • (Process #49) explorer.exe executes WMI query: select * from Win32_DiskDrive. • (Process #49) explorer.exe executes WMI query: select * from Win32_PhysicalMemory. • (Process #49) explorer.exe executes WMI query: select Caption,Description,Vendor,Version,InstallDate,InstallSource,PackageName from Win32_Product.		
2/5	Discovery	Collects hardware properties	2	-
	• (Process #23) explorer.exe queries hardware properties via WMI. • (Process #49) explorer.exe queries hardware properties via WMI.			
2/5	Discovery	Reads network adapter information	2	-
	• (Process #45) ipconfig.exe reads the network adapters' addresses by API. • (Process #65) ipconfig.exe reads the network adapters' addresses by API.			
2/5	Discovery	Collects BIOS properties	2	-
	• (Process #23) explorer.exe queries BIOS properties via WMI. • (Process #49) explorer.exe queries BIOS properties via WMI.			
2/5	Masquerade	Creates a new process from a system binary	1	-
	• (Process #7) dadjtxjf.exe creates a new explorer.exe process.			
2/5	Task Scheduling	Schedules task	1	-
	• Schedules task for command "regsvr32.exe", to be triggered by Time. Task has been rescheduled by the analyzer.			
2/5	Task Scheduling	Schedules task via schtasks	1	-
	• Schedules task "lmtrjjbrh" via the schtasks command line utility.			
1/5	Discovery	Enumerates running processes	21	-

Score	Category	Operation	Count	Classification
		• (Process #7) dadjtxjf.exe enumerates running processes. • (Process #17) dadjtxjf.exe enumerates running processes. • (Process #3) dadjtxjf.exe enumerates running processes. • (Process #5) dadjtxjf.exe enumerates running processes. • (Process #12) dadjtxjf.exe enumerates running processes. • (Process #4) dadjtxjf.exe enumerates running processes. • (Process #2) dadjtxjf.exe enumerates running processes. • (Process #19) dadjtxjf.exe enumerates running processes. • (Process #15) dadjtxjf.exe enumerates running processes. • (Process #18) dadjtxjf.exe enumerates running processes. • (Process #13) dadjtxjf.exe enumerates running processes. • (Process #16) dadjtxjf.exe enumerates running processes. • (Process #10) dadjtxjf.exe enumerates running processes. • (Process #14) dadjtxjf.exe enumerates running processes. • (Process #11) dadjtxjf.exe enumerates running processes. • (Process #9) dadjtxjf.exe enumerates running processes. • (Process #6) dadjtxjf.exe enumerates running processes. • (Process #8) dadjtxjf.exe enumerates running processes. • (Process #23) explorer.exe enumerates running processes. • (Process #48) regsvr32.exe enumerates running processes. • (Process #49) explorer.exe enumerates running processes.		
1/5	Hide Tracks	Creates process with hidden window	41	-

Score	Category	Operation	Count	Classification
		• (Process #7) dadjtxjf.exe starts (process #20) explorer.exe with a hidden window. • (Process #17) dadjtxjf.exe starts (process #21) explorer.exe with a hidden window. • (Process #3) dadjtxjf.exe starts (process #22) explorer.exe with a hidden window. • (Process #5) dadjtxjf.exe starts (process #23) explorer.exe with a hidden window. • (Process #4) dadjtxjf.exe starts (process #27) explorer.exe with a hidden window. • (Process #12) dadjtxjf.exe starts (process #24) explorer.exe with a hidden window. • (Process #9) dadjtxjf.exe starts (process #26) explorer.exe with a hidden window. • (Process #18) dadjtxjf.exe starts (process #25) explorer.exe with a hidden window. • (Process #15) dadjtxjf.exe starts (process #30) explorer.exe with a hidden window. • (Process #14) dadjtxjf.exe starts (process #29) explorer.exe with a hidden window. • (Process #19) dadjtxjf.exe starts (process #33) explorer.exe with a hidden window. • (Process #2) dadjtxjf.exe starts (process #31) explorer.exe with a hidden window. • (Process #11) dadjtxjf.exe starts (process #34) explorer.exe with a hidden window. • (Process #8) dadjtxjf.exe starts (process #32) explorer.exe with a hidden window. • (Process #6) dadjtxjf.exe starts (process #35) explorer.exe with a hidden window. • (Process #16) dadjtxjf.exe starts (process #28) explorer.exe with a hidden window. • (Process #13) dadjtxjf.exe starts (process #36) explorer.exe with a hidden window. • (Process #23) explorer.exe starts (process #37) schtasks.exe with a hidden window. • (Process #23) explorer.exe starts (process #42) whoami.exe with a hidden window. • (Process #47) regsvr32.exe starts (process #48) regsvr32.exe with a hidden window. • (Process #48) regsvr32.exe starts (process #49) explorer.exe with a hidden window. • (Process #49) explorer.exe starts (process #50) reg.exe with a hidden window. • (Process #49) explorer.exe starts (process #51) reg.exe with a hidden window. • (Process #23) explorer.exe starts nltest with a hidden window. • (Process #23) explorer.exe starts (process #53) net.exe with a hidden window. • (Process #23) explorer.exe starts (process #55) route.exe with a hidden window. • (Process #23) explorer.exe starts (process #56) netstat.exe with a hidden window. • (Process #23) explorer.exe starts (process #57) net.exe with a hidden window. • (Process #23) explorer.exe starts qwinsta with a hidden window. • (Process #49) explorer.exe starts (process #62) whoami.exe with a hidden window. • (Process #49) explorer.exe starts (process #63) cmd.exe with a hidden window. • (Process #49) explorer.exe starts (process #64) arp.exe with a hidden window. • (Process #49) explorer.exe starts (process #65) ipconfig.exe with a hidden window. • (Process #49) explorer.exe starts (process #66) net.exe with a hidden window. • (Process #49) explorer.exe starts (process #67) nslookup.exe with a hidden window. • (Process #49) explorer.exe starts nltest with a hidden window. • (Process #49) explorer.exe starts (process #68) net.exe with a hidden window. • (Process #49) explorer.exe starts (process #70) route.exe with a hidden window. • (Process #49) explorer.exe starts (process #71) netstat.exe with a hidden window. • (Process #49) explorer.exe starts (process #72) net.exe with a hidden window. • (Process #49) explorer.exe starts qwinsta with a hidden window.		
1/5	Obfuscation	Creates a page with write and execute permissions	15	-

Score	Category	Operation	Count	Classification
		• (Process #2) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #17) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #6) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #8) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #4) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #16) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #9) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #12) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #5) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #7) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #3) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #13) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #14) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #11) dadjtxjf.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #48) regsvr32.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ").		
1/5	Mutex	Creates mutex	33	-
		• (Process #23) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #23) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #20) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #20) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #28) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #28) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #26) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #26) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #31) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #31) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #27) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #27) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #21) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #21) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #36) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #36) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #24) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #24) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #29) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #29) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #22) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #22) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #32) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #32) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #35) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #35) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #34) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #34) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}". • (Process #23) explorer.exe creates mutex with name "{14A78D04-6F1A-4927-AECE-0EE9DEB87429}". • (Process #49) explorer.exe creates mutex with name "Global\{F9B41FAF-4994-487E-87C0-862C1DC89AD9}". • (Process #49) explorer.exe creates mutex with name "{F9B41FAF-4994-487E-87C0-862C1DC89AD9}". • (Process #49) explorer.exe creates mutex with name "{14A78D04-6F1A-4927-AECE-0EE9DEB87429}". • (Process #23) explorer.exe creates mutex with name "cllysffhhoemybawevnr".		

Score	Category	Operation	Count	Classification
1/5	Network Connection	Tries to connect using an uncommon port	2	-

- (Process #23) explorer.exe tries to connect to TCP port 995 at 24.229.150.54.
- (Process #49) explorer.exe tries to connect to TCP port 993 at 96.37.113.36.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	34	-

- (Process #2) dadjtxjf.exe resolves 99 API functions by name.
- (Process #3) dadjtxjf.exe resolves 99 API functions by name.
- (Process #4) dadjtxjf.exe resolves 99 API functions by name.
- (Process #5) dadjtxjf.exe resolves 99 API functions by name.
- (Process #6) dadjtxjf.exe resolves 99 API functions by name.
- (Process #7) dadjtxjf.exe resolves 99 API functions by name.
- (Process #8) dadjtxjf.exe resolves 96 API functions by name.
- (Process #9) dadjtxjf.exe resolves 99 API functions by name.
- (Process #10) dadjtxjf.exe resolves 96 API functions by name.
- (Process #11) dadjtxjf.exe resolves 99 API functions by name.
- (Process #12) dadjtxjf.exe resolves 99 API functions by name.
- (Process #13) dadjtxjf.exe resolves 99 API functions by name.
- (Process #14) dadjtxjf.exe resolves 99 API functions by name.
- (Process #15) dadjtxjf.exe resolves 99 API functions by name.
- (Process #16) dadjtxjf.exe resolves 99 API functions by name.
- (Process #17) dadjtxjf.exe resolves 99 API functions by name.
- (Process #18) dadjtxjf.exe resolves 99 API functions by name.
- (Process #19) dadjtxjf.exe resolves 99 API functions by name.
- (Process #22) explorer.exe resolves 91 API functions by name.
- (Process #29) explorer.exe resolves 91 API functions by name.
- (Process #28) explorer.exe resolves 91 API functions by name.
- (Process #27) explorer.exe resolves 91 API functions by name.
- (Process #21) explorer.exe resolves 91 API functions by name.
- (Process #35) explorer.exe resolves 91 API functions by name.
- (Process #23) explorer.exe resolves 94 API functions by name.
- (Process #34) explorer.exe resolves 91 API functions by name.
- (Process #20) explorer.exe resolves 91 API functions by name.
- (Process #31) explorer.exe resolves 91 API functions by name.
- (Process #26) explorer.exe resolves 91 API functions by name.
- (Process #32) explorer.exe resolves 91 API functions by name.
- (Process #24) explorer.exe resolves 91 API functions by name.
- (Process #36) explorer.exe resolves 91 API functions by name.
- (Process #48) regsvr32.exe resolves 92 API functions by name.
- (Process #49) explorer.exe resolves 94 API functions by name.

Score	Category	Operation	Count	Classification
1/5	Execution	Drops PE file	1	-

- (Process #20) explorer.exe drops file "C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll".

Score	Category	Operation	Count	Classification
-	Trusted	Known clean file	1	-

- File "c:\windows\syswow64\config\systemprofile\appdata\local\microsoft\windows\temporary internet files\content.ie5\a23kvyay\desktop.ini" is a known clean file.

Mitre ATT&CK Matrix

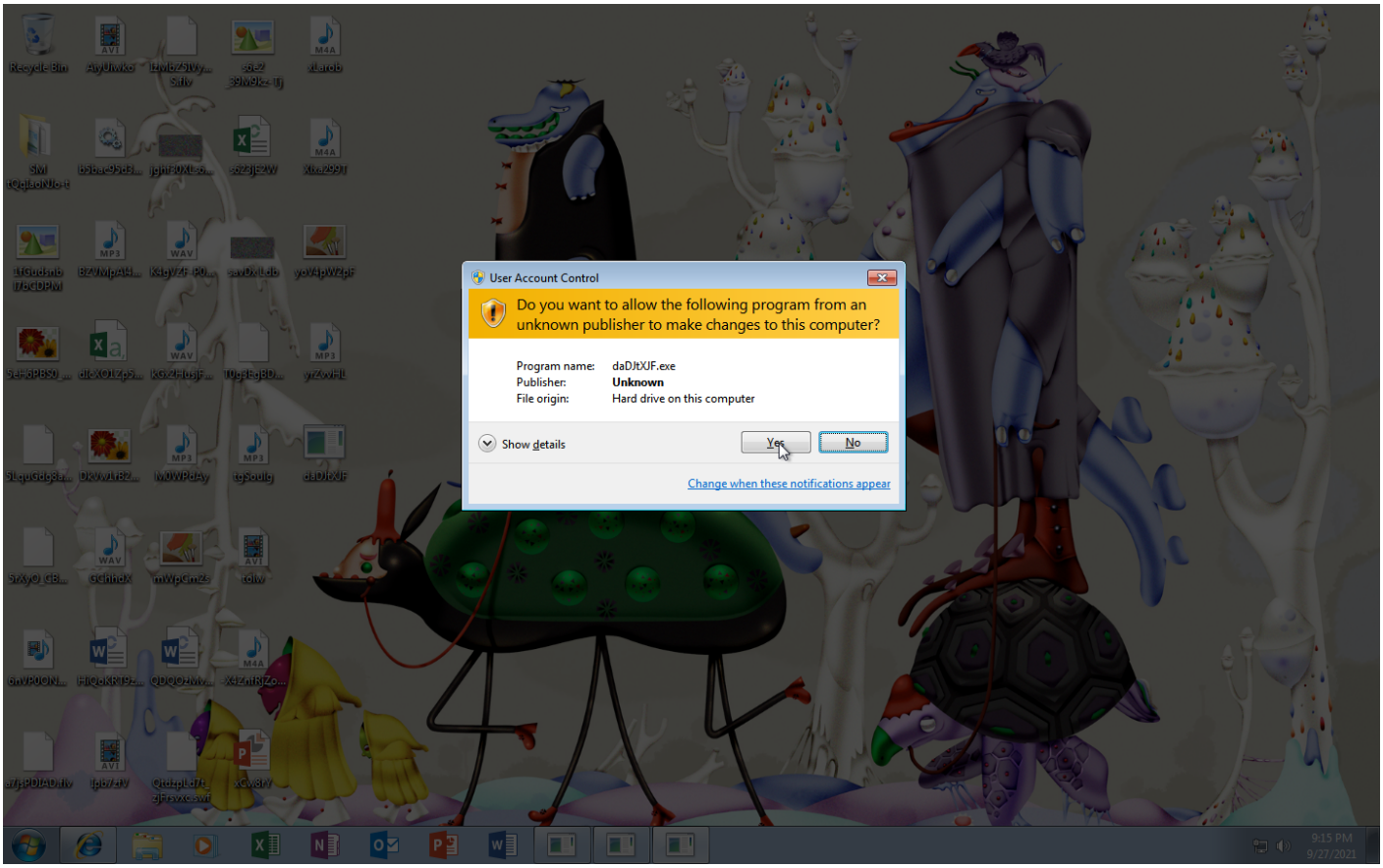
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window		#T1057 Process Discovery			#T1065 Uncommonly Used Port		
	#T1053 Scheduled Task			#T1045 Software Packing		#T1082 System Information Discovery					
				#T1089 Disabling Security Tools		#T1063 Security Software Discovery					
				#T1112 Modify Registry		#T1016 System Network Configuration Discovery					

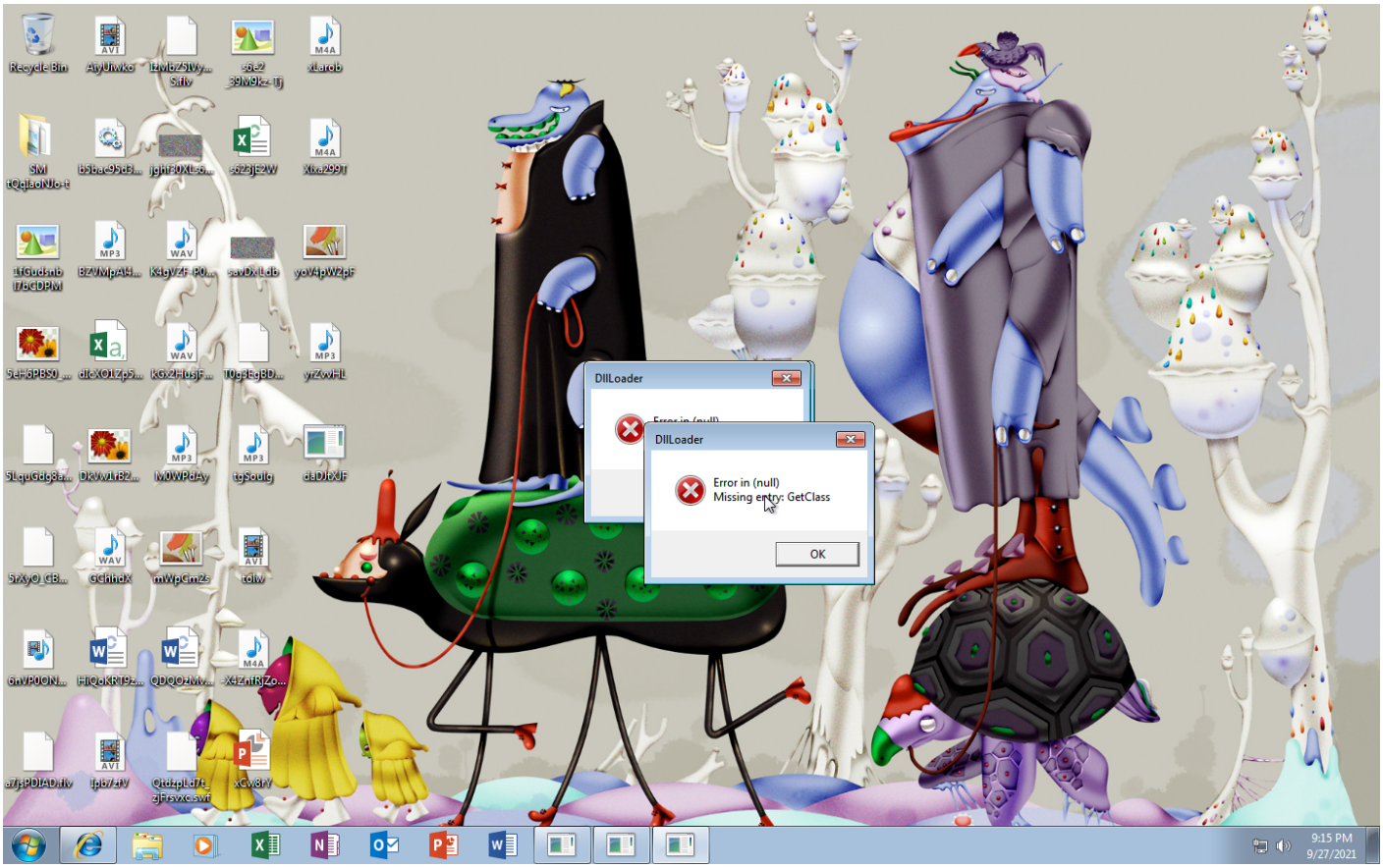
Sample Information

ID	#2780822
MD5	b9c2828409584dcb2d0a968f1968e00f
SHA1	28f7cdd53a24dd293f4d8233844fe4b609681a82
SHA256	b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969
SSDeep	3072:Do6vBnby4Yx0XjFFzPQ0MslzERfQB24hLxBVi/b/9+PdpiWC35ol/uwfTuT2b2M8:vs6Xpq0H3Jhds/9+qC/zfTPLi
ImpHash	ef258cd2a69e4871222e8a6651dd9af8
File Name	b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll
File Size	378.00 KB
Sample Type	Windows DLL (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-27 23:15 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	66
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	0


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



Screenshots truncated

NETWORK

General

221.80 KB total sent

151.79 KB total received

4 ports 993, 443, 53, 995

7 contacted IP addresses

0 URLs extracted

2 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

6 URLs contacted, 6 servers

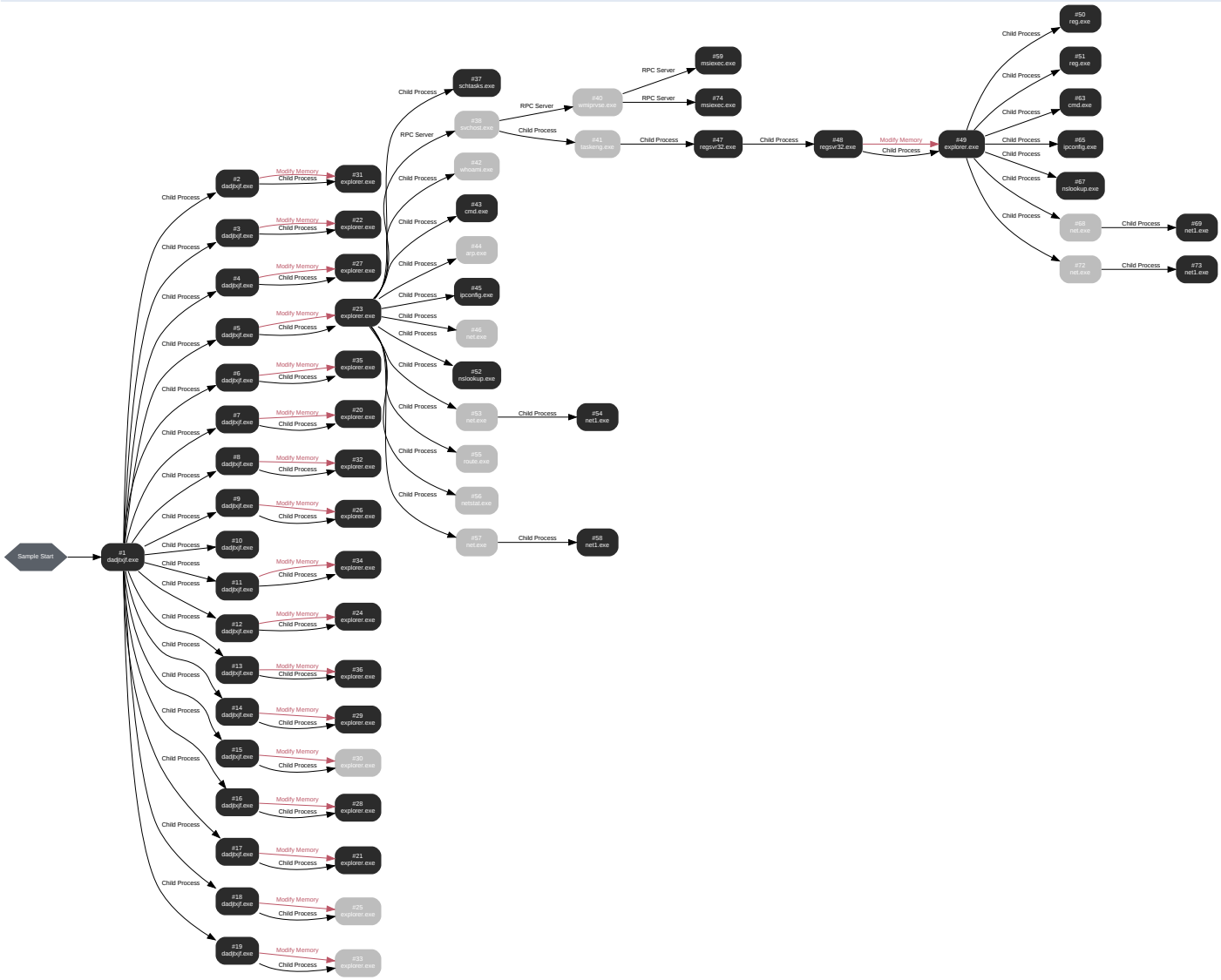
104 sessions, 221.41 KB sent, 151.05 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	https://120.151.47.189/t4	-	-		0 bytes	NA
POST	https://24.229.150.54/t4	-	-		0 bytes	NA
POST	https://96.37.113.36/t4	-	-		0 bytes	NA
POST	https://103.148.120.144/t4	-	-		0 bytes	NA
POST	https://2.188.27.77/t4	-	-		0 bytes	NA
POST	https://140.82.49.12/t4	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: dadjtxjf.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmpb141g1rs" /s
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 30746, Reason: Analysis Target
Unmonitor End Time	End Time: 52388, Reason: Terminated
Monitor duration	21.64s
Return Code	0
PID	3592
Parent PID	1116
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll	378.00 KB	b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969	✗
C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll	378.00 KB	17d261eaca2629ef9907d0c00fb2271201e466796f06dcb7232900d711c29330	✗

Host Behavior

Type	Count
System	2
Module	20
File	7
Environment	1
Process	18

Process #2: dadjtxjf.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 45425, Reason: Child Process
Unmonitor End Time	End Time: 80615, Reason: Terminated
Monitor duration	35.19s
Return Code	4294967292
PID	3620
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	5
Process	115
-	5
-	2
-	1

Process #3: dadjtxjf.exe

ID	3
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 45556, Reason: Child Process
Unmonitor End Time	End Time: 88659, Reason: Terminated
Monitor duration	43.10s
Return Code	4294967292
PID	3636
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	6
Process	114
-	5
-	2
-	1

Process #4: dadjtxjf.exe

ID	4
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 45657, Reason: Child Process
Unmonitor End Time	End Time: 78072, Reason: Terminated
Monitor duration	32.41s
Return Code	4294967292
PID	3648
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	5
Process	114
-	5
-	2
-	1

Process #5: dadjtxjf.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 46034, Reason: Child Process
Unmonitor End Time	End Time: 77559, Reason: Terminated
Monitor duration	31.52s
Return Code	4294967292
PID	3660
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	5
Process	114
-	5
-	2
-	1

Process #6: dadjtxjf.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 46966, Reason: Child Process
Unmonitor End Time	End Time: 79213, Reason: Terminated
Monitor duration	32.25s
Return Code	4294967292
PID	3672
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	5
Process	114
-	5
-	2
-	1

Process #7: dadjtxjf.exe

ID	7
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 47072, Reason: Child Process
Unmonitor End Time	End Time: 89577, Reason: Terminated
Monitor duration	42.51s
Return Code	4294967292
PID	3684
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	3
Environment	5
Window	2
-	6
Process	114
-	5
-	2
-	1

Process #8: dadjtxjf.exe

ID	8
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 47934, Reason: Child Process
Unmonitor End Time	End Time: 88554, Reason: Terminated
Monitor duration	40.62s
Return Code	4294967292
PID	3700
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	140
File	3
Environment	5
Window	2
-	6
Process	114
-	5
-	2
-	1

Process #9: dadjtxjf.exe

ID	9
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 49087, Reason: Child Process
Unmonitor End Time	End Time: 85877, Reason: Terminated
Monitor duration	36.79s
Return Code	4294967292
PID	3712
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	5
Process	114
-	5
-	2
-	1

Process #10: dadjtxjf.exe

ID	10
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 49295, Reason: Child Process
Unmonitor End Time	End Time: 64841, Reason: Terminated
Monitor duration	15.55s
Return Code	4294967292
PID	3724
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	136
File	3
Environment	5
Window	1
-	4
Process	102

Process #11: dadjtxjf.exe

ID	11
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 49368, Reason: Child Process
Unmonitor End Time	End Time: 75195, Reason: Terminated
Monitor duration	25.83s
Return Code	4294967292
PID	3736
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	4
Process	116
-	5
-	2
-	1

Process #12: dadjtxjf.exe

ID	12
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 50144, Reason: Child Process
Unmonitor End Time	End Time: 85831, Reason: Terminated
Monitor duration	35.69s
Return Code	4294967292
PID	3748
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	5
Process	114
-	5
-	2
-	1

Process #13: dadjtxjf.exe

ID	13
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 50205, Reason: Child Process
Unmonitor End Time	End Time: 88183, Reason: Terminated
Monitor duration	37.98s
Return Code	4294967292
PID	3760
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	5
Process	115
-	5
-	2
-	1

Process #14: dadjtxjf.exe

ID	14
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 50307, Reason: Child Process
Unmonitor End Time	End Time: 85219, Reason: Terminated
Monitor duration	34.91s
Return Code	4294967292
PID	3772
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	5
Process	114
-	5
-	2
-	1

Process #15: dadjtxjf.exe

ID	15
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 50522, Reason: Child Process
Unmonitor End Time	End Time: 74589, Reason: Terminated
Monitor duration	24.07s
Return Code	4294967292
PID	3784
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	4
Process	114
-	2

Process #16: dadjtxjf.exe

ID	16
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 50613, Reason: Child Process
Unmonitor End Time	End Time: 88844, Reason: Terminated
Monitor duration	38.23s
Return Code	4294967292
PID	3796
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	5
Process	115
-	5
-	2
-	1

Process #17: dadjtxjf.exe

ID	17
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 50827, Reason: Child Process
Unmonitor End Time	End Time: 82173, Reason: Terminated
Monitor duration	31.35s
Return Code	4294967292
PID	3808
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	5
Process	114
-	5
-	2
-	1

Process #18: dadjtxjf.exe

ID	18
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 51034, Reason: Child Process
Unmonitor End Time	End Time: 74623, Reason: Terminated
Monitor duration	23.59s
Return Code	4294967292
PID	3820
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	4
Process	114
-	2

Process #19: dadjtxjf.exe

ID	19
File Name	c:\users\keecfmwgj\desktop\dadjtxjf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 51132, Reason: Child Process
Unmonitor End Time	End Time: 74589, Reason: Terminated
Monitor duration	23.46s
Return Code	4294967292
PID	3832
Parent PID	3592
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	145
File	4
Environment	5
Window	2
-	4
Process	114
-	2

Process #20: explorer.exe

ID	20
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 62152, Reason: Child Process
Unmonitor End Time	End Time: 90055, Reason: Terminated
Monitor duration	27.90s
Return Code	0
PID	2248
Parent PID	3684
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#7: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf28	0x70000(458752)	0x21000	✓	1
Modify Memory	#7: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf28	0xa0000(655360)	0x1ac4	✓	1
Modify Memory	#7: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf28	0xf80efa(16256762)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	720
Registry	3
File	729
Mutex	2

Process #21: explorer.exe

ID	21
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 63682, Reason: Child Process
Unmonitor End Time	End Time: 90735, Reason: Terminated
Monitor duration	27.05s
Return Code	0
PID	2524
Parent PID	3808
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#17: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf88	0x70000(458752)	0x21000	✓	1
Modify Memory	#17: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf88	0xa0000(655360)	0x1ac4	✓	1
Modify Memory	#17: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf88	0xf80efa(16256762)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	735
Registry	3
File	744
Mutex	2

Process #22: explorer.exe

ID	22
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 63757, Reason: Child Process
Unmonitor End Time	End Time: 90488, Reason: Terminated
Monitor duration	26.73s
Return Code	0
PID	2536
Parent PID	3636
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#3: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf38	0xc0000(786432)	0x21000	✓	1
Modify Memory	#3: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf38	0x70000(458752)	0x1ac4	✓	1
Modify Memory	#3: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf38	0xf80efa(16256762)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	787
Registry	4
File	796
Mutex	2

Process #23: explorer.exe

ID	23
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 63814, Reason: Child Process
Unmonitor End Time	End Time: 271702, Reason: Terminated by Timeout
Monitor duration	207.89s
Return Code	Unknown
PID	2544
Parent PID	3660
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf34	0x70000(458752)	0x21000	✓	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf34	0xa0000(655360)	0x1ac4	✓	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf34	0xf80efa(16256762)	0x5	✓	1

Dropped Files (107)

File Name	File Size	SHA256	YARA Match
-	184 bytes	6967fc3dfaeaf0d1ff656ebe62ce114ea2a92dc32ad99fe19e255be3665d1cc2	✗
-	157.23 KB	3d249db46b4bd1cfae8f56b272f7116b218ac9d64225d1109751ee487fa9f3ae	✗
-	59.72 KB	f8e90fb0557fe49d7702cfb506312ac0b24c97802f9c782696db6d47f434e8e9	✗
-	96 bytes	62f2df959ba7b4e526f6cf6e7fb34ffd55717603c5b29b3f7f64f79ad93d895d	✗
-	832 bytes	a425c1e63bdb66c592d651c0009470b1b20a2fca9cd42362d474b71ad24cd575	✗
-	872 bytes	94ec44d89755cd8a104eebc4cffd3beae846d9a9840023f3a77f795be9d1ba5f	✗
-	752 bytes	2914df66053dd1612fee35b5041ed5fd61724f48eadef2182c717f8ab84228f6	✗
-	740 bytes	3ed9d7cc09f8ef0f09b4f9b7d41cc39fe01f9e2af75ed307f696a83cb0113b4f	✗
-	764 bytes	7bfd337714c3ec96ced3983d3e206736fcf47a5240a7184ccdda6a3136ebc312	✗
-	1.19 KB	3f5207337ff8bb0963011de2fb3b1ed1587be48278a83a9e80b1ec5eac2fad42	✗
-	1.20 KB	378cdde06fe842afa25160f372eec804eca7699b3f4198cab25b52f8ec02b6e4	✗
-	700 bytes	3c60e6057455ec0992d5418e25f17c965368ec4dbea78c07cfe950042854003c	✗
-	688 bytes	8a5b00d743d4033d8dbc3eea3158ff5e927876d418ee5716cd7f886e1d487fe7	✗

File Name	File Size	SHA256	YARA Match
-	804 bytes	8184165e644de0fc2aadb9ca0372969730d583e5edc37096ccf2be95e2ec5e6c	✗
-	672 bytes	65c2055621ae8f4112de9fabd71656580378f460b255842b56244f8e69482519	✗
-	740 bytes	de27dc3c8e753594f393e5b46930a5f5716504ad350d78362779050ff5a284b1	✗
-	632 bytes	b8844924cb201b58e9882609df6968f5f8dba5c479591588aaadbc5a9d966318	✗
-	588 bytes	089298dd9955d114593defabe74283b6711a2c7cd3e082b1231ee852400498a8	✗
-	1.13 KB	d8795506bd2f368fd2442e3c7b85cbcdc7a11550dc60b19805d50e1c564074be	✗
-	900 bytes	f1f8040b3229d13e729a6bd7f4fe0f3bbab3e53149213ed6118517e4008986f6	✗
-	1.09 KB	4bbb59462e7b4fbaafc8497bf6045c2d48b1695f05dc2fa58ed474c14b9cc3b4	✗
-	1.18 KB	cfaab4877ee2c5e6d3de409166ad490889a012cae1b2ea583b4f6770c25e941c	✗
-	584 bytes	25967f957c17ce21c7549aa48948155a56308c0f40cbfc1a83bcb093dc40c6ab	✗
-	584 bytes	66f71c2a1ddc2cfe1d7c4845392756b75227f9c5c13064ba9e7bfd7153df56ec	✗
-	660 bytes	d839448622e34f0c06e623ba7fc3fcc57b13914829b836bfe2e37b451cec5638	✗
-	580 bytes	90ddad000b834b7071bdde8aff3ac72baaf3dc7bb8e8eaecbf5f06922a7c526d	✗
-	668 bytes	329ebc4079b9f52a650820d60f56e5a90bc5e3d946ae892b5831d1a8ce88e013	✗
-	732 bytes	4b098e4adda352f0dad1884ce79a221eb856a9db88624dbae94a548aa1abb553	✗
-	744 bytes	5bb32eccfa27ac9210d687fd52e37b5ca26fc53dcff09c5627c27286f02df0c9	✗
-	640 bytes	69b084deca6f02b3aaf5f1a9b5305d191197b4f9b3e47306d7e2fc69448ece54	✗
-	1.02 KB	01ff90e901b8914ff3275cdfac897b6e08ef007675dd095238224157b18df8c5	✗
-	876 bytes	4561419960bc2b4858a22d0852cb333b1a9b9714c2211c3519ccf2048eba4968	✗
-	712 bytes	f22b05f22db93ca9d915be8abf0fc23d7c7bbf4ed690e8e0a375a4abff6ad8a1	✗
-	572 bytes	6c150b82b2601582bd73213a335baac82fa21433f387145ff4eaaf51adac478f	✗
-	908 bytes	3c256a0b06c9f16e33de22ddbb8e3e67549fb7b8ab8cd3adeff1f8d04b711c3f	✗
-	1020 bytes	6025e84fb6fa8d3459a5c8aecc3dd6993a0bda5bea2e1b0ce37c2a857978bc63	✗
-	700 bytes	f090b20634d887264e4093055dda3a7c50140014e0e4cef66a313e5e71b850d6	✗
-	724 bytes	42b107356f85fe512ca70d14e06ff72041761eab8c42e9df14c0ceb6e889be95	✗
-	988 bytes	c5384fba03d42908df45c6df3a42ee4226d0340d506d6ddb66a3fdc6be28dfac	✗
-	808 bytes	01fd8c295cb1b46eb8149829abb4de932d3a636e2e6acd1f43bf59e9c5332c04	✗
-	732 bytes	69d860b7492408ff84d89e5f7f534452ec619c205f7018d13bbaa4a890d62953	✗
-	1.01 KB	b0421ff4f7d9f4a6e69760e1b97d2336e6a0b01c08e79038e18ec4d3b23699f6	✗

File Name	File Size	SHA256	YARA Match
-	1.19 KB	ec5412edf00277993f7525894882c520083973d99223bf28e289352ef932c30a	✗
-	744 bytes	780d1c0b6424410e8fa0a9f7174b5e0504579a73be1b23c5900ff87b60e6d062	✗
-	1.08 KB	7d592cc9452c1fd9e7f4af929513c732239b208463791c0f5c8e4ac4114559a5	✗
-	960 bytes	8f633797484fbaca1e0747844f85935d92f72d6a1b100357b1e4e5ecf565f0c6	✗
-	852 bytes	4bd644d479189c0db51ed6510ba5aeadebe20497f8a103a04fbd20bf442cce4a	✗
-	948 bytes	352c53d284d4cb4c99b8ef4a47cb59373979ee511cfde170f49ceeaa660bd0ba	✗
-	1.20 KB	efbe7dd9d2084015b810919790b2995d5c1d8158880d777b3702519a50fc3e8f	✗
-	1.10 KB	94d0ca8b726d21c1ea1c57049a3ea3e31cb73151824d9fe984e7972d941945f7	✗
-	864 bytes	747951de356479f06e1ec3be37e6ae88297a1e4d79b6173566c3176717962a46	✗
-	1.02 KB	93a6d9a7c2bbecfb11033630327b84f33da2e22956e3e19c445b8f1fe38921e2	✗
-	1.08 KB	a9cbacd88514de1ccec836c24b6aa099104bfbe1533f3b7afb596e2537fe8ae1	✗
-	776 bytes	f4ee736fbc5b02122f9eaab49447235a76d00e1b9b5abd5b1ad04fb40f7d239b	✗
-	1.20 KB	b4b0cf5f0feface2baf1e9cf4a0f8f6f987ada80ddf1ab0fb1dc72adf75f4c8a	✗
-	1.19 KB	e0931e407a2bb39f3690fb437058cfac00deeef8aef8a07682d5a19a33d082a3	✗
-	932 bytes	a89f28ff0493fc67512ebe6e3b279dfe2006bf7c8b55b996e3e845573a9091cf	✗
-	976 bytes	859cb26c0e17977a980241e9cd7e1e4e991224e75e3458358828b9d418fb1233	✗
-	688 bytes	cbbdeb28df90dfe3395aaf8d6c4271a87e5476eb161a73d9f07cb1d1a937c035	✗
-	884 bytes	bd061ef0da493a63f8ecb7126d59fcf37fbc1954ea5fcee54296a5e4dd6a74db	✗
-	1.15 KB	5c5f747341fbf0859aeb5c276dd5b343571f02597a3a79b89bd39329c615ba9a	✗
-	1.12 KB	802655a077efd4c8e8e39a4f31eb026b72e3a5b213694186c1db5d6f359e1066	✗
-	576 bytes	2b86011d070e041616b570eb69bf456a544690d9593369df53c277b178a3bbdc	✗
-	1.19 KB	2372126c451d3f79ddfb4514ba717141d4fcbc5ce81fabf421fa52935f66577e	✗
-	616 bytes	d7e126a531f2c9f38b2e1f05297339df6f7f3a7bebae25e1072248c0b3591a47	✗
-	576 bytes	cb3eb2d31d4ed16ba87506d80f9d7aa00f84dd445ad8120ad7511a842f29be7a	✗
-	1004 bytes	ee9742683b7d6f508512b1c0171ffa50ec0e08ada82d66d4f3acd7c8afed724b	✗
-	1.19 KB	0df5457272b590e47a0945d175ed5a50dd6fcd5eef72bb11b022cfa4b7106724	✗
-	820 bytes	bf2c1327abb7c89b8e350b3ca6a72d3d66d6d7ad08183492cf4ca3dab7112741	✗
-	888 bytes	a22be379a72f80027c32b82adcaf4580c9f8c317dc5197068fd5d6b135bf8bd2	✗
-	1.16 KB	672222e2a1a49c8b4dcf33087b734f26d5ab7da02b1bfa2b0453f08f62475fcb	✗

File Name	File Size	SHA256	YARA Match
-	604 bytes	ff344daa261f431886844c621c96a0e2d98006d1c86df9385a49ce1409f2f4b6	✗
-	1.12 KB	0ddc3ee0b381ac20265d5ff0e942327fc26428bca48e07b4b9c6cd4a90ea1931	✗
-	588 bytes	2bec6888128a5698ab3874ce6376e83f0f63b11ac09df152d13913af89f7bb79	✗
-	628 bytes	06ec5b8e097376516b55c468363d154f175cf79bd17fd37685c2dd538b8eb64e	✗
-	904 bytes	6a26b3e8d42522298c86cf33405b4b688d8728c21b9307a3d237103032cd5b64	✗
-	972 bytes	9ac3643a0730f6e901e95bcd0d8fb9f5428e648e8562805384bedca06e22b7a0	✗
-	876 bytes	2ecb90fe7e1321ab5da72eda541e78d7ef999f04ab8a163c10c1166963dd7b2b	✗
-	1.05 KB	a77cb61a7d73bad2d570fe34c1f7669c3b635b023abc0741aaa5b50540d634b4	✗
-	576 bytes	a004c8d7784259a26dba530247767c5b9833f49b89a842c7d60efb2030c0aa5a	✗
-	572 bytes	fb229203706d0fe73dc9be52b22f9960b3b384348dd254a646a7715f038de675	✗
-	1.11 KB	d9c5a389c2142809a9d6a6d38c0da0fcd1485b638d09c157156112f7d8c85a49	✗
-	1.02 KB	6c7616f333d1605156db02c8018ae2d78796933fceff1650f0b4250ae20d6d59	✗
-	580 bytes	332a6ae8f80aee84d48aa71c17558ae96dbb1bb014cc15e28cda6d6b4ad640d3	✗
-	788 bytes	732f68c64d1c0e73c0a08706293f2adda0600a5564fcd9a0336239d9dca4b09c	✗
-	1.18 KB	609317ae077d0e7d0bbf19275697970ad4df3680f30cd5f03a83b6fe48f99111	✗
-	740 bytes	788f62baf4d594d62ff6e16999b94af302b22be2c7ca98649b8e769db4d4f887	✗
-	1.20 KB	52738accb94fb232530592886 23f05eecbb258232f0f6e4b1665bfc16b2b8cd8	✗
-	716 bytes	8fc6fcbfc652e7671d6bbdbf869abdeed7fb7a0bd2cfd99763dff677a82b0a6e	✗
-	840 bytes	9e1ab262d151e08925c794150d62afe02baa77f61675b07b17dfc7976df9f5d4	✗
-	624 bytes	cbd9ec8d1d2c5ebfa69650ea70ae1d5a16dde399ad934eebd1f1b9e0681ceb96	✗
-	776 bytes	7122466044329cbd1c6bc8343c11812b83def33228308bbe836b32c4be4fba29	✗
-	1.21 KB	f5f8f20153e7b0ea70ed01e25a9c8c00339c7ae5aea962eac927a62744a87fdb	✗
-	812 bytes	06a6691701fcb5eff9ab2c6fbaf5c5f141612c6d15530429e4a6eb65caa64588	✗
-	664 bytes	8fea1adcbd1b446ceffcc07acf35e5aaa5905c101fc3accf2659de6d6449ec7c	✗
-	832 bytes	7f0f5bd3f16808cc9e6764ce5089a526183984339a98ebf9accd19a2beee3b6c	✗
-	1.13 KB	ddbd4e254a4cf5a0fb071f9e65ce7885bc543508d4b5351dba68f6f9244081a4	✗
-	824 bytes	55b6d4245b6be4e04aa97bfb4062d63e7f954fce1feccffda6f5ff861d1b6990	✗
-	1012 bytes	3d58547facead0572c750c60f316c33d1133b03310714ad437dfc1c465b1161f	✗
-	792 bytes	5c1b5bf53aca6765fcabd2824c57100e8f6c81e0066250771fdc0b0a70aee5ad	✗

File Name	File Size	SHA256	YARA Match
-	980 bytes	b7b58effa85964b0d14bc59ea54cb0e95fd64135d7ec5e11d272c981420a44a4	✗
-	1.05 KB	b90b46bb74c4c20f88a92a95bae5f7d356e21f9b04a160fbb2f65339c0768762	✗
-	1.14 KB	f05d81e2ff891b17819a928cf5ebfa93d08f304602aea9a2c29a20b74565dbf2	✗
-	864 bytes	5ff797c05b398de48ae6e34e14bf0014f38a696d4cb8329ae04cbe553b83bb80	✗
-	872 bytes	72c8f06540e7a58a76e854b68d8195a7aebae3ad9df751c877f96d64c62bebcd	✗
-	1.21 KB	9df48405bb7a356eb1d4447f888c6db604dc24c6a4e6da4142a6e3e3cb5ee996	✗
-	1.18 KB	00206ea3d0fb8cb7b10b6f3b8e2b2889cdedac264a286c55d5ecdf25f1de5c60	✗

Host Behavior

Type	Count
Module	122
Process	275
System	19273
Registry	5447
File	2526
Mutex	2344
Keyboard	2
-	1
-	294
Window	1
COM	9
-	9

Network Behavior

Type	Count
HTTPS	106
TCP	99

Process #24: explorer.exe

ID	24
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 64149, Reason: Child Process
Unmonitor End Time	End Time: 90819, Reason: Terminated
Monitor duration	26.67s
Return Code	0
PID	2568
Parent PID	3748
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#12: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf74	0x70000(458752)	0x21000	✓	1
Modify Memory	#12: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf74	0xa0000(655360)	0x1ac4	✓	1
Modify Memory	#12: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf74	0xf80efa(16256762)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	689
Registry	3
File	698
Mutex	2

Process #25: explorer.exe

ID	25
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 64276, Reason: Child Process
Unmonitor End Time	End Time: 271702, Reason: Terminated by Timeout
Monitor duration	207.43s
Return Code	Unknown
PID	2628
Parent PID	3820
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#18: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf94	0x70000(458752)	0x21000	✓	1
Modify Memory	#18: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf94	0xa0000(655360)	0x1ac4	✓	1

Process #26: explorer.exe

ID	26
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65025, Reason: Child Process
Unmonitor End Time	End Time: 90133, Reason: Terminated
Monitor duration	25.11s
Return Code	0
PID	2832
Parent PID	3712
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#9: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf68	0xb0000(720896)	0x21000	✓	1
Modify Memory	#9: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf68	0xe0000(917504)	0x1ac4	✓	1
Modify Memory	#9: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf68	0xf80efa(16256762)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	694
Registry	3
File	703
Mutex	2

Process #27: explorer.exe

ID	27
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65105, Reason: Child Process
Unmonitor End Time	End Time: 90231, Reason: Terminated
Monitor duration	25.13s
Return Code	0
PID	2968
Parent PID	3648
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#4: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf20	0x70000(458752)	0x21000	✓	1
Modify Memory	#4: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf20	0xa0000(655360)	0x1ac4	✓	1
Modify Memory	#4: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf20	0xf80efa(16256762)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	742
Registry	3
File	751
Mutex	2

Process #28: explorer.exe

ID	28
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65117, Reason: Child Process
Unmonitor End Time	End Time: 90055, Reason: Terminated
Monitor duration	24.94s
Return Code	0
PID	2976
Parent PID	3796
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#16: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf8c	0xb0000(720896)	0x21000	✓	1
Modify Memory	#16: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf8c	0xe0000(917504)	0x1ac4	✓	1
Modify Memory	#16: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf8c	0xf80efa(16256762)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	736
Registry	3
File	745
Mutex	2

Process #29: explorer.exe

ID	29
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65128, Reason: Child Process
Unmonitor End Time	End Time: 91828, Reason: Terminated
Monitor duration	26.70s
Return Code	0
PID	2744
Parent PID	3772
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#14: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf7c	0xc0000(786432)	0x21000	✓	1
Modify Memory	#14: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf7c	0x70000(458752)	0x1ac4	✓	1
Modify Memory	#14: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf7c	0xf80efa(16256762)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	776
Registry	3
File	785
Mutex	2

Process #30: explorer.exe

ID	30
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65130, Reason: Child Process
Unmonitor End Time	End Time: 271702, Reason: Terminated by Timeout
Monitor duration	206.57s
Return Code	Unknown
PID	948
Parent PID	3784
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#15: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf98	0x70000(458752)	0x21000	✓	1
Modify Memory	#15: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf98	0xa0000(655360)	0x1ac4	✓	1

Process #31: explorer.exe

ID	31
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65132, Reason: Child Process
Unmonitor End Time	End Time: 90152, Reason: Terminated
Monitor duration	25.02s
Return Code	0
PID	3252
Parent PID	3620
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf50	0x70000(458752)	0x21000	✓	1
Modify Memory	#2: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf50	0xa0000(655360)	0x1ac4	✓	1
Modify Memory	#2: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf50	0xf80efa(16256762)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	697
Registry	3
File	706
Mutex	2

Process #32: explorer.exe

ID	32
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65135, Reason: Child Process
Unmonitor End Time	End Time: 90102, Reason: Terminated
Monitor duration	24.97s
Return Code	0
PID	936
Parent PID	3700
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#8: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf64	0x70000(458752)	0x21000	✓	1
Modify Memory	#8: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf64	0xe0000(917504)	0x1ac4	✓	1
Modify Memory	#8: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf64	0xf80efa(16256762)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	689
Registry	3
File	698
Mutex	2

Process #33: explorer.exe

ID	33
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65136, Reason: Child Process
Unmonitor End Time	End Time: 271702, Reason: Terminated by Timeout
Monitor duration	206.57s
Return Code	Unknown
PID	3288
Parent PID	3832
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#19: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf9c	0x120000(1179648)	0x21000	✓	1
Modify Memory	#19: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf9c	0x70000(458752)	0x1ac4	✓	1

Process #34: explorer.exe

ID	34
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65138, Reason: Child Process
Unmonitor End Time	End Time: 90600, Reason: Terminated
Monitor duration	25.46s
Return Code	0
PID	3284
Parent PID	3736
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#11: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf78	0x70000(458752)	0x21000	✓	1
Modify Memory	#11: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf78	0xa0000(655360)	0x1ac4	✓	1
Modify Memory	#11: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf78	0xf80efa(16256762)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	731
Registry	3
File	740
Mutex	2

Process #35: explorer.exe

ID	35
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65141, Reason: Child Process
Unmonitor End Time	End Time: 89673, Reason: Terminated
Monitor duration	24.53s
Return Code	0
PID	3268
Parent PID	3672
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf3c	0xc0000(786432)	0x21000	✓	1
Modify Memory	#6: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf3c	0x70000(458752)	0x1ac4	✓	1
Modify Memory	#6: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf3c	0xf80efa(16256762)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	733
Registry	3
File	742
Mutex	2

Process #36: explorer.exe

ID	36
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65170, Reason: Child Process
Unmonitor End Time	End Time: 90770, Reason: Terminated
Monitor duration	25.60s
Return Code	0
PID	3296
Parent PID	3760
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#13: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf90	0x70000(458752)	0x21000	✓	1
Modify Memory	#13: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf90	0xe0000(917504)	0x1ac4	✓	1
Modify Memory	#13: c:\users\keecfmwgj\desktop\dadjtxjf.exe	0xf90	0xf80efa(16256762)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	688
Registry	3
File	697
Mutex	2

Process #37: schtasks.exe

ID	37
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\system32\schtasks.exe" /Create /RU "NT AUTHORITY\SYSTEM" /tn lmtrjjbrh /tr "regsvr32.exe -s \"C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll\"" /SC ONCE /Z /ST 21:19 /ET 21:31
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89248, Reason: Child Process
Unmonitor End Time	End Time: 91828, Reason: Terminated
Monitor duration	2.58s
Return Code	0
PID	2508
Parent PID	2544
Bitness	32 Bit

Host Behavior

Type	Count
System	5
Module	11
COM	1
User	1
File	5

Process #38: svchost.exe

ID	38
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 96977, Reason: RPC Server
Unmonitor End Time	End Time: 271702, Reason: Terminated by Timeout
Monitor duration	174.72s
Return Code	Unknown
PID	868
Parent PID	448
Bitness	64 Bit

Process #40: wmiprvse.exe

ID	40
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 101706, Reason: RPC Server
Unmonitor End Time	End Time: 271702, Reason: Terminated by Timeout
Monitor duration	170.00s
Return Code	Unknown
PID	2044
Parent PID	584
Bitness	64 Bit

Process #41: taskeng.exe

ID	41
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {C9CD2011-1E8F-43F4-974C-D55AEA23B22B} S-1-5-18:NT AUTHORITY\System:Service:
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 113967, Reason: Child Process
Unmonitor End Time	End Time: 271702, Reason: Terminated by Timeout
Monitor duration	157.74s
Return Code	Unknown
PID	2224
Parent PID	868
Bitness	64 Bit

Process #42: whoami.exe

ID	42
File Name	c:\windows\syswow64\whoami.exe
Command Line	whoami /all
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 115847, Reason: Child Process
Unmonitor End Time	End Time: 117457, Reason: Terminated
Monitor duration	1.61s
Return Code	0
PID	1720
Parent PID	2544
Bitness	32 Bit

Process #43: cmd.exe

ID	43
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd /c set
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 116461, Reason: Child Process
Unmonitor End Time	End Time: 118140, Reason: Terminated
Monitor duration	1.68s
Return Code	0
PID	2552
Parent PID	2544
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	155

Process #44: arp.exe

ID	44
File Name	c:\windows\syswow64\arp.exe
Command Line	arp -a
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 117149, Reason: Child Process
Unmonitor End Time	End Time: 118997, Reason: Terminated
Monitor duration	1.85s
Return Code	0
PID	2648
Parent PID	2544
Bitness	32 Bit

Process #45: ipconfig.exe

ID	45
File Name	c:\windows\syswow64\ipconfig.exe
Command Line	ipconfig /all
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 117811, Reason: Child Process
Unmonitor End Time	End Time: 120135, Reason: Terminated
Monitor duration	2.32s
Return Code	0
PID	2672
Parent PID	2544
Bitness	32 Bit

Host Behavior

Type	Count
System	9
Module	1
File	91
COM	1
-	3
Registry	4

Process #46: net.exe

ID	46
File Name	c:\windows\syswow64\net.exe
Command Line	net view /all
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 119147, Reason: Child Process
Unmonitor End Time	End Time: 134020, Reason: Terminated
Monitor duration	14.87s
Return Code	2
PID	2820
Parent PID	2544
Bitness	32 Bit

Process #47: regsvr32.exe

ID	47
File Name	c:\windows\system32\regsvr32.exe
Command Line	regsvr32.exe -s "C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 121873, Reason: Child Process
Unmonitor End Time	End Time: 129400, Reason: Terminated
Monitor duration	7.53s
Return Code	0
PID	3360
Parent PID	2224
Bitness	64 Bit

Host Behavior

Type	Count
System	4
Module	2
Registry	4
File	3
Process	1

Process #48: regsvr32.exe

ID	48
File Name	c:\windows\syswow64\regsvr32.exe
Command Line	-s "C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 122963, Reason: Child Process
Unmonitor End Time	End Time: 129000, Reason: Terminated
Monitor duration	6.04s
Return Code	0
PID	3160
Parent PID	3360
Bitness	32 Bit

Host Behavior

Type	Count
System	17
Module	124
Registry	4
Window	1
-	5
Process	105
Environment	4
-	5
-	2
-	1

Process #49: explorer.exe

ID	49
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 127602, Reason: Child Process
Unmonitor End Time	End Time: 271702, Reason: Terminated by Timeout
Monitor duration	144.10s
Return Code	Unknown
PID	1400
Parent PID	3160
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#48: c:\windows\syswow64\regsvr32.exe	0xca4	0xf0000(983040)	0x21000	✓	1
Modify Memory	#48: c:\windows\syswow64\regsvr32.exe	0xca4	0x120000(1179648)	0x1ac4	✓	1
Modify Memory	#48: c:\windows\syswow64\regsvr32.exe	0xca4	0xf80efa(16256762)	0x5	✓	1

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
-	67 bytes	2842973d15a14323e08598be1dfb87e54bf88a76be8c7bc94c56b079446edf38	✗
-	124 bytes	71d7b2ceb630b9c0402673c02c400829b3992381d1b2a5719474f88c2965aa92	✗

Host Behavior

Type	Count
Module	122
Process	306
System	14130
Registry	2732
File	21
Mutex	1250
Keyboard	2
Environment	1
-	192
-	1
Window	1
COM	8
-	8

Network Behavior

Type	Count
HTTPS	15
TCP	5

Process #50: reg.exe

ID	50
File Name	c:\windows\system32\reg.exe
Command Line	C:\Windows\system32\reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /f /t REG_DWORD /v "C:\ProgramData\Microsoft\Cuaohnwer" /d "0"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 128169, Reason: Child Process
Unmonitor End Time	End Time: 129603, Reason: Terminated
Monitor duration	1.43s
Return Code	0
PID	3484
Parent PID	1400
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	1
Registry	4
File	5

Process #51: reg.exe

ID	51
File Name	c:\windows\system32\reg.exe
Command Line	C:\Windows\system32\reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /f /t REG_DWORD /v "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Mqloaubiwjuo" /d "0"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 128671, Reason: Child Process
Unmonitor End Time	End Time: 129402, Reason: Terminated
Monitor duration	0.73s
Return Code	0
PID	1364
Parent PID	1400
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	1
Registry	4
File	5

Process #52: nslookup.exe

ID	52
File Name	c:\windows\syswow64\nslookup.exe
Command Line	nslookup -querytype=ALL -timeout=10 _ldap._tcp.dc._msdcs.WORKGROUP
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 133014, Reason: Child Process
Unmonitor End Time	End Time: 134933, Reason: Terminated
Monitor duration	1.92s
Return Code	0
PID	3856
Parent PID	2544
Bitness	32 Bit

Host Behavior

Type	Count
System	4
Module	1
Registry	7
File	5

Network Behavior

Type	Count
UDP	1

Process #53: net.exe

ID	53
File Name	c:\windows\syswow64\net.exe
Command Line	net share
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 133939, Reason: Child Process
Unmonitor End Time	End Time: 135783, Reason: Terminated
Monitor duration	1.84s
Return Code	0
PID	3872
Parent PID	2544
Bitness	32 Bit

Process #54: net1.exe

ID	54
File Name	c:\windows\syswow64\net1.exe
Command Line	C:\Windows\system32\net1 share
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 134096, Reason: Child Process
Unmonitor End Time	End Time: 135782, Reason: Terminated
Monitor duration	1.69s
Return Code	0
PID	3860
Parent PID	3872
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	3
File	39

Process #55: route.exe

ID	55
File Name	c:\windows\syswow64\route.exe
Command Line	route print
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 134758, Reason: Child Process
Unmonitor End Time	End Time: 136202, Reason: Terminated
Monitor duration	1.44s
Return Code	0
PID	3768
Parent PID	2544
Bitness	32 Bit

Process #56: netstat.exe

ID	56
File Name	c:\windows\syswow64\netstat.exe
Command Line	netstat -nao
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 135215, Reason: Child Process
Unmonitor End Time	End Time: 136980, Reason: Terminated
Monitor duration	1.76s
Return Code	0
PID	3852
Parent PID	2544
Bitness	32 Bit

Process #57: net.exe

ID	57
File Name	c:\windows\syswow64\net.exe
Command Line	net localgroup
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 135944, Reason: Child Process
Unmonitor End Time	End Time: 137701, Reason: Terminated
Monitor duration	1.76s
Return Code	0
PID	3928
Parent PID	2544
Bitness	32 Bit

Process #58: net1.exe

ID	58
File Name	c:\windows\syswow64\net1.exe
Command Line	C:\Windows\system32\net1 localgroup
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 136093, Reason: Child Process
Unmonitor End Time	End Time: 137701, Reason: Terminated
Monitor duration	1.61s
Return Code	0
PID	3904
Parent PID	3928
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	3
Module	3
File	45
User	1

Process #59: msiexec.exe

ID	59
File Name	c:\windows\system32\msiexec.exe
Command Line	C:\Windows\system32\msiexec.exe /V
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 141299, Reason: RPC Server
Unmonitor End Time	End Time: 166588, Reason: Terminated
Monitor duration	25.29s
Return Code	0
PID	3948
Parent PID	448
Bitness	64 Bit

Host Behavior

Type	Count
Module	72
System	43

Process #63: cmd.exe

ID	63
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd /c set
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 245540, Reason: Child Process
Unmonitor End Time	End Time: 246710, Reason: Terminated
Monitor duration	1.17s
Return Code	0
PID	1708
Parent PID	1400
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	143

Process #65: ipconfig.exe

ID	65
File Name	c:\windows\syswow64\ipconfig.exe
Command Line	ipconfig /all
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 245904, Reason: Child Process
Unmonitor End Time	End Time: 247335, Reason: Terminated
Monitor duration	1.43s
Return Code	0
PID	3980
Parent PID	1400
Bitness	32 Bit

Host Behavior

Type	Count
System	9
Module	1
File	91
COM	1
-	3
Registry	4

Process #67: nslookup.exe

ID	67
File Name	c:\windows\syswow64\nslookup.exe
Command Line	nslookup -querytype=ALL -timeout=10 _ldap._tcp.dc._msdcs.WORKGROUP
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 258723, Reason: Child Process
Unmonitor End Time	End Time: 259992, Reason: Terminated
Monitor duration	1.27s
Return Code	0
PID	3100
Parent PID	1400
Bitness	32 Bit

Host Behavior

Type	Count
System	4
Module	1
Registry	7
File	5

Network Behavior

Type	Count
UDP	1

Process #68: net.exe

ID	68
File Name	c:\windows\syswow64\net.exe
Command Line	net share
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 258979, Reason: Child Process
Unmonitor End Time	End Time: 260432, Reason: Terminated
Monitor duration	1.45s
Return Code	0
PID	3764
Parent PID	1400
Bitness	32 Bit

Process #69: net1.exe

ID	69
File Name	c:\windows\syswow64\net1.exe
Command Line	C:\Windows\system32\net1 share
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 259105, Reason: Child Process
Unmonitor End Time	End Time: 260298, Reason: Terminated
Monitor duration	1.19s
Return Code	0
PID	3476
Parent PID	3764
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	3
File	39

Process #72: net.exe

ID	72
File Name	c:\windows\syswow64\net.exe
Command Line	net localgroup
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 259994, Reason: Child Process
Unmonitor End Time	End Time: 261340, Reason: Terminated
Monitor duration	1.35s
Return Code	2
PID	3092
Parent PID	1400
Bitness	32 Bit

Process #73: net1.exe

ID	73
File Name	c:\windows\syswow64\net1.exe
Command Line	C:\Windows\system32\net1 localgroup
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 260121, Reason: Child Process
Unmonitor End Time	End Time: 261312, Reason: Terminated
Monitor duration	1.19s
Return Code	2
PID	1860
Parent PID	3092
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	3
File	10
User	1

Process #74: msiexec.exe

ID	74
File Name	c:\windows\system32\msiexec.exe
Command Line	C:\Windows\system32\msiexec.exe /V
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 260918, Reason: RPC Server
Unmonitor End Time	End Time: 271702, Reason: Terminated by Timeout
Monitor duration	10.78s
Return Code	Unknown
PID	2760
Parent PID	448
Bitness	64 Bit

Host Behavior

Type	Count
Module	66
System	43

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969	C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll	Dropped File	378.00 KB	application/vnd.microsoft.portable-executable	Write, Access, Read, Create	MALICIOUS
17d261eaca2629ef9907d0c00fb2271201e466796f06dcb7232900d711c29330	C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll	Dropped File	378.00 KB	application/vnd.microsoft.portable-executable	Write, Access, Read, Create	CLEAN
6967fc3dfaeaf0d1ff656ebe62ce114ea2a92dc32ad99fe19e255be3665d1cc2	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	184 bytes	text/plain	-	CLEAN
2842973d15a14323e08598be1dfb87e54bf88a76be8c7bc94c56b079446edf38	c:\windows\syswow64\config\systemprofile\appdata\local\microsoft\windows\temporary internet files\content.ie5\a23kvyay\desktop.ini	Dropped File	67 bytes	application/x-wine-extension-ini	-	CLEAN
3d249db46b4bd1cfae8f56b272f7116b218ac9d64225d1109751ee487fa9f3ae	authroot.stl	Embedded File	157.23 KB	application/octet-stream	-	CLEAN
62f2df959ba7b4e526f6cf6e7fb34ffd55717603c5b29b3f7f64f79ad93d895d	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	96 bytes	text/plain	-	CLEAN
a425c1e63bdb66c592d651c0009470b1b20a2fca9cd42362d474b71ad24cd575	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	832 bytes	text/plain	-	CLEAN
94ec44d89755cd8a104eebc4cffd3beae846d9a9840023f3a77f795be9d1ba5f	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	872 bytes	text/plain	-	CLEAN
2914df66053dd1612fee35b5041ed5fd61724f48eadef2182c717f8ab84228f6	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	752 bytes	text/plain	-	CLEAN
3ed9d7cc09f8ef0f09b4f9b7d41cc39fe01f9e2af75ed307f696a83cb0113b4f	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	740 bytes	text/plain	-	CLEAN
7bfd337714c3ec96ced3983d3e206736fcf47a5240a7184ccdda6a3136ebc312	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	764 bytes	text/plain	-	CLEAN
3f5207337ff8bb0963011de2fb3b1ed1587be48278a83a9e80b1ec5eac2fad42	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.19 KB	text/plain	-	CLEAN
378cdde06fe842afa25160f372eec804eca7699b3f4198cab25b52f8ec02b6e4	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.20 KB	text/plain	-	CLEAN
3c60e6057455ec0992d5418e25f17c965368ec4dbea78c07cfe950042854003c	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	700 bytes	text/plain	-	CLEAN
8a5b00d743d4033d8dbc3eea3158ff5e927876d418ee5716cd7f886e1d487fe7	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	688 bytes	text/plain	-	CLEAN
8184165e644de0fc2aadb9ca0372969730d583e5edc37096ccf2be95e2ec5e6c	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	804 bytes	text/plain	-	CLEAN
65c2055621ae8f4112de9fabd71656580378f460b255842b56244f8e69482519	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	672 bytes	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
de27dc3c8e753594f393e5b46930a5f5716504ad350d78362779050ff5a284b1	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	740 bytes	text/plain	-	CLEAN
b8844924cb201b58e9882609df6968f5f8dba5c479591588aaadbc5a9d966318	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	632 bytes	text/plain	-	CLEAN
089298dd9955d114593defabe74283b6711a2c7cd3e082b1231ee852400498a8	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	588 bytes	text/plain	-	CLEAN
d8795506bd2f368fd2442e3c7b85cbcdc7a11550dc60b19805d50e1c564074be	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.13 KB	text/plain	-	CLEAN
f1f8040b3229d13e729a6bd7f4fe0f3bbab3e53149213ed6118517e4008986f6	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	900 bytes	text/plain	-	CLEAN
4bbb59462e7b4fbaafc8497bf6045c2d48b1695f05dc2fa58ed474c14b9cc3b4	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.09 KB	text/plain	-	CLEAN
cfaab4877ee2c5e6d3de409166ad490889a012cae1b2ea583b4f6770c25e941c	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.18 KB	text/plain	-	CLEAN
25967f957c17ce21c7549aa48948155a56308c0f40cbfc1a83bcb093dc40c6ab	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	584 bytes	text/plain	-	CLEAN
66f71c2a1ddc2cfe1d7c4845392756b75227f9c5c13064ba9e7bfd7153df56ec	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	584 bytes	text/plain	-	CLEAN
d839448622e34f0c06e623ba7fc3fcc57b13914829b836bfe2e37b451cec5638	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	660 bytes	text/plain	-	CLEAN
90ddad000b834b7071bdde8aff3ac72baaf3dc7bb8e8eaecbf5f06922a7c526d	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	580 bytes	text/plain	-	CLEAN
329ebc4079b9f52a650820d60f56e5a90bc5e3d946ae892b5831d1a8ce88e013	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	668 bytes	text/plain	-	CLEAN
4b098e4adda352f0dad1884ce79a221eb856a9db88624dbae94a548aa1abb553	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	732 bytes	text/plain	-	CLEAN
5bb32eccfa27ac9210d687fd52e37b5ca26fc53dcff09c5627c27286f02df0c9	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	744 bytes	text/plain	-	CLEAN
69b084deca6f02b3aaf5f1a9b5305d191197b4f9b3e47306d7e2fc69448ece54	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	640 bytes	text/plain	-	CLEAN
01ff90e901b8914ff3275cdfac897b6e08ef007675dd095238224157b18df8c5	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.02 KB	text/plain	-	CLEAN
4561419960bc2b4858a22d0852cb333b1a9b9714c2211c3519ccf2048eba4968	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	876 bytes	text/plain	-	CLEAN
f22b05f22db93ca9d915be8abf0fc23d7c7bbf4ed690e8e0a375a4abff6ad8a1	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	712 bytes	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6c150b82b2601582bd73213a335baac82fa21433f387145ff4eaaf51adac478f	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	572 bytes	text/plain	-	CLEAN
3c256a0b06c9f16e33de22ddbb8e3e67549fb7b8ab8cd3adeff1f8d04b711c3f	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	908 bytes	text/plain	-	CLEAN
6025e84fb6fa8d3459a5c8aecc3dd6993a0bda5bea2e1b0ce37c2a857978bc63	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1020 bytes	text/plain	-	CLEAN
f090b20634d887264e4093055dda3a7c50140014e0e4cef66a313e5e71b850d6	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	700 bytes	text/plain	-	CLEAN
42b107356f85fe512ca70d14e06ff72041761eab8c42e9df14c0ceb6e889be95	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	724 bytes	text/plain	-	CLEAN
c5384fba03d42908df45c6df3a42ee4226d0340d506d6ddb66a3fdc6be28dfac	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	988 bytes	text/plain	-	CLEAN
01fd8c295cb1b46eb8149829abb4de932d3a636e2e6acd1f43bf59e9c5332c04	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	808 bytes	text/plain	-	CLEAN
69d860b7492408ff84d89e5f7f534452ec619c205f7018d13bbaa4a890d62953	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	732 bytes	text/plain	-	CLEAN
b0421ff4f7d9f4a6e69760e1b97d2336e6a0b01c08e79038e18ec4d3b23699f6	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.01 KB	text/plain	-	CLEAN
ec5412edf00277993f7525894882c520083973d99223bf28e289352ef932c30a	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.19 KB	text/plain	-	CLEAN
780d1c0b6424410e8fa0a9f7174b5e0504579a73be1b23c5900ff87b60e6d062	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	744 bytes	text/plain	-	CLEAN
7d592cc9452c1fd9e7f4af929513c732239b208463791c0f5c8e4ac4114559a5	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.08 KB	text/plain	-	CLEAN
8f633797484fbaca1e0747844f85935d92f72d6a1b100357b1e4e5ecf565f0c6	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	960 bytes	text/plain	-	CLEAN
4bd644d479189c0db51ed6510ba5aeadebe20497f8a103a04fbd20bf442cce4a	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	852 bytes	text/plain	-	CLEAN
352c53d284d4cb4c99b8ef4a47cb59373979ee511cfde170f49ceeaa660bd0ba	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	948 bytes	text/plain	-	CLEAN
efbe7dd9d2084015b810919790b2995d5c1d8158880d777b3702519a50fc3e8f	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.20 KB	text/plain	-	CLEAN
94d0ca8b726d21c1ea1c57049a3ea3e31cb73151824d9fe984e7972d941945f7	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.10 KB	text/plain	-	CLEAN
747951de356479f06e1ec3be37e6ae88297a1e4d79b6173566c3176717962a46	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	864 bytes	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
93a6d9a7c2bbecfb11033630327b84f33da2e22956e3e19c445b8f1fe38921e2	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.02 KB	text/plain	-	CLEAN
a9cbacd88514de1ccec836c24b6aa099104bfbe1533f3b7afb596e2537fe8ae1	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.08 KB	text/plain	-	CLEAN
f4ee736fbc5b02122f9eaab49447235a76d00e1b9b5abd5b1ad04fb40f7d239b	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	776 bytes	text/plain	-	CLEAN
b4b0cf5f0feface2baf1e9cf4a0f8f6f987ada80ddf1ab0fb1dc72adf75f4c8a	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.20 KB	text/plain	-	CLEAN
e0931e407a2bb39f3690fb437058cfac00deeef8aef8a07682d5a19a33d082a3	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.19 KB	text/plain	-	CLEAN
a89f28ff0493fc67512ebe6e3b279dfe2006bf7c8b55b996e3e845573a9091cf	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	932 bytes	text/plain	-	CLEAN
859cb26c0e17977a980241e9cd7e1e4e991224e75e3458358828b9d418fb1233	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	976 bytes	text/plain	-	CLEAN
cbbdeb28df90dfe3395aaf8d6c4271a87e5476eb161a73d9f07cb1d1a937c035	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	688 bytes	text/plain	-	CLEAN
bd061ef0da493a63f8ecb7126d59fcf37fbc1954ea5fcee54296a5e4dd6a74db	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	884 bytes	text/plain	-	CLEAN
5c5f747341fbf0859aeb5c276dd5b343571f02597a3a79b89bd39329c615ba9a	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.15 KB	text/plain	-	CLEAN
802655a077efd4c8e8e39a4f31eb026b72e3a5b213694186c1db5d6f359e1066	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.12 KB	text/plain	-	CLEAN
2b86011d070e041616b570eb69bf456a544690d9593369df53c277b178a3bbdc	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	576 bytes	text/plain	-	CLEAN
2372126c451d3f79ddfb4514ba717141d4fcbc5ce81fabf421fa52935f66577e	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.19 KB	text/plain	-	CLEAN
d7e126a531f2c9f38b2e1f05297339df6f7f3a7bebae25e1072248c0b3591a47	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	616 bytes	text/plain	-	CLEAN
cb3eb2d31d4ed16ba87506d80f9d7aa00f84dd445ad8120ad7511a842f29be7a	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	576 bytes	text/plain	-	CLEAN
ee9742683b7d6f508512b1c0171ffa50ec0e08ada82d66d4f3acd7c8afed724b	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1004 bytes	text/plain	-	CLEAN
0df5457272b590e47a0945d175ed5a50dd6fcd5eef72bb11b022cfa4b7106724	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.19 KB	text/plain	-	CLEAN
bf2c1327abb7c89b8e350b3ca6a72d3d66d6d7ad08183492cf4ca3dab7112741	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	820 bytes	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a22be379a72f80027c32b82adcaf4580c9f8c317dc5197068fd5d6b135bf8bd2	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	888 bytes	text/plain	-	CLEAN
672222e2a1a49c8b4dcf33087b734f26d5ab7da02b1bfa2b0453f08f62475fcb	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.16 KB	text/plain	-	CLEAN
ff344daa261f431886844c621c96a0e2d98006d1c86df9385a49ce1409f2f4b6	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	604 bytes	text/plain	-	CLEAN
0ddc3ee0b381ac20265d5ff0e942327fc26428bca48e07b4b9c6cd4a90ea1931	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.12 KB	text/plain	-	CLEAN
2bec6888128a5698ab3874ce6376e83f0f63b11ac09df152d13913af89f7bb79	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	588 bytes	text/plain	-	CLEAN
06ec5b8e097376516b55c468363d154f175cf79bd17fd37685c2dd538b8eb64e	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	628 bytes	text/plain	-	CLEAN
6a26b3e8d42522298c86cf33405b4b688d8728c21b9307a3d237103032cd5b64	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	904 bytes	text/plain	-	CLEAN
9ac3643a0730f6e901e95bcd0d8fb9f5428e648e8562805384bedca06e22b7a0	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	972 bytes	text/plain	-	CLEAN
2ecb90fe7e1321ab5da72eda541e78d7ef999f04ab8a163c10c1166963dd7b2b	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	876 bytes	text/plain	-	CLEAN
a77cb61a7d73bad2d570fe34c1f7669c3b635b023abc0741aaa5b50540d634b4	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.05 KB	text/plain	-	CLEAN
a004c8d7784259a26dba530247767c5b9833f49b89a842c7d60efb2030c0aa5a	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	576 bytes	text/plain	-	CLEAN
fb229203706d0fe73dc9be52b22f9960b3b384348dd254a646a7715f038de675	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	572 bytes	text/plain	-	CLEAN
d9c5a389c2142809a9d6a6d38c0da0fcd1485b638d09c157156112f7d8c85a49	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.11 KB	text/plain	-	CLEAN
6c7616f333d1605156db02c8018ae2d78796933fceff1650f0b4250ae20d6d59	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.02 KB	text/plain	-	CLEAN
332a6ae8f80aee84d48aa71c17558ae96dbb1bb014cc15e28cda6d6b4ad640d3	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	580 bytes	text/plain	-	CLEAN
732f68c64d1c0e73c0a08706293f2adda0600a5564fcd9a0336239d9dca4b09c	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	788 bytes	text/plain	-	CLEAN
609317ae077d0e7d0bbf19275697970ad4df3680f30cd5f03a83b6fe48f99111	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.18 KB	text/plain	-	CLEAN
788f62baf4d594d62ff6e16999b94af302b22be2c7ca98649b8e769db4d4f887	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	740 bytes	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
52738accb94fb23253059288623f05eecbb258232f0f6e4b1665bfc16b2b8cd8	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.20 KB	text/plain	-	CLEAN
8fc6fcbfc652e7671d6bbdbf869abdeed7fb7a0bd2cfd99763dff677a82b0a6e	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	716 bytes	text/plain	-	CLEAN
9e1ab262d151e08925c794150d62afe02baa77f61675b07b17dfc7976df9f5d4	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	840 bytes	text/plain	-	CLEAN
cbd9ec8d1d2c5ebfa69650ea70ae1d5a16dde399ad934eebd1f1b9e0681ceb96	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	624 bytes	text/plain	-	CLEAN
7122466044329cbd1c6bc8343c11812b83def33228308bbe836b32c4be4fba29	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	776 bytes	text/plain	-	CLEAN
f5f8f20153e7b0ea70ed01e25a9c8c00339c7ae5aea962eac927a62744a87fdb	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.21 KB	text/plain	-	CLEAN
06a6691701fcb5eff9ab2c6fbaf5c5f141612c6d15530429e4a6eb65caa64588	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	812 bytes	text/plain	-	CLEAN
8fea1adcbd1b446ceffcc07acf35e5aaa5905c101fc3accf2659de6d6449ec7c	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	664 bytes	text/plain	-	CLEAN
7f0f5bd3f16808cc9e6764ce5089a526183984339a98ebf9accd19a2beee3b6c	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	832 bytes	text/plain	-	CLEAN
ddbd4e254a4cf5a0fb071f9e65ce7885bc543508d4b5351dba68f6f9244081a4	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.13 KB	text/plain	-	CLEAN
55b6d4245b6be4e04aa97bfb4062d63e7f954fce1feccffda6f5ff861d1b6990	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	824 bytes	text/plain	-	CLEAN
3d58547facead0572c750c60f316c33d1133b03310714ad437dfc1c465b1161f	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1012 bytes	text/plain	-	CLEAN
5c1b5bf53aca6765fcabd2824c57100e8f6c81e0066250771fdc0b0a70aee5ad	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	792 bytes	text/plain	-	CLEAN
b7b58effa85964b0d14bc59ea54cb0e95fd64135d7ec5e11d272c981420a44a4	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	980 bytes	text/plain	-	CLEAN
b90b46bb74c4c20f88a92a95bae5f7d356e21f9b04a160fbb2f65339c0768762	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.05 KB	text/plain	-	CLEAN
f05d81e2ff891b17819a928cf5ebfa93d08f304602aea9a2c29a20b74565dbf2	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.14 KB	text/plain	-	CLEAN
5ff797c05b398de48ae6e34e14bf0014f38a696d4cb8329ae04cbe553b83bb80	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	864 bytes	text/plain	-	CLEAN
72c8f06540e7a58a76e854b68d8195a7aebae3ad9df751c877f96d64c62bebcd	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	872 bytes	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9df48405bb7a356eb1d4447f888c6db604dc24c6a4e6da4142a6e3e3cb5ee996	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.21 KB	text/plain	-	CLEAN
00206ea3d0fb8cb7b10b6f3b8e2b2889cdedac264a286c55d5ecdf25f1de5c60	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\t4[1]	Dropped File	1.18 KB	text/plain	-	CLEAN
71d7b2ceb630b9c0402673c02c400829b3992381d1b2a5719474f88c2965aa92	c:\windows\syswow64\config\systemprofile\appdata\local\microsoft\windows\temporary internet files\content.ie5\a23kvyay\t4[1]	Downloaded File	124 bytes	text/plain	-	CLEAN
f8e90fb0557fe49d7702cfb506312ac0b24c97802f9c782696db6d47f434e8e9	c:\users\keecfmwgj\appdata\local\temp\cab32e5.tmp	Downloaded File	59.72 KB	application/vnd.ms-cab-compressed	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\tmpb141g1rs	Accessed File	Access, Read	CLEAN
C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll	Dropped File	Write, Access, Read, Create	CLEAN
C:\INTERNAL__empty	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\explorer.exe	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\amstream.dll	Accessed File	Access, Read	CLEAN
C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll.cfg	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Mqloaubiwjuo	Accessed File	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Mqloaubiwjuo\xpgxmeky.dvv	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\regsvr32.exe	Accessed File	Access	CLEAN
C:\ProgramData\Microsoft\Cuaohnwer	Accessed File	Access, Create	CLEAN
C:\ProgramData\Microsoft\Cuaohnwer\mnqfikbirm.jdz	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\net1.exe	Accessed File	Access	CLEAN
c:\hiberfil.sysss	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Mqloaubiwjuo\cgyquyp32.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Mqloaubiwjuo\gyquyp32.dll	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://24.229.150.54/t4	-	24.229.150.54	-	POST	MALICIOUS
https://96.37.113.36/t4	-	96.37.113.36	-	POST	MALICIOUS
https://140.82.49.12/t4	-	140.82.49.12	-	POST	MALICIOUS
https://120.151.47.189/t4	-	120.151.47.189	-	POST	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://103.148.120.144/t4	-	103.148.120.144	-	POST	CLEAN
https://2.188.27.77/t4	-	2.188.27.77	-	POST	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
140.82.49.12	-	United States	TLS, TCP	MALICIOUS
127.0.0.1	-	-	-	CLEAN
192.168.0.1	-	-	UDP, DNS	CLEAN
24.229.150.54	-	United States	TLS, TCP	CLEAN
103.148.120.144	-	India	TCP, HTTP	CLEAN
2.188.27.77	-	Iran	TLS, TCP, HTTP	CLEAN
120.151.47.189	-	Australia	TCP, HTTPS	CLEAN
96.37.113.36	-	United States	TCP, HTTP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}	access	explorer.exe	CLEAN
{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}	access	explorer.exe	CLEAN
{14A78D04-6F1A-4927-AECE-0EE9DEB87429}	access	explorer.exe	CLEAN
Global\{F9B41FAF-4994-487E-87C0-862C1DC89AD9}	access	explorer.exe	CLEAN
{F9B41FAF-4994-487E-87C0-862C1DC89AD9}	access	explorer.exe	CLEAN
cllysffhhoemybawevnr	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\C:\ProgramData\Microsoft\Cuaohnwer	write, access, read	reg.exe	SUSPICIOUS
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Mqloaubiwjuo	write, access, read	reg.exe	SUSPICIOUS
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\ec6e59d3	write, access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-4219442223-4223814209-3835049652-1000	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-4219442223-4223814209-3835049652-1000\ProfileImagePath	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\d9f1899d	write, access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\ee2f79af	write, access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\56931eca	write, access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\2b9b5140	write, access, read	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\93273625	write, access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-4219442223-4223814209-3835049652-500	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-4219442223-4223814209-3835049652-501	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\1e04810e	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\54d23eb6	write, access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\a6b8e66b	write, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\a4f9c617	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\71b9616a	write, access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\6b76894d	write, access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\79c326a3	write, access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\b40d4985	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{2E4C7576-F100-4C39-A70C-5E6D4E6BF9B7}	access	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{2E4C7576-F100-4C39-A70C-5E6D4E6BF9B7}\DhcpcvClassId	access, read	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{2E4C7576-F100-4C39-A70C-5E6D4E6BF9B7}	access	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{2E4C7576-F100-4C39-A70C-5E6D4E6BF9B7}\DhcpClassId	access, read	ipconfig.exe	CLEAN
HKEY_CLASSES_ROOT\.dll	access, read	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\dllfile	access	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\dllfile\AutoRegister	access	regsvr32.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup	access, create	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\cee47b30	access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\a1599b54	write, access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths	access, create	reg.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\94c64b1a	write, access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\a318bb28	write, access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\1ba4dc4d	write, access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\66ac93c7	write, access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\de10f4a2	write, access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\5333438 9	access, read	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\19e5fc31	write, access	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\eb8f24ec	write, access	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\e9ce0490	access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\3c8ea3ed	access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\26414bca	access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\34f4e424	access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\f93a8b02	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters	access	nslookup.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DNSLookupOrder	access, read	nslookup.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Domain	access, read	nslookup.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DhcpDomain	access, read	nslookup.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\DNSClient	access	nslookup.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SearchList	access, read	nslookup.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DhcpSearchList	access, read	nslookup.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\4426b124	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\4cb6929	write, access	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
explorer.exe	C:\Windows\SysWOW64\explorer.exe	SUSPICIOUS
schtasks.exe	"C:\Windows\system32\schtasks.exe" /Create /RU "NT AUTHORITY\SYSTEM" /tn lmtrjjbrh /tr "regsvr32.exe -s \"C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll\"" /SC ONCE /Z /ST 21:19 /ET 21:31	SUSPICIOUS
ipconfig.exe	ipconfig /all	SUSPICIOUS
regsvr32.exe	-s "C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll"	SUSPICIOUS
reg.exe	C:\Windows\system32\reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /f /t REG_DWORD /v "C:\ProgramData\Microsoft\Cuaohnwer" /d "0"	SUSPICIOUS
reg.exe	C:\Windows\system32\reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /f /t REG_DWORD /v "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Mqloaubiwjuo" /d "0"	SUSPICIOUS
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmpb141g1rs" /s	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass	CLEAN

Process Name	Commandline	Verdict
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="0"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="0"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="1"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="1"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="Install"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="Install"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="DefaultInstall"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="DefaultInstall"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="127.0.0.1"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="127.0.0.1"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="explorer.exe"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="explorer.exe"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="iexplore.exe"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="iexplore.exe"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=GetClass /fn_args="%Temp%\IXP000.TMP\"	CLEAN
dadjtxjf.exe	"C:\Users\kEecfMwgj\Desktop\daDJtXJF.exe" /dll="C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll" /fn_id=SetClass /fn_args="%Temp%\IXP000.TMP\"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -Embedding	CLEAN
taskeng.exe	taskeng.exe {C9CD2011-1E8F-43F4-974C-D55AEA23B22B} S-1-5-18:NT AUTHORITY\System:Service:	CLEAN
whoami.exe	whoami /all	CLEAN
cmd.exe	cmd /c set	CLEAN
arp.exe	arp -a	CLEAN
net.exe	net view /all	CLEAN
regsvr32.exe	regsvr32.exe -s "C:\Users\KEECFM~1\Desktop\b5bac95d38c0b9a246cf01fd76276870c42bdb38e2c5bab7d47ae04f1c52e969.dll"	CLEAN
nslookup.exe	nslookup -querytype=ALL -timeout=10 _ldap._tcp.dc._msdcs.WORKGROUP	CLEAN

Process Name	Commandline	Verdict
net.exe	net share	CLEAN
net1.exe	C:\Windows\system32\net1 share	CLEAN
route.exe	route print	CLEAN
netstat.exe	netstat -nao	CLEAN
net.exe	net localgroup	CLEAN
net1.exe	C:\Windows\system32\net1 localgroup	CLEAN
msiexec.exe	C:\Windows\system32\msiexec.exe /V	CLEAN

YARA / AV

Antivirus (1)

File Type	Threat Name	File Name	Verdict
Memory Dump	Gen:Variant.Bulz.604474	-	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	2021-09-27 18:53:08+00:00
Built-in AV Database Records	10474020

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