MALICIOUS

Classifications: Spyware

Threat Names: Trojan.GenericKDZ.76753 | Gen:Variant.Mikey.113998

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll**
ID	#2782988
MD5	94f8317b419e9476120b14a29d9b05d2
SHA1	f2b03dd4441f3808468bdbb8b26273cfb41b5298
SHA256	2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862
File Size	1208.00 KB
Report Created	2021-09-28 14:38 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (16 rules, 197 matches)

Score	Category	Operation	Count	Classification
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #2) jlbxcalqx.exe alters context of (process #14) explorer.exe.			
4/5	Privilege Escalation	Creates elevated child process	1	-
	• (Process #14) explorer.exe creates (process #108) recdisc.exe with elevated privileges.			
4/5	Antivirus	Malicious content was detected by heuristic scan	10	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.76753". • Built-in AV detected the dropped file C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\OLEACC.dll as "Trojan.GenericKDZ.76753". • Built-in AV detected the dropped file C:\Users\kEecfMwgj\AppData\Local\aAIRi\WTSAPI32.dll as "Trojan.GenericKDZ.76753". • Built-in AV detected the dropped file C:\Users\kEecfMwgj\AppData\Local\kza5B6\slc.dll as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #3) jlbxcalqx.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #14) explorer.exe as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #40) jlbxcalqx.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #46) jlbxcalqx.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #97) snippingtool.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #106) psr.exe as "Gen:Variant.Mikey.113998".			
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #14) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Hide Tracks	Deletes file after execution	3	-
	• (Process #14) explorer.exe deletes executed executable "c:\users\keecfmwgj\appdata\local\j6eppj\snippingtool.exe". • (Process #14) explorer.exe deletes executed executable "c:\users\keecfmwgj\appdata\local\aalri\psr.exe". • (Process #14) explorer.exe deletes executed executable "c:\windows \system32\recdisc.exe".			
2/5	Task Scheduling	Schedules task	1	-
	• Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Office\CuPXu597CI\psr.exe", to be triggered by Time. Task has been rescheduled by the analyzer.			
1/5	Discovery	Reads system data	47	-

Score	Category	Operation	Count	Classification
		• (Process #3) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #2) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #4) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #5) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #6) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #7) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #8) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #9) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #10) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #11) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #12) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #13) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #15) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #16) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #17) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #18) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #19) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #20) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #21) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #22) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #23) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #24) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #25) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #26) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #27) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #28) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #29) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #30) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #31) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #32) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #33) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #14) explorer.exe reads the Windows installation date from registry. • (Process #35) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #38) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #39) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #51) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #37) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #52) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #47) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #57) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #83) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #89) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #50) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #58) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #64) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #72) jlbxcalqx.exe reads the Windows installation date from registry. • (Process #54) jlbxcalqx.exe reads the Windows installation date from registry.		
1/5	Mutex	Creates mutex	100	-

- (Process #3) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #2) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #4) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #2) jlbxcalqx.exe creates mutex with name "{ba62725d-6184-50d2-b706-2d7b865dd82b}".
- (Process #3) jlbxcalqx.exe creates mutex with name "{ba62725d-6184-50d2-b706-2d7b865dd82b}".
- (Process #5) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #6) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #7) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #8) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #9) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #10) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #11) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #12) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #13) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #15) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #16) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #18) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #17) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #19) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #20) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #21) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #22) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #23) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #24) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #25) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #26) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #27) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #28) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #29) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #30) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #31) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #32) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #33) jlbxcalqx.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #14) explorer.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #14) explorer.exe creates mutex with name "{33ff21cb-ff8c-80f2-435a-9f14e40fde6b}".
- (Process #14) explorer.exe creates mutex with name "{ad66cb9e-7ae1-701b-6069-4a7b793507ac}".
- (Process #14) explorer.exe creates mutex with name "{6ae03f50-7a2d-c6e9-ca75-492d6e54c058}".
- (Process #14) explorer.exe creates mutex with name "{13e06e4b-2481-b368-8f42-2212f1d59822}".
- (Process #14) explorer.exe creates mutex with name "{65c8ac9c-25ba-82f3-37f2-3fe3857eeb82}".
- (Process #14) explorer.exe creates mutex with name "{78fd2f71-b653-7ea3-c562-0b3dc695dbfd}".
- (Process #14) explorer.exe creates mutex with name "{ef30bf64-6e77-af44-2844-a272c4a251e4}".
- (Process #14) explorer.exe creates mutex with name "{d0c8c370-4e74-9e4a-c235-fabccc75324d}".
- (Process #14) explorer.exe creates mutex with name "{93f0b9bd-750b-91aa-43ce-42ee557a016a}".
- (Process #14) explorer.exe creates mutex with name "{0a229cb1-bb57-9bd8-01b2-31e4b7cbf515}".
- (Process #14) explorer.exe creates mutex with name "{4126ed8b-1649-b296-c1a8-6a31b31e936e}".
- (Process #14) explorer.exe creates mutex with name "{50a49a66-4b11-240c-8816-398b6bd70ed6}".
- (Process #14) explorer.exe creates mutex with name "{2d7bccd8-c070-8723-c092-31c38068d849}".
- (Process #14) explorer.exe creates mutex with name "{aa8eec2a-1624-d913-f987-9558cbeacce1}".
- (Process #14) explorer.exe creates mutex with name "{9124fc0f-aad1-69ca-f087-b6f4b4618452}".
- (Process #14) explorer.exe creates mutex with name "{3424d05e-75d9-fa9d-601e-13c62053c3c5}".
- (Process #14) explorer.exe creates mutex with name "{91af0379-7553-2b9a-1768-bb6f0281e3e9}".
- (Process #14) explorer.exe creates mutex with name "{821b3d72-6d45-a55c-2ff2-657dbbeba155}".
- (Process #14) explorer.exe creates mutex with name "{87870dec-87d4-3464-8983-690c1429eba9}".
- (Process #14) explorer.exe creates mutex with name "{9a382e7d-fa1b-dd43-a0dd-294ace4cebfc}".
- (Process #14) explorer.exe creates mutex with name "{8da6b341-b6ae-4ed6-a4db-b8d7a21d3ce2}".
- (Process #14) explorer.exe creates mutex with name "{9da07381-49bd-fcd5-49f0-db565310a644}".
- (Process #14) explorer.exe creates mutex with name "{d3b3213a-9735-bc53-9894-9fb345059836}".
- (Process #14) explorer.exe creates mutex with name "{65b97bfc-3a12-e27a-fd30-cf51840b6a30}".
- (Process #14) explorer.exe creates mutex with name "{6b15b196-f9d7-4a9c-57e8-3bbe0bf6efc5}".
- (Process #14) explorer.exe creates mutex with name "{46ea2b8d-13ef-8da4c95d28262917f001}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #2) jlbxcalqx.exe reads from (process #14) explorer.exe.			
1/5	Hide Tracks	Creates process with hidden window	16	-
	• (Process #14) explorer.exe starts C:\Windows\system32\hdwwiz.exe with a hidden window. • (Process #14) explorer.exe starts (process #94) snippingtool.exe with a hidden window. • (Process #14) explorer.exe starts C:\Windows\system32\iscsicpl.exe with a hidden window. • (Process #14) explorer.exe starts (process #96) lpksetup.exe with a hidden window. • (Process #14) explorer.exe starts (process #97) snippingtool.exe with a hidden window. • (Process #14) explorer.exe starts C:\Windows\system32\rstrui.exe with a hidden window. • (Process #14) explorer.exe starts C:\Windows\system32\MultiDigiMon.exe with a hidden window. • (Process #14) explorer.exe starts (process #100) psr.exe with a hidden window. • (Process #14) explorer.exe starts (process #101) newdev.exe with a hidden window. • (Process #14) explorer.exe starts C:\Windows\system32\ntprint.exe with a hidden window. • (Process #14) explorer.exe starts C:\Windows\system32\ocsetup.exe with a hidden window. • (Process #14) explorer.exe starts C:\Windows\system32\odbcad32.exe with a hidden window. • (Process #14) explorer.exe starts C:\Windows\system32\recdisc.exe with a hidden window. • (Process #14) explorer.exe starts (process #106) psr.exe with a hidden window. • (Process #14) explorer.exe starts (process #108) recdisc.exe with a hidden window. • (Process #14) explorer.exe starts (process #110) unregmp2.exe with a hidden window.			
1/5	Hide Tracks	Writes an unusually large amount of data to the registry	1	-
	• (Process #14) explorer.exe hides 3600 bytes in "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{71BC1377-8B48-A04B-D279-F048DCF94E7E}\ShellFolder\{A9577F80-3C4C-8D64-356D-A45BDAD3C842}".			
1/5	System Modification	Modifies operating system directory	2	-
	• (Process #14) explorer.exe creates file "\\?\C:\Windows \system32\ReAgent.dll" in the OS directory. • (Process #14) explorer.exe creates file "\\?\C:\Windows \system32\recdisc.exe" in the OS directory.			
1/5	Execution	Drops PE file	8	-
	• (Process #14) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\OLEACC.dll". • (Process #14) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\aAlRi\WTSAPI32.dll". • (Process #14) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\kza5B6\slc.dll". • (Process #14) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\SnippingTool.exe". • (Process #14) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\aAlRi\psr.exe". • (Process #14) explorer.exe drops file "\\?\C:\Windows \system32\ReAgent.dll". • (Process #14) explorer.exe drops file "\\?\C:\Windows \system32\recdisc.exe". • (Process #14) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\kza5B6\unregmp2.exe".			
1/5	Execution	Executes dropped PE file	3	-
	• Executes dropped file "C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\SnippingTool.exe". • Executes dropped file "C:\Users\kEecfMwgj\AppData\Local\aAlRi\psr.exe". • Executes dropped file "\\?\C:\Windows \system32\recdisc.exe".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #14) explorer.exe resolves 26 API functions by name.			
-	Trusted	Known clean file	5	-

Score	Category	Operation	Count	Classification
		• File "C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\SnippingTool.exe" is a known clean file. • File "C:\Users\kEecfMwgj\AppData\Local\aAlRi\psr.exe" is a known clean file. • File "\\?\C:\Windows \system32\recdisc.exe" is a known clean file. • File "C:\Users\kEecfMwgj\AppData\Local\kza5B6\unregmp2.exe" is a known clean file. • File "c:\users\keecfmwgj\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-4219442223-4223814209-3835049652-1000\4fe4574abf1bcb0f6ed6a78aa750fb2c_b9c8f16e-2e51-4052-9ecb-f86ae5d96ef6" is a known clean file.		

Mitre ATT&CK Matrix

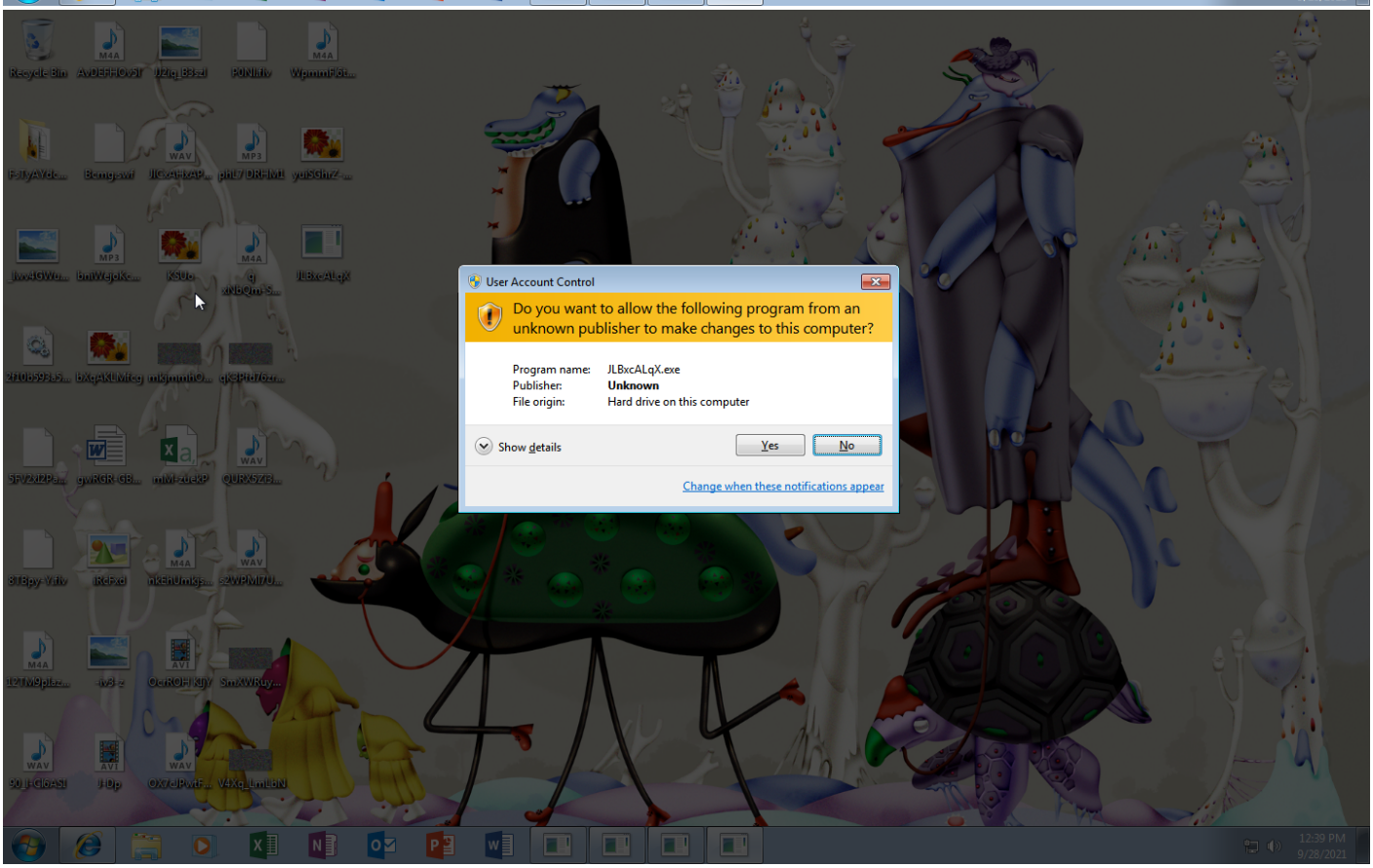
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window		#T1082 System Information Discovery					
				#T1112 Modify Registry		#T1012 Query Registry					
				#T1045 Software Packing							

Sample Information

ID	#2782988
MD5	94f8317b419e9476120b14a29d9b05d2
SHA1	f2b03dd4441f3808468bdbb8b26273cfb41b5298
SHA256	2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862
SSDeep	12288:+VI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:jfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
ImpHash	6668be91e2c948b183827f040944057f
File Name	2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll
File Size	1208.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 14:38 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	111
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	11
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: JLBxcALqX.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
12:39 PM
9/28/2021

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

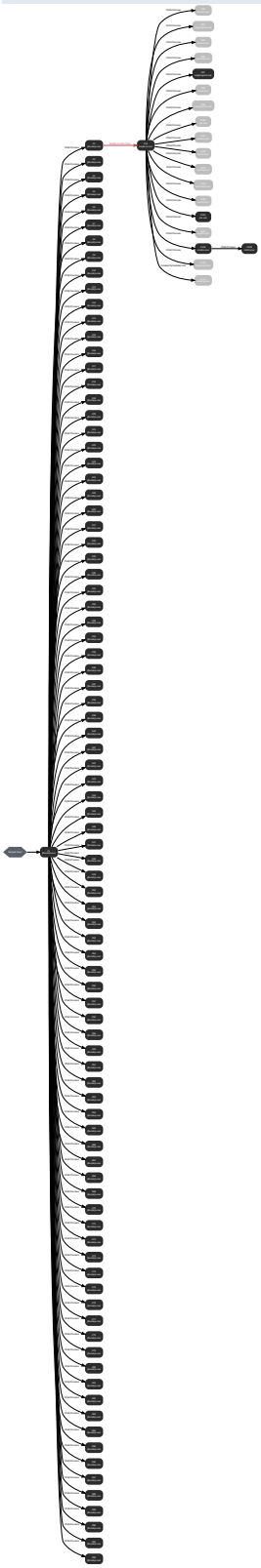
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: jlbxcalqx.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmp67j7r2f9" /s
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 46926, Reason: Analysis Target
Unmonitor End Time	End Time: 125010, Reason: Terminated
Monitor duration	78.08s
Return Code	0
PID	3684
Parent PID	1116
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	8
Environment	1
Process	90

Process #2: jlbxcalqx.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 64031, Reason: Child Process
Unmonitor End Time	End Time: 122170, Reason: Terminated
Monitor duration	58.14s
Return Code	0
PID	3712
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	55
Module	41
File	118
Environment	2
Registry	589
Mutex	6
Process	2
-	66
-	49
-	141

Process #3: jlbxcalqx.exe

ID	3
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65439, Reason: Child Process
Unmonitor End Time	End Time: 74267, Reason: Terminated
Monitor duration	8.83s
Return Code	0
PID	3728
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	6

Process #4: jlbxcalqx.exe

ID	4
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65514, Reason: Child Process
Unmonitor End Time	End Time: 76074, Reason: Terminated
Monitor duration	10.56s
Return Code	0
PID	3740
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #5: jlbxcalqx.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 66026, Reason: Child Process
Unmonitor End Time	End Time: 85370, Reason: Terminated
Monitor duration	19.34s
Return Code	0
PID	3756
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #6: jlbxcalqx.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 66917, Reason: Child Process
Unmonitor End Time	End Time: 85369, Reason: Terminated
Monitor duration	18.45s
Return Code	0
PID	3768
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #7: jlbxcalqx.exe

ID	7
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 67209, Reason: Child Process
Unmonitor End Time	End Time: 87008, Reason: Terminated
Monitor duration	19.80s
Return Code	0
PID	3780
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #8: jlbxcalqx.exe

ID	8
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 68661, Reason: Child Process
Unmonitor End Time	End Time: 88178, Reason: Terminated
Monitor duration	19.52s
Return Code	0
PID	3792
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #9: jlbxcalqx.exe

ID	9
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 68989, Reason: Child Process
Unmonitor End Time	End Time: 88054, Reason: Terminated
Monitor duration	19.07s
Return Code	0
PID	3804
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #10: jlbxcalqx.exe

ID	10
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 71115, Reason: Child Process
Unmonitor End Time	End Time: 88306, Reason: Terminated
Monitor duration	17.19s
Return Code	0
PID	3832
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #11: jlbxcalqx.exe

ID	11
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 71534, Reason: Child Process
Unmonitor End Time	End Time: 89956, Reason: Terminated
Monitor duration	18.42s
Return Code	0
PID	3844
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #12: jlbxcalqx.exe

ID	12
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 75670, Reason: Child Process
Unmonitor End Time	End Time: 91781, Reason: Terminated
Monitor duration	16.11s
Return Code	0
PID	3872
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #13: jlbxcalqx.exe

ID	13
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 76608, Reason: Child Process
Unmonitor End Time	End Time: 92400, Reason: Terminated
Monitor duration	15.79s
Return Code	0
PID	3884
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #14: explorer.exe

ID	14
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 77076, Reason: Injection
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	210.48s
Return Code	Unknown
PID	1116
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (109)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x460	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x4b8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x4bc	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x4cc	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x4d4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x52c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x534	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x540	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x5d8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x478	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x510	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x514	0x777313f0(2004030448)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x51c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x53c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x350	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x354	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x5a4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x1b8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x57c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x238	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x110	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x4b0	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x6c0	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x530	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x824	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x834	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0xcc8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0xcf0	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0xd20	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0xd4c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77732ed0(2004037328)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77732ed0(2004037328)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x460	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x4b8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x4bc	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x4cc	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x4d4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x52c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x534	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x540	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x5d8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x478	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x510	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x514	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x51c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x53c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x350	0x777313f0(2004030448)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x354	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x5a4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x1b8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x57c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x238	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x110	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x4b0	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x6c0	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x530	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x824	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x834	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0xcc8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0xcf0	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0xd20	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0xd4c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x50c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x77526a30(2001889840)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\jlbxcalqx.exe	0xe84 / 0x474	0x77526a60(2001889888)	-	✓	1

Dropped Files (12)

File Name	File Size	SHA256	YARA Match
-	50 bytes	2d970fea1e7ebc4c9bae287309fa032cb2ac90323c0cdb49ca9593dc7d074c98	✗
C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\OLEACC.dll	1212.00 KB	8a2cc9a59220bfafa0ab618dc08f3760f516f0697fc24ad4a5d1f00eba4b01f9	✗
C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\SnippingTool.exe	421.00 KB	890884c7fe7d037e6debd21d1877e9c9c5e7790cdba007ddb219ae6a55667f78	✗
C:\Users\kEecfMwgj\AppData\Local\aAIRi\WTSAPI32.dll	1212.00 KB	f82f912c345800653932585fb15f0991a16b1347daf7cfdf1e36270ca8e6868f	✗
C:\Users\kEecfMwgj\AppData\Local\aAIRi\psr.exe	715.50 KB	68910f8aae867e938b6a3b76cdf176898ba275d9ade85b4ce00b03232de4c495	✗
\\?\C:\Windows \system32\ReAgent.dll	306.50 KB	e2b09cfdead0313843c3dbf5233833c1d9c80a33078bf4739760b64fb1fd524a	✗
\\?\C:\Windows \system32\recdisc.exe	232.50 KB	dcaeb590394b42d180e23e3cef4dd135513395b026e0ed489aec49848b85b8f0	✗
C:\Users\kEecfMwgj\AppData\Local\kza5B6\slc.dll	1212.00 KB	b5e85d4434bbdc83c020f4d1bc70908b76643e8b6a9b8b51c3942d8a6db500c1	✗
C:\Users\kEecfMwgj\AppData\Local\kza5B6\unregmp2.exe	316.00 KB	7d6be433ba7dd4a2b8f8b79d7b87055da8daafa3e0404432d40469c39c2040e1	✗
-	1.40 KB	edc6261c01e8e88b2a9b225e36582e88791b1ca755237819b5d143a5e2a11a91	✗
-	1.40 KB	72275404c470b62a5ff49013e3f952d9480afd5c7e45b6c504235823da4894ae	✗
-	1.42 KB	a650f61765d668cb35df7c2a2f08112f67ef6b5011a14290922cbc7eca79bd3c	✗

Host Behavior

Type	Count
Module	44
File	1780
System	291
Process	29
Registry	30259
Environment	1

Type	Count
-	11
Mutex	10606
-	3
COM	2

Process #15: jlbxcalqx.exe

ID	15
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85969, Reason: Child Process
Unmonitor End Time	End Time: 96882, Reason: Terminated
Monitor duration	10.91s
Return Code	0
PID	3908
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #16: jlbxcalqx.exe

ID	16
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87119, Reason: Child Process
Unmonitor End Time	End Time: 98961, Reason: Terminated
Monitor duration	11.84s
Return Code	0
PID	3928
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #17: jlbxcalqx.exe

ID	17
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 88055, Reason: Child Process
Unmonitor End Time	End Time: 99706, Reason: Terminated
Monitor duration	11.65s
Return Code	0
PID	3944
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #18: jlbxcalqx.exe

ID	18
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 88308, Reason: Child Process
Unmonitor End Time	End Time: 99940, Reason: Terminated
Monitor duration	11.63s
Return Code	0
PID	3956
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #19: jlbxcalqx.exe

ID	19
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89721, Reason: Child Process
Unmonitor End Time	End Time: 101157, Reason: Terminated
Monitor duration	11.44s
Return Code	0
PID	3972
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #20: jlbxcalqx.exe

ID	20
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 90026, Reason: Child Process
Unmonitor End Time	End Time: 101775, Reason: Terminated
Monitor duration	11.75s
Return Code	0
PID	3984
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #21: jlbxcalqx.exe

ID	21
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 92147, Reason: Child Process
Unmonitor End Time	End Time: 102358, Reason: Terminated
Monitor duration	10.21s
Return Code	0
PID	3996
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #22: jlbxcalqx.exe

ID	22
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 92465, Reason: Child Process
Unmonitor End Time	End Time: 103731, Reason: Terminated
Monitor duration	11.27s
Return Code	0
PID	4008
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #23: jlbxcalqx.exe

ID	23
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 95339, Reason: Child Process
Unmonitor End Time	End Time: 105281, Reason: Terminated
Monitor duration	9.94s
Return Code	0
PID	4028
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #24: jlbxcalqx.exe

ID	24
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 97102, Reason: Child Process
Unmonitor End Time	End Time: 106289, Reason: Terminated
Monitor duration	9.19s
Return Code	0
PID	4048
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #25: jlbxcalqx.exe

ID	25
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 98943, Reason: Child Process
Unmonitor End Time	End Time: 107319, Reason: Terminated
Monitor duration	8.38s
Return Code	0
PID	4068
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #26: jlbxcalqx.exe

ID	26
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 100833, Reason: Child Process
Unmonitor End Time	End Time: 110926, Reason: Terminated
Monitor duration	10.09s
Return Code	0
PID	4088
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #27: jlbxcalqx.exe

ID	27
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 101311, Reason: Child Process
Unmonitor End Time	End Time: 111484, Reason: Terminated
Monitor duration	10.17s
Return Code	0
PID	2828
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #28: jlbxcalqx.exe

ID	28
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 103795, Reason: Child Process
Unmonitor End Time	End Time: 118254, Reason: Terminated
Monitor duration	14.46s
Return Code	0
PID	3156
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #29: jlbxcalqx.exe

ID	29
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 104042, Reason: Child Process
Unmonitor End Time	End Time: 120017, Reason: Terminated
Monitor duration	15.97s
Return Code	0
PID	3220
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #30: jlbxcalqx.exe

ID	30
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 105712, Reason: Child Process
Unmonitor End Time	End Time: 120099, Reason: Terminated
Monitor duration	14.39s
Return Code	0
PID	3192
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #31: jlbxcalqx.exe

ID	31
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 106237, Reason: Child Process
Unmonitor End Time	End Time: 120840, Reason: Terminated
Monitor duration	14.60s
Return Code	0
PID	3208
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #32: jlbxcalqx.exe

ID	32
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 107928, Reason: Child Process
Unmonitor End Time	End Time: 120293, Reason: Terminated
Monitor duration	12.37s
Return Code	0
PID	3244
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #33: jlbxcalqx.exe

ID	33
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 109413, Reason: Child Process
Unmonitor End Time	End Time: 120922, Reason: Terminated
Monitor duration	11.51s
Return Code	0
PID	2112
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #34: jlbxcalqx.exe

ID	34
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 109908, Reason: Child Process
Unmonitor End Time	End Time: 178969, Reason: Terminated
Monitor duration	69.06s
Return Code	0
PID	3240
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #35: jlbxcalqx.exe

ID	35
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 111435, Reason: Child Process
Unmonitor End Time	End Time: 190715, Reason: Terminated
Monitor duration	79.28s
Return Code	0
PID	1484
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	171

Process #36: jlbxcalqx.exe

ID	36
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 111673, Reason: Child Process
Unmonitor End Time	End Time: 176987, Reason: Terminated
Monitor duration	65.31s
Return Code	0
PID	1160
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	67

Process #37: jlbxcalqx.exe

ID	37
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 112767, Reason: Child Process
Unmonitor End Time	End Time: 167304, Reason: Terminated
Monitor duration	54.54s
Return Code	0
PID	384
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #38: jlbxcalqx.exe

ID	38
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 112921, Reason: Child Process
Unmonitor End Time	End Time: 168455, Reason: Terminated
Monitor duration	55.53s
Return Code	0
PID	3248
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #39: jlbxcalqx.exe

ID	39
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 113577, Reason: Child Process
Unmonitor End Time	End Time: 167304, Reason: Terminated
Monitor duration	53.73s
Return Code	0
PID	1916
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #40: jlbxcalqx.exe

ID	40
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 113718, Reason: Child Process
Unmonitor End Time	End Time: 191187, Reason: Terminated
Monitor duration	77.47s
Return Code	0
PID	3376
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	93

Process #41: jlbxcalqx.exe

ID	41
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 114057, Reason: Child Process
Unmonitor End Time	End Time: 203579, Reason: Terminated
Monitor duration	89.52s
Return Code	0
PID	540
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #42: jlbxcalqx.exe

ID	42
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 114144, Reason: Child Process
Unmonitor End Time	End Time: 205006, Reason: Terminated
Monitor duration	90.86s
Return Code	0
PID	2132
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #43: jlbxcalqx.exe

ID	43
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 114323, Reason: Child Process
Unmonitor End Time	End Time: 203462, Reason: Terminated
Monitor duration	89.14s
Return Code	0
PID	2144
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #44: jlbxcalqx.exe

ID	44
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 114401, Reason: Child Process
Unmonitor End Time	End Time: 205006, Reason: Terminated
Monitor duration	90.61s
Return Code	0
PID	2156
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #45: jlbxcalqx.exe

ID	45
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 114550, Reason: Child Process
Unmonitor End Time	End Time: 203885, Reason: Terminated
Monitor duration	89.33s
Return Code	0
PID	2168
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #46: jlbxcalqx.exe

ID	46
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 114602, Reason: Child Process
Unmonitor End Time	End Time: 209863, Reason: Terminated
Monitor duration	95.26s
Return Code	0
PID	2180
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #47: jlbxcalqx.exe

ID	47
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 114734, Reason: Child Process
Unmonitor End Time	End Time: 225239, Reason: Terminated
Monitor duration	110.50s
Return Code	0
PID	2248
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #48: jlbxcalqx.exe

ID	48
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 114977, Reason: Child Process
Unmonitor End Time	End Time: 233965, Reason: Terminated
Monitor duration	118.99s
Return Code	0
PID	2492
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	142

Process #49: jlbxcalqx.exe

ID	49
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 115040, Reason: Child Process
Unmonitor End Time	End Time: 143584, Reason: Terminated
Monitor duration	28.54s
Return Code	0
PID	2504
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	91
Mutex	4

Process #50: jlbxcalqx.exe

ID	50
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 115223, Reason: Child Process
Unmonitor End Time	End Time: 246334, Reason: Terminated
Monitor duration	131.11s
Return Code	0
PID	2532
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #51: jlbxcalqx.exe

ID	51
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 115291, Reason: Child Process
Unmonitor End Time	End Time: 189922, Reason: Terminated
Monitor duration	74.63s
Return Code	0
PID	2544
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	171

Process #52: jlbxcalqx.exe

ID	52
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 115596, Reason: Child Process
Unmonitor End Time	End Time: 168923, Reason: Terminated
Monitor duration	53.33s
Return Code	0
PID	2556
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #53: jlbxcalqx.exe

ID	53
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 115653, Reason: Child Process
Unmonitor End Time	End Time: 168923, Reason: Terminated
Monitor duration	53.27s
Return Code	0
PID	2568
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	135
Mutex	4

Process #54: jlbxcalqx.exe

ID	54
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 115870, Reason: Child Process
Unmonitor End Time	End Time: 255063, Reason: Terminated
Monitor duration	139.19s
Return Code	0
PID	2588
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #55: jlbxcalqx.exe

ID	55
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 115942, Reason: Child Process
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	171.61s
Return Code	Unknown
PID	2608
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	102

Process #56: jlbxcalqx.exe

ID	56
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 116117, Reason: Child Process
Unmonitor End Time	End Time: 233866, Reason: Terminated
Monitor duration	117.75s
Return Code	0
PID	2624
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #57: jlbxcalqx.exe

ID	57
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 116175, Reason: Child Process
Unmonitor End Time	End Time: 224549, Reason: Terminated
Monitor duration	108.37s
Return Code	0
PID	2636
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #58: jlbxcalqx.exe

ID	58
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 116363, Reason: Child Process
Unmonitor End Time	End Time: 248065, Reason: Terminated
Monitor duration	131.70s
Return Code	0
PID	2648
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #59: jlbxcalqx.exe

ID	59
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 116458, Reason: Child Process
Unmonitor End Time	End Time: 207599, Reason: Terminated
Monitor duration	91.14s
Return Code	0
PID	2660
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #60: jlbxcalqx.exe

ID	60
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 116730, Reason: Child Process
Unmonitor End Time	End Time: 217938, Reason: Terminated
Monitor duration	101.21s
Return Code	0
PID	2672
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #61: jlbxcalqx.exe

ID	61
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 116874, Reason: Child Process
Unmonitor End Time	End Time: 223462, Reason: Terminated
Monitor duration	106.59s
Return Code	0
PID	2684
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #62: jlbxcalqx.exe

ID	62
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 117183, Reason: Child Process
Unmonitor End Time	End Time: 212468, Reason: Terminated
Monitor duration	95.28s
Return Code	0
PID	2872
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #63: jlbxcalqx.exe

ID	63
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 117297, Reason: Child Process
Unmonitor End Time	End Time: 220466, Reason: Terminated
Monitor duration	103.17s
Return Code	0
PID	1364
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #64: jlbxcalqx.exe

ID	64
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 117544, Reason: Child Process
Unmonitor End Time	End Time: 248873, Reason: Terminated
Monitor duration	131.33s
Return Code	0
PID	3388
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #65: jlbxcalqx.exe

ID	65
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 117610, Reason: Child Process
Unmonitor End Time	End Time: 207599, Reason: Terminated
Monitor duration	89.99s
Return Code	0
PID	3384
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #66: jlbxcalqx.exe

ID	66
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 117686, Reason: Child Process
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	169.87s
Return Code	Unknown
PID	3340
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #67: jlbxcalqx.exe

ID	67
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 117898, Reason: Child Process
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	169.65s
Return Code	Unknown
PID	3420
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	145

Process #68: jlbxcalqx.exe

ID	68
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 117972, Reason: Child Process
Unmonitor End Time	End Time: 284863, Reason: Terminated
Monitor duration	166.89s
Return Code	0
PID	3408
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #69: jlbxcalqx.exe

ID	69
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 118054, Reason: Child Process
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	169.50s
Return Code	Unknown
PID	3284
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	169

Process #70: jlbxcalqx.exe

ID	70
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 118215, Reason: Child Process
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	169.34s
Return Code	Unknown
PID	3336
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	136

Process #71: jlbxcalqx.exe

ID	71
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 118268, Reason: Child Process
Unmonitor End Time	End Time: 220792, Reason: Terminated
Monitor duration	102.52s
Return Code	0
PID	3580
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #72: jlbxcalqx.exe

ID	72
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 118604, Reason: Child Process
Unmonitor End Time	End Time: 254280, Reason: Terminated
Monitor duration	135.68s
Return Code	0
PID	3608
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #73: jlbxcalqx.exe

ID	73
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 118707, Reason: Child Process
Unmonitor End Time	End Time: 236798, Reason: Terminated
Monitor duration	118.09s
Return Code	0
PID	3588
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #74: jlbxcalqx.exe

ID	74
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 119101, Reason: Child Process
Unmonitor End Time	End Time: 235489, Reason: Terminated
Monitor duration	116.39s
Return Code	0
PID	3540
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #75: jlbxcalqx.exe

ID	75
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 119197, Reason: Child Process
Unmonitor End Time	End Time: 220790, Reason: Terminated
Monitor duration	101.59s
Return Code	0
PID	3644
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #76: jlbxcalqx.exe

ID	76
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 119520, Reason: Child Process
Unmonitor End Time	End Time: 257627, Reason: Terminated
Monitor duration	138.11s
Return Code	0
PID	3544
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	79

Process #77: jlbxcalqx.exe

ID	77
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 119735, Reason: Child Process
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	167.82s
Return Code	Unknown
PID	3516
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #78: jlbxcalqx.exe

ID	78
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 119881, Reason: Child Process
Unmonitor End Time	End Time: 221886, Reason: Terminated
Monitor duration	102.00s
Return Code	0
PID	3680
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #79: jlbxcalqx.exe

ID	79
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 119970, Reason: Child Process
Unmonitor End Time	End Time: 238219, Reason: Terminated
Monitor duration	118.25s
Return Code	0
PID	3692
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	91

Process #80: jlbxcalqx.exe

ID	80
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 120106, Reason: Child Process
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	167.45s
Return Code	Unknown
PID	3724
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	67

Process #81: jlbxcalqx.exe

ID	81
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 120174, Reason: Child Process
Unmonitor End Time	End Time: 235488, Reason: Terminated
Monitor duration	115.31s
Return Code	0
PID	3752
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #82: jlbxcalqx.exe

ID	82
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 120328, Reason: Child Process
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	167.22s
Return Code	Unknown
PID	3268
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #83: jlbxcalqx.exe

ID	83
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 120450, Reason: Child Process
Unmonitor End Time	End Time: 233903, Reason: Terminated
Monitor duration	113.45s
Return Code	0
PID	3260
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #84: jlbxcalqx.exe

ID	84
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 120599, Reason: Child Process
Unmonitor End Time	End Time: 243796, Reason: Terminated
Monitor duration	123.20s
Return Code	0
PID	3788
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	89

Process #85: jlbxcalqx.exe

ID	85
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 120657, Reason: Child Process
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	166.90s
Return Code	Unknown
PID	3256
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #86: jlbxcalqx.exe

ID	86
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 121002, Reason: Child Process
Unmonitor End Time	End Time: 247391, Reason: Terminated
Monitor duration	126.39s
Return Code	0
PID	3672
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #87: jlbxcalqx.exe

ID	87
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 121060, Reason: Child Process
Unmonitor End Time	End Time: 271357, Reason: Terminated
Monitor duration	150.30s
Return Code	0
PID	3668
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	165

Process #88: jlbxcalqx.exe

ID	88
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 121235, Reason: Child Process
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	166.32s
Return Code	Unknown
PID	3840
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #89: jlbxcalqx.exe

ID	89
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 121310, Reason: Child Process
Unmonitor End Time	End Time: 240781, Reason: Terminated
Monitor duration	119.47s
Return Code	0
PID	1028
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #90: jlbxcalqx.exe

ID	90
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 121815, Reason: Child Process
Unmonitor End Time	End Time: 235495, Reason: Terminated
Monitor duration	113.68s
Return Code	0
PID	3636
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	70

Process #91: jlbxcalqx.exe

ID	91
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 121928, Reason: Child Process
Unmonitor End Time	End Time: 236798, Reason: Terminated
Monitor duration	114.87s
Return Code	0
PID	3728
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #92: jlbxcalqx.exe

ID	92
File Name	c:\users\keecfmwgj\desktop\jlbxcalqx.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 122825, Reason: Child Process
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	164.73s
Return Code	Unknown
PID	3740
Parent PID	3684
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #93: hdwwiz.exe

ID	93
File Name	c:\windows\system32\hdwwiz.exe
Command Line	C:\Windows\system32\hdwwiz.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 138707, Reason: Child Process
Unmonitor End Time	End Time: 143237, Reason: Terminated
Monitor duration	4.53s
Return Code	3221226540
PID	3868
Parent PID	1116
Bitness	64 Bit

Process #94: snippingtool.exe

ID	94
File Name	c:\windows\system32\snippingtool.exe
Command Line	C:\Windows\system32\SnippingTool.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 145097, Reason: Child Process
Unmonitor End Time	End Time: 148259, Reason: Terminated
Monitor duration	3.16s
Return Code	0
PID	3792
Parent PID	1116
Bitness	64 Bit

Process #95: iscsicpl.exe

ID	95
File Name	c:\windows\system32\iscsicpl.exe
Command Line	C:\Windows\system32\iscsicpl.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 152517, Reason: Child Process
Unmonitor End Time	End Time: 156568, Reason: Terminated
Monitor duration	4.05s
Return Code	3221226540
PID	3804
Parent PID	1116
Bitness	64 Bit

Process #96: lpksetup.exe

ID	96
File Name	c:\windows\system32\lpksetup.exe
Command Line	C:\Windows\system32\lpksetup.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 157667, Reason: Child Process
Unmonitor End Time	End Time: 161034, Reason: Terminated
Monitor duration	3.37s
Return Code	0
PID	3836
Parent PID	1116
Bitness	64 Bit

Process #97: snippingtool.exe

ID	97
File Name	c:\users\keecfmwgj\appdata\local\j6eppj\snippingtool.exe
Command Line	C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\SnippingTool.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 173208, Reason: Child Process
Unmonitor End Time	End Time: 187783, Reason: Terminated
Monitor duration	14.57s
Return Code	0
PID	3920
Parent PID	1116
Bitness	64 Bit

Host Behavior

Type	Count
File	109
Module	11

Process #98: rstrui.exe

ID	98
File Name	c:\windows\system32\rstrui.exe
Command Line	C:\Windows\system32\rstrui.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189225, Reason: Child Process
Unmonitor End Time	End Time: 193680, Reason: Terminated
Monitor duration	4.46s
Return Code	3221226540
PID	3980
Parent PID	1116
Bitness	64 Bit

Process #99: multidigimon.exe

ID	99
File Name	c:\windows\system32\multidigimon.exe
Command Line	C:\Windows\system32\MultiDigiMon.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189277, Reason: Child Process
Unmonitor End Time	End Time: 193680, Reason: Terminated
Monitor duration	4.40s
Return Code	3221226540
PID	3876
Parent PID	1116
Bitness	64 Bit

Process #100: psr.exe

ID	100
File Name	c:\windows\system32\psr.exe
Command Line	C:\Windows\system32\psr.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 197498, Reason: Child Process
Unmonitor End Time	End Time: 201277, Reason: Terminated
Monitor duration	3.78s
Return Code	0
PID	3888
Parent PID	1116
Bitness	64 Bit

Process #101: newdev.exe

ID	101
File Name	c:\windows\system32\newdev.exe
Command Line	C:\Windows\system32\newdev.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 200288, Reason: Child Process
Unmonitor End Time	End Time: 203758, Reason: Terminated
Monitor duration	3.47s
Return Code	0
PID	4004
Parent PID	1116
Bitness	64 Bit

Process #102: ntprint.exe

ID	102
File Name	c:\windows\system32\ntprint.exe
Command Line	C:\Windows\system32\ntprint.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237456, Reason: Child Process
Unmonitor End Time	End Time: 242758, Reason: Terminated
Monitor duration	5.30s
Return Code	3221226540
PID	3960
Parent PID	1116
Bitness	64 Bit

Process #103: ocsetup.exe

ID	103
File Name	c:\windows\system32\ocsetup.exe
Command Line	C:\Windows\system32\ocsetup.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 243125, Reason: Child Process
Unmonitor End Time	End Time: 246617, Reason: Terminated
Monitor duration	3.49s
Return Code	3221226540
PID	3976
Parent PID	1116
Bitness	64 Bit

Process #104: odbcad32.exe

ID	104
File Name	c:\windows\system32\odbcad32.exe
Command Line	C:\Windows\system32\odbcad32.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 246618, Reason: Child Process
Unmonitor End Time	End Time: 249344, Reason: Terminated
Monitor duration	2.73s
Return Code	3221226540
PID	4076
Parent PID	1116
Bitness	64 Bit

Process #105: recdisc.exe

ID	105
File Name	c:\windows\system32\recdisc.exe
Command Line	C:\Windows\system32\recdisc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 251455, Reason: Child Process
Unmonitor End Time	End Time: 254101, Reason: Terminated
Monitor duration	2.65s
Return Code	3221226540
PID	4080
Parent PID	1116
Bitness	64 Bit

Process #106: psr.exe

ID	106
File Name	c:\users\keecfmwgj\appdata\local\aalri\psr.exe
Command Line	C:\Users\kEecfMwgj\AppData\Local\aAlRi\psr.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 253203, Reason: Child Process
Unmonitor End Time	End Time: 259493, Reason: Terminated
Monitor duration	6.29s
Return Code	0
PID	1392
Parent PID	1116
Bitness	64 Bit

Host Behavior

Type	Count
File	109
Module	14
System	3
Registry	139
-	1
Environment	1

Process #107: recdisc.exe

ID	107
File Name	c:\windows \system32\recdisc.exe
Command Line	"C:\Windows \system32\recdisc.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 254102, Reason: Child Process
Unmonitor End Time	End Time: 255378, Reason: Terminated
Monitor duration	1.28s
Return Code	3221226540
PID	336
Parent PID	1116
Bitness	64 Bit

Process #108: recdisc.exe

ID	108
File Name	c:\windows \system32\recdisc.exe
Command Line	"C:\Windows \system32\recdisc.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 258809, Reason: Child Process
Unmonitor End Time	End Time: 285835, Reason: Terminated
Monitor duration	27.03s
Return Code	258
PID	2044
Parent PID	1116
Bitness	64 Bit

Host Behavior

Type	Count
Process	1

Process #109: netsh.exe

ID	109
File Name	c:\windows\system32\netsh.exe
Command Line	C:\Windows\system32\netsh.exe advfirewall firewall add rule name="Core Networking - Multicast Listener Done (ICMPv4-In)" program="C:\Windows\Explorer.EXE" dir=in action=allow protocol=TCP localport=any
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 261287, Reason: Child Process
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	26.27s
Return Code	Unknown
PID	3232
Parent PID	2044
Bitness	64 Bit

Host Behavior

Type	Count
System	17
Module	36
Registry	18

Process #110: unregmp2.exe

ID	110
File Name	c:\windows\system32\unregmp2.exe
Command Line	C:\Windows\system32\unregmp2.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 263343, Reason: Child Process
Unmonitor End Time	End Time: 265029, Reason: Terminated
Monitor duration	1.69s
Return Code	0
PID	2104
Parent PID	1116
Bitness	64 Bit

Process #111: taskeng.exe

ID	111
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {76156B83-E44C-46B5-B5E8-86A5B965E65D} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 282710, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 287552, Reason: Terminated by Timeout
Monitor duration	4.84s
Return Code	Unknown
PID	3276
Parent PID	868
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862	C:\Users\kEecfMwgj\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll, C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll	Sample File	1208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
8a2cc9a59220bfafa0ab618dc08f3760f516f0697fc24ad4a5d1f00eba4b01f9	C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\OLEACC.dll	Dropped File	1212.00 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	MALICIOUS
f82f912c345800653932585fb15f0991a16b1347daf7cfdf1e36270ca8e6868f	C:\Users\kEecfMwgj\AppData\Local\aAlRi\WTSAPI32.dll, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Office\CuPXu597CI\WTSAPI32.dll	Dropped File	1212.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
b5e85d4434bbdc83c020f4d1bc70908b76643e8b6a9b8b51c3942d8a6db500c1	C:\Users\kEecfMwgj\AppData\Local\kza5B6\slc.dll	Dropped File	1212.00 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	MALICIOUS
890884c7fe7d037e6debd21d1877e9c9c5e7790cdba007ddb219ae6a55667f78	C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\SnippingTool.exe	Dropped File	421.00 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	SUSPICIOUS
68910f8aae867e938b6a3b76cdf176898ba275d9ade85b4ce00b03232de4c495	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Office\CuPXu597CI\psr.exe, C:\Users\kEecfMwgj\AppData\Local\aAlRi\psr.exe	Dropped File	715.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	SUSPICIOUS
dcaeb590394b42d180e23e3cef4dd135513395b026e0ed489aec49848b85b8f0	\\?\C:\Windows \system32\recdisc.exe	Dropped File	232.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	SUSPICIOUS
2d970fea1e7ebc4c9bae287309fa032cb2ac90323c0cdb49ca9593dc7d074c98	c:\users\keecfmwgj\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-4219442223-4223814209-3835049652-1000\4fe4574abf1bcb0f6ed6a78aa750fb2c_b9c8f16e-2e51-4052-9ecb-f86ae5d96ef6	Dropped File	50 bytes	application/octet-stream	-	CLEAN
e2b09cfdead0313843c3dbf5233833c1d9c80a33078bf4739760b64fb1fd524a	\\?\C:\Windows \system32\ReAgent.dll	Dropped File	306.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	CLEAN
7d6be433ba7dd4a2b8f8b79d7b87055da8daafa3e0404432d40469c39c2040e1	C:\Users\kEecfMwgj\AppData\Local\kza5B6\unregmp2.exe	Dropped File	316.00 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	CLEAN
edc6261c01e8e88b2a9b225e36582e88791b1ca755237819b5d143a5e2a11a91	c:\users\keecfmwgj\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-4219442223-4223814209-3835049652-1000\4fe4574abf1bcb0f6ed6a78aa750fb2c_b9c8f16e-2e51-4052-9ecb-f86ae5d96ef6	Dropped File	1.40 KB	application/octet-stream	-	CLEAN
72275404c470b62a5ff49013e3f952d9480afd5c7e45b6c504235823da4894ae	c:\users\keecfmwgj\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-4219442223-4223814209-3835049652-1000\4fe4574abf1bcb0f6ed6a78aa750fb2c_b9c8f16e-2e51-4052-9ecb-f86ae5d96ef6	Dropped File	1.40 KB	application/octet-stream	-	CLEAN
a650f61765d668cb35df7c2a2f08112f67ef6b5011a14290922cbc7eca79bd3c	c:\users\keecfmwgj\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-4219442223-4223814209-3835049652-1000\4fe4574abf1bcb0f6ed6a78aa750fb2c_b9c8f16e-2e51-4052-9ecb-f86ae5d96ef6	Dropped File	1.42 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\tmp67j7r2f9	Accessed File	Access, Read	CLEAN

File Name	Category	Operations	Verdict
C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll	Accessed File	Access, Read	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\Explorer.EXE	Accessed File	Access	CLEAN
C:\Windows\system32\netsh.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\gpresult.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\gpscript.exe	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\Internet Explorer\iexplore.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\gpupdate.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\grpconv.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\hdwwiz.exe	Accessed File	Access, Read	CLEAN
C:\Program Files\Uninstall Information\outlook.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\help.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\HOSTNAME.EXE	Accessed File	Access, Read	CLEAN
C:\Windows\system32\hwrcomp.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\hwrreg.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\icacls.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\icardagt.exe	Accessed File	Access, Read	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Office\CuPXu597CI	Accessed File	Access, Create	CLEAN
C:\Windows\system32\SnippingTool.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\icsunattend.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ie4uinit.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ieUnatt.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\iexpress.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\OLEACC.dll	Accessed File	Access, Read	CLEAN
C:\Windows\system32\InfDefaultInstall.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ipconfig.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\irftp.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\iscsicli.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\iscsicpl.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\isoburn.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\klist.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ksetup.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ktmutil.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\label.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\LocationNotifications.exe	Accessed File	Access, Read	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\Locator.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\lodctr.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\logagent.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\logman.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\logoff.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\LogonUI.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\lpksetup.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\lpremove.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\lsass.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\lsm.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\Magnify.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\makecab.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\manage-bde.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\mblctr.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\mcbuilder.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\mctadmin.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\MdRes.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\MdSched.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\mfpmp.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\MigAutoPlay.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\mmc.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\mobsync.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\mountvol.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\mpnotify.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\MpSigStub.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\MRINFO.EXE	Accessed File	Access, Read	CLEAN
C:\Windows\system32\msdt.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\msdtc.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\msfeedssync.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\msg.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\mshta.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\msiexec.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\msinfo32.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\mspaint.exe	Accessed File	Access, Read	CLEAN
C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\	Accessed File	Access, Delete, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\OLEACC.dll	Dropped File	Access, Write, Delete, Create	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\SnippingTool.exe	Dropped File	Access, Write, Delete, Create	CLEAN
C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesCommonX86\system\msmapi\1033\msmapi32.dll	Accessed File	Access, Read	CLEAN
C:\Windows\system32\mstsc.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\convert.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\diskraid.exe	Accessed File	Access	CLEAN
C:\Windows\system32\verifier.exe	Accessed File	Access	CLEAN
C:\Windows\system32\rstrui.exe	Accessed File	Access	CLEAN
C:\Windows\system32\mtstocom.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\MuiUnattend.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\MultiDigiMon.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\fc.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\NAPSTAT.EXE	Accessed File	Access, Read	CLEAN
C:\Windows\system32\qprocess.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\Narrator.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\cmdl32.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\DeviceEject.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\nbtstat.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ndadmin.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\wiawow64.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\wininit.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\typeperf.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\unlodctr.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\net.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\net1.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\control.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\RpcPing.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\netbtugc.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\credwiz.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\psr.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\netcfg.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WTSAPI32.dll	Accessed File	Access, Read	CLEAN
C:\Windows\system32\netiougc.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\Netplwiz.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\NetProj.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\NETSTAT.EXE	Accessed File	Access, Read	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\newdev.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\nltest.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\notepad.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\nslookup.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ntoskrnl.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ntprint.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ocsetup.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\odbcad32.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\odbcconf.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\openfiles.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\OptionalFeatures.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\osk.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\p2phost.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PATHPING.EXE	Accessed File	Access, Read	CLEAN
C:\Windows\system32\pcalua.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\pcaui.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\pcawrk.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\pcwrun.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PING.EXE	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PkgMgr.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\plasrv.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PnPUnattend.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PnPutil.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\poqexec.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\powercfg.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PresentationHost.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PresentationSettings.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\prevhost.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\print.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PrintBrmUi.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\printfilterpipelinesvc.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PrintIsolationHost.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\printui.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\proquota.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PushPrinterConnections.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\qappsrv.exe	Accessed File	Access, Read	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\query.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\quser.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\qwinsta.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\rasautou.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\rasdial.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\raserver.exe	Accessed File	Access, Read	CLEAN

Reduced dataset

IP

IP Address	Domains	Country	Protocols	Verdict
127.0.0.1	-	-	-	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{bbfa96fb-03e2-244a-e13e-86541d1b182b}	access	jlbxcalqx.exe	CLEAN
{ba62725d-6184-50d2-b706-2d7b865dd82b}	access	jlbxcalqx.exe	CLEAN
{33ff21cb-ff8c-80f2-435a-9f14e40fde6b}	access	explorer.exe	CLEAN
{ad66cb9e-7ae1-701b-6069-4a7b793507ac}	access	explorer.exe	CLEAN
{6ae03f50-7a2d-c6e9-ca75-492d6e54c058}	access	explorer.exe	CLEAN
{13e06e4b-2481-b368-8f42-2212f1d59822}	access	explorer.exe	CLEAN
{65c8ac9c-25ba-82f3-37f2-3fe3857eeb82}	access	explorer.exe	CLEAN
{78fd2f71-b653-7ea3-c562-0b3dc695dbfd}	access	explorer.exe	CLEAN
{ef30bf64-6e77-af44-2844-a272c4a251e4}	access	explorer.exe	CLEAN
{d0c8c370-4e74-9e4a-c235-fabccc75324d}	access	explorer.exe	CLEAN
{93f0b9bd-750b-91aa-43ce-42ee557a016a}	access	explorer.exe	CLEAN
{0a229cb1-bb57-9bd8-01b2-31e4b7cbf515}	access	explorer.exe	CLEAN
{4126ed8b-1649-b296-c1a8-6a31b31e936e}	access	explorer.exe	CLEAN
{50a49a66-4b11-240c-8816-398b6bd70ed6}	access	explorer.exe	CLEAN
{2d7bccd8-c070-8723-c092-31c38068d849}	access	explorer.exe	CLEAN
{aa8eec2a-1624-d913-f987-9558cbeacce1}	access	explorer.exe	CLEAN
{9124fc0f-aad1-69ca-f087-b6f4b4618452}	access	explorer.exe	CLEAN
{3424d05e-75d9-fa9d-601e-13c62053c3c5}	access	explorer.exe	CLEAN
{91af0379-7553-2b9a-1768-bb6f0281e3e9}	access	explorer.exe	CLEAN
{821b3d72-6d45-a55c-2ff2-657dbbeba155}	access	explorer.exe	CLEAN
{87870dec-87d4-3464-8983-690c1429eba9}	access	explorer.exe	CLEAN
{9a382e7d-fa1b-dd43-a0dd-294ace4cebfc}	access	explorer.exe	CLEAN
{8da6b341-b6ae-4ed6-a4db-b8d7a21d3ce2}	access	explorer.exe	CLEAN
{9da07381-49bd-fcd5-49f0-db565310a644}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{d3b3213a-9735-bc53-9894-9fb345059836}	access	explorer.exe	CLEAN
{65b97bfc-3a12-e27a-fd30-cf51840b6a30}	access	explorer.exe	CLEAN
{6b15b196-f9d7-4a9c-57e8-3bbe0bf6efc5}	access	explorer.exe	CLEAN
{46ea2d8a-13ee-8aca-c95c-2826291ff9b1}	access	explorer.exe	CLEAN
{01717a9f-bea9-34be-904d-4afb909970c3}	access	explorer.exe	CLEAN
{d2e7374a-940d-481d-c27a-a6169257d900}	access	explorer.exe	CLEAN
{8dcd38ec-186f-5df8-2880-e7d897695e42}	access	explorer.exe	CLEAN
{dbf760ba-fee3-a258-2c95-0bf2ae6f687c}	access	explorer.exe	CLEAN
{d8e8ed8e-ed18-d8b2-20c5-9722faa1d0a2}	access	explorer.exe	CLEAN
{80201a2a-288f-e732-af04-107e1e1a69c7}	access	explorer.exe	CLEAN
{a3d4095e-f27a-67d6-2464-abda051cfafa}	access	explorer.exe	CLEAN
{154d0f50-802b-6f8c-d8b4-bd483b0ff833}	access	explorer.exe	CLEAN
{caa06b3e-973d-438d-79d0-3e6c5db86ec5}	access	explorer.exe	CLEAN
{5e89745e-2bbf-60af-a0ef-083127d838a9}	access	explorer.exe	CLEAN
{17d4920a-9b19-143e-d3b3-d14bd4004ac0}	access	explorer.exe	CLEAN
{651f06bf-b213-5b95-d5dc-02674261bea0}	access	explorer.exe	CLEAN
{4ca8eece-035e-8a0d-7a2e-528308213fe7}	access	explorer.exe	CLEAN
{cd567760-31c3-d001-1dc5-e0d85270a1af}	access	explorer.exe	CLEAN
{846c0c41-20da-8dfa-40fb-821268816aa6}	access	explorer.exe	CLEAN
{4fcb2055-abca-fec3-d74a-bfb7cf6a8643}	access	explorer.exe	CLEAN
{d189e67d-849b-b3dd-09ea-c7315e6b8c88}	access	explorer.exe	CLEAN
{ecb21098-bef5-28a8-b53b-d0a835b3ed90}	access	explorer.exe	CLEAN
{3b0383b1-04ff-7268-3a25-0c45514d5b49}	access	explorer.exe	CLEAN
{5db73888-05c6-bb30-d3f1-3f30da04606d}	access	explorer.exe	CLEAN
{ceae25b2-bfbf-6042-9ff7-234e83e9ca86}	access	explorer.exe	CLEAN
{4f5b125e-5cc2-9060-9381-4a1c6dbb9577}	access	explorer.exe	CLEAN
{40c757e9-1678-8610-9f1a-c69050d037d1}	access	explorer.exe	CLEAN
{7d2fd42a-e6aa-fd2c-38ad-084cd9d2c907}	access	explorer.exe	CLEAN
{9fbb67e6-7dfb-7615-898e-882c739fd135}	access	explorer.exe	CLEAN
{b598475b-5134-5e51-728b-296b574f100b}	access	explorer.exe	CLEAN
{03ebac9a-7cb3-376a-2aba-295e5c829591}	access	explorer.exe	CLEAN
{77c31159-d018-e6c8-e14a-220fb7ff5df3}	access	explorer.exe	CLEAN
{831cdbe1-2408-1e5a-7415-c4e69eafebc3}	access	explorer.exe	CLEAN
{58686fd1-c00c-aac7-11ae-1d948bcfdeef}	access	explorer.exe	CLEAN
{226e5239-0a41-4cee-fd93-21c269356f14}	access	explorer.exe	CLEAN
{84879af4-fe09-7803-56b4-622c9ca2bc5f}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{14a53b80-b6de-81e7-ed6c-2690e7bf017c}	access	explorer.exe	CLEAN
{123791ad-06f4-9671-c776-3422a38fcfb4}	access	explorer.exe	CLEAN
{981764c6-b91b-534f-d7e6-2632ffbe9834}	access	explorer.exe	CLEAN
{78330561-2f5a-7da1-d365-5dcc0a0c3083}	access	explorer.exe	CLEAN
{4e9eeb26-8717-b563-b21c-f084b6749315}	access	explorer.exe	CLEAN
{b5f3e81b-49f1-e546-9c39-ce8355b85841}	access	explorer.exe	CLEAN
{c5b5a595-0c7a-8aaf-62db-24bc5e1a0d45}	access	explorer.exe	CLEAN
{da9d0ee5-41cc-043e-1ed9-a55c3425df10}	access	explorer.exe	CLEAN
{e491d418-bd3e-f65e-2664-43d1dc901091}	access	explorer.exe	CLEAN
{c0bd6d0a-0f6f-2806-7d4b-5d43dbd575de}	access	explorer.exe	CLEAN
{12920e4a-f87d-9a09-47aa-5d12e08784a1}	access	explorer.exe	CLEAN
{a92f3a1d-574f-d091-59cd-283d029f66ff}	access	explorer.exe	CLEAN
{6023568b-098e-f9d4-0ef2-2d1f0cd7b83d}	access	explorer.exe	CLEAN
{1aae18c5-16a2-98f2-2e4c-4810e654cc18}	access	explorer.exe	CLEAN
{8abda610-788f-33bc-6353-86519e84f6f2}	access	explorer.exe	CLEAN
{af7e12dd-2381-2cf8-9224-3dcb8026908e}	access	explorer.exe	CLEAN
{88ce680e-ad15-3b82-1bdb-11ca2b349e17}	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
-	access, create	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE	access	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE	access	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft	access	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT	access	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate	access, read	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows	access	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version	access	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Policies	access	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Policies\System	access	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Policies\System\EnableLUA	access, read	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Policies\System\ConsentPromptBehaviorAdmin	access, read	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Policies\System\PromptOnSecureDesktop	access, read	jlbxcalqx.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer	access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{79665E8E-4365-6B8F-DA00-D0B828D4FEEC}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{71BC1377-8B48-A04B-D279-F048DCF94E7E}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{40B0E89D-864F-7B36-E7BA-299B4295A387}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{658B8EB4-E886-BA66-3237-86E65BEB1E60}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5F4CA0A3-A910-CB32-91E3-65C4C90E354E}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{DDF3826C-BF0E-D11A-3ABF-ED0CA6E11CF7}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{30E6C3C1-A382-20F0-0569-B60929C9A348}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{A6D924EE-443F-B6B2-7A21-B2F64E00F2EC}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{961EFF9D-BB8C-3A05-CE8E-AB9FF0211A1C}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F7EBB03F-F792-B7CA-EA56-C982AFE2C903}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{09EBA979-3626-0867-E995-47290ADFECDE}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{FFF9BCDE-8935-C1CF-14B1-3FE011D23CE0}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BD5CE409-7117-60F0-7C10-5E495810A4FD}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E8C1261E-A3EA-CD08-28CD-4DBC093C573E}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{09EBA979-3626-0867-E995-47290ADFECDE}\ShellFolder\{83D44767-2972-B125-AF79-72675FB905C0}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{961EFF9D-BB8C-3A05-CE8E-AB9FF0211A1C}\ShellFolder\{56DE12AA-FD0E-1391-9876-67C61E36562C}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9A97E6A9-29FC-3B68-4B33-94C2960CC881}\ShellFolder	access, create	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4663F19F-2DFA-ECF3-DDFB-370E2E26C4FA}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{49E122CC-49ED-565C-A828-344EDBE840A6}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BBF565DE-9A24-D768-2CD0-543EF86AD28F}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InstallDate	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{16735AF7-1D8D-3681-94A5-C578A61EC832}	access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{16735AF7-1D8D-3681-94A5-C578A61EC832}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{16735AF7-1D8D-3681-94A5-C578A61EC832}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{71BC1377-8B48-A04B-D279-F048DCF94E7E}\ShellFolder\{A9577F80-3C4C-8D64-356D-A45BDAD3C842}	access, write	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\InstallDate	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\InstallDate	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetSh	access	netsh.exe	CLEAN

Process

Process Name	Commandline	Verdict
snippingtool.exe	C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\SnippingTool.exe	MALICIOUS
psr.exe	C:\Users\kEecfMwgj\AppData\Local\aAlRi\psr.exe	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmp67j7r2f9" /s	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW	CLEAN

Process Name	Commandline	Verdict
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="0"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="0"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="0"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="0"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="0"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="0"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="0"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="0"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="0"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="0"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="1"	CLEAN

Process Name	Commandline	Verdict
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="Install"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="Install"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="Install"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="Install"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="Install"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="Install"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="Install"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="Install"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="Install"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="Install"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="DefaultInstall"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="DefaultInstall"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="DefaultInstall"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="DefaultInstall"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="DefaultInstall"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="DefaultInstall"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="DefaultInstall"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="DefaultInstall"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="DefaultInstall"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="DefaultInstall"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="127.0.0.1"	CLEAN

Process Name	Commandline	Verdict
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="127.0.0.1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="127.0.0.1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="127.0.0.1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="127.0.0.1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="127.0.0.1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="127.0.0.1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="127.0.0.1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="127.0.0.1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="127.0.0.1"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="explorer.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="explorer.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="explorer.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="explorer.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="explorer.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="explorer.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="explorer.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="explorer.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="explorer.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="explorer.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="iexplore.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="iexplore.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="iexplore.exe"	CLEAN

Process Name	Commandline	Verdict
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="iexplore.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="iexplore.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="iexplore.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="iexplore.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="iexplore.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="iexplore.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="iexplore.exe"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=DisplaySYSDMCPL /fn_args="%Temp%\IXP000.TMP\"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditEnvironmentVariables /fn_args="%Temp%\IXP000.TMP\"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EditUserProfiles /fn_args="%Temp%\IXP000.TMP\"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=EnableExecuteProtectionSupportW /fn_args="%Temp%\IXP000.TMP\"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=ModifyExecuteProtectionSupportW /fn_args="%Temp%\IXP000.TMP\"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutList /fn_args="%Temp%\IXP000.TMP\"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteAddFileOptOutListW /fn_args="%Temp%\IXP000.TMP\"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteProcessExceptionW /fn_args="%Temp%\IXP000.TMP\"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutList /fn_args="%Temp%\IXP000.TMP\"	CLEAN
jlbxcalqx.exe	"C:\Users\kEecfMwgj\Desktop\JLBxcALqX.exe" /dll="C:\Users\KEECFM~1\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll" /fn_id=NoExecuteRemoveFileOptOutListW /fn_args="%Temp%\IXP000.TMP\"	CLEAN
hdwwiz.exe	C:\Windows\system32\hdwwiz.exe	CLEAN
snippingtool.exe	C:\Windows\system32\SnippingTool.exe	CLEAN
iscsicpl.exe	C:\Windows\system32\iscsicpl.exe	CLEAN
lpksetup.exe	C:\Windows\system32\lpksetup.exe	CLEAN
rstrui.exe	C:\Windows\system32\rstrui.exe	CLEAN
multidigimon.exe	C:\Windows\system32\MultiDigiMon.exe	CLEAN
psr.exe	C:\Windows\system32\psr.exe	CLEAN
newdev.exe	C:\Windows\system32\newdev.exe	CLEAN

Process Name	Commandline	Verdict
ntprint.exe	C:\Windows\system32\ntprint.exe	CLEAN
ocsetup.exe	C:\Windows\system32\ocsetup.exe	CLEAN
odbcad32.exe	C:\Windows\system32\odbcad32.exe	CLEAN
recdisc.exe	C:\Windows\system32\recdisc.exe	CLEAN
recdisc.exe	"C:\Windows \system32\recdisc.exe"	CLEAN
netsh.exe	C:\Windows\system32\netsh.exe advfirewall firewall add rule name="Core Networking - Multicast Listener Done (ICMPv4-In)" program="C:\Windows\Explorer.EXE" dir=in action=allow protocol=TCP localport=any	CLEAN
unregmp2.exe	C:\Windows\system32\unregmp2.exe	CLEAN
taskeng.exe	taskeng.exe {76156B83-E44C-46B5-B5E8-86A5B965E65D} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]	CLEAN

YARA / AV

Antivirus (11)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\kEecfMwgj\Desktop\2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862.exe.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.76753	C:\Users\kEecfMwgj\AppData\Local\j6EpPJ\OLEACC.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.76753	C:\Users\kEecfMwgj\AppData\Local\aAlRi\WTSAPI32.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.76753	C:\Users\kEecfMwgj\AppData\Local\kza5B6\slc.dll	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

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

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH

User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp
System Root	C:\Windows