MALICIOUS

Classifications: Spyware

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

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll**
ID	#2782665
MD5	2cd9944b4c51630053a486adf9ba7928
SHA1	fbbe87d4587c694c6b44870bb99e30e1d48d1c06
SHA256	a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca
File Size	2276.00 KB
Report Created	2021-09-28 12:49 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (8 rules, 195 matches)

Score	Category	Operation	Count	Classification
4/5	Antivirus	Malicious content was detected by heuristic scan	4	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #7) vfuusnkaf.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #192) explorer.exe as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #134) vfuusnkaf.exe as "Trojan.GenericKDZ.76753".			
4/5	Injection	Modifies control flow of another process	4	-
	• (Process #4) vfuusnkaf.exe alters context of (process #20) explorer.exe. • (Process #12) vfuusnkaf.exe alters context of (process #20) explorer.exe. • (Process #14) vfuusnkaf.exe alters context of (process #20) explorer.exe. • (Process #24) vfuusnkaf.exe alters context of (process #192) explorer.exe.			
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
1/5	Discovery	Reads system data	79	-

• (Process #7) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #4) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #3) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #2) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #5) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #11) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #6) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #8) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #9) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #10) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #12) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #13) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #14) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #16) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #18) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #15) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #17) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #19) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #23) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #24) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #28) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #32) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #21) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #31) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #30) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #25) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #41) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #45) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #51) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #58) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #33) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #35) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #38) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #63) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #43) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #37) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #39) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #36) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #60) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #49) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #57) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #53) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #22) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #77) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #97) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #56) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #128) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #48) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #133) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #67) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #155) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #80) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #142) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #134) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #132) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #40) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #94) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #109) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #121) vfuusnkaf.exe reads the Windows installation date from registry.
• (Process #52) vfuusnkaf.exe reads the Windows installation date from registry.

Score	Category	Operation	Count	Classification
1/5	Mutex	Creates mutex	100	-

- (Process #7) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #4) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #3) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #2) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #5) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #4) vfuusnkaf.exe creates mutex with name "{ba62725d-6184-50d2-b706-2d7b865dd82b}".
- (Process #11) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #6) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #8) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #9) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #10) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #12) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #13) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #14) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #16) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #18) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #15) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #17) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #19) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #12) vfuusnkaf.exe creates mutex with name "{ba62725d-6184-50d2-b706-2d7b865dd82b}".
- (Process #23) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #24) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #28) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #32) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #21) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #31) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #30) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #25) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #41) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #45) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #51) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #14) vfuusnkaf.exe creates mutex with name "{ba62725d-6184-50d2-b706-2d7b865dd82b}".
- (Process #58) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #33) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #35) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #38) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #16) vfuusnkaf.exe creates mutex with name "{ba62725d-6184-50d2-b706-2d7b865dd82b}".
- (Process #63) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #43) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #21) vfuusnkaf.exe creates mutex with name "{ba62725d-6184-50d2-b706-2d7b865dd82b}".
- (Process #37) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #39) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #36) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #24) vfuusnkaf.exe creates mutex with name "{712d24f9-647f-9b8f-21cf-5266fada45a5}".
- (Process #60) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #53) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #49) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #57) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #22) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #77) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #97) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #56) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #128) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #48) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #133) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #67) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #155) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #80) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #142) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #134) vfuusnkaf.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	5	-
	• (Process #4) vfuusnkaf.exe reads from (process #20) explorer.exe. • (Process #12) vfuusnkaf.exe reads from (process #20) explorer.exe. • (Process #14) vfuusnkaf.exe reads from (process #20) explorer.exe. • (Process #16) vfuusnkaf.exe reads from (process #20) explorer.exe. • (Process #24) vfuusnkaf.exe reads from (process #192) explorer.exe.			
1/5	Crash	A monitored process crashed	1	-
	• (Process #20) explorer.exe crashed.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #192) explorer.exe resolves 26 API functions by name.			
-	Trusted	Known clean file	1	-
	• 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

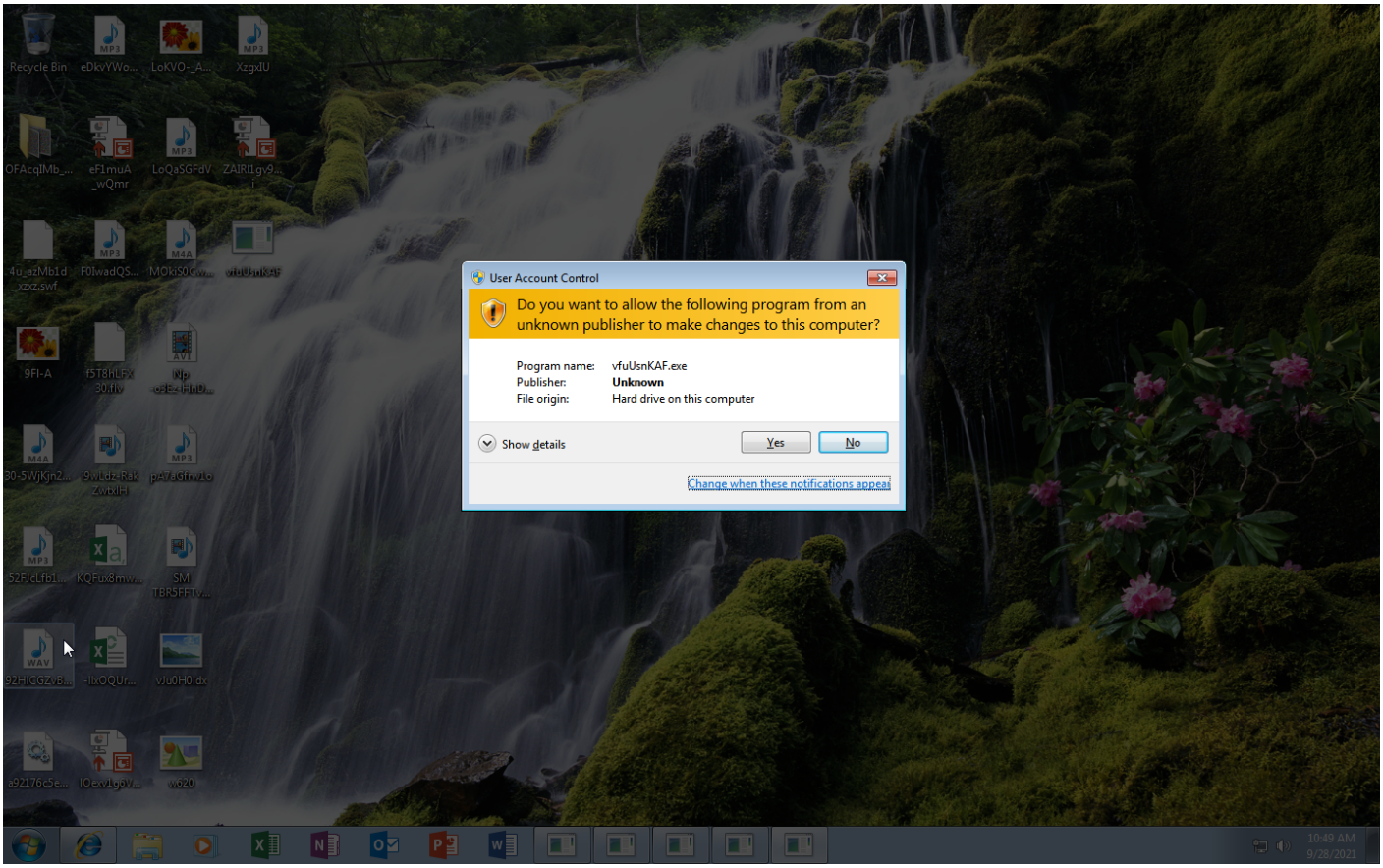
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1045 Software Packing		#T1082 System Information Discovery					
						#T1012 Query Registry					

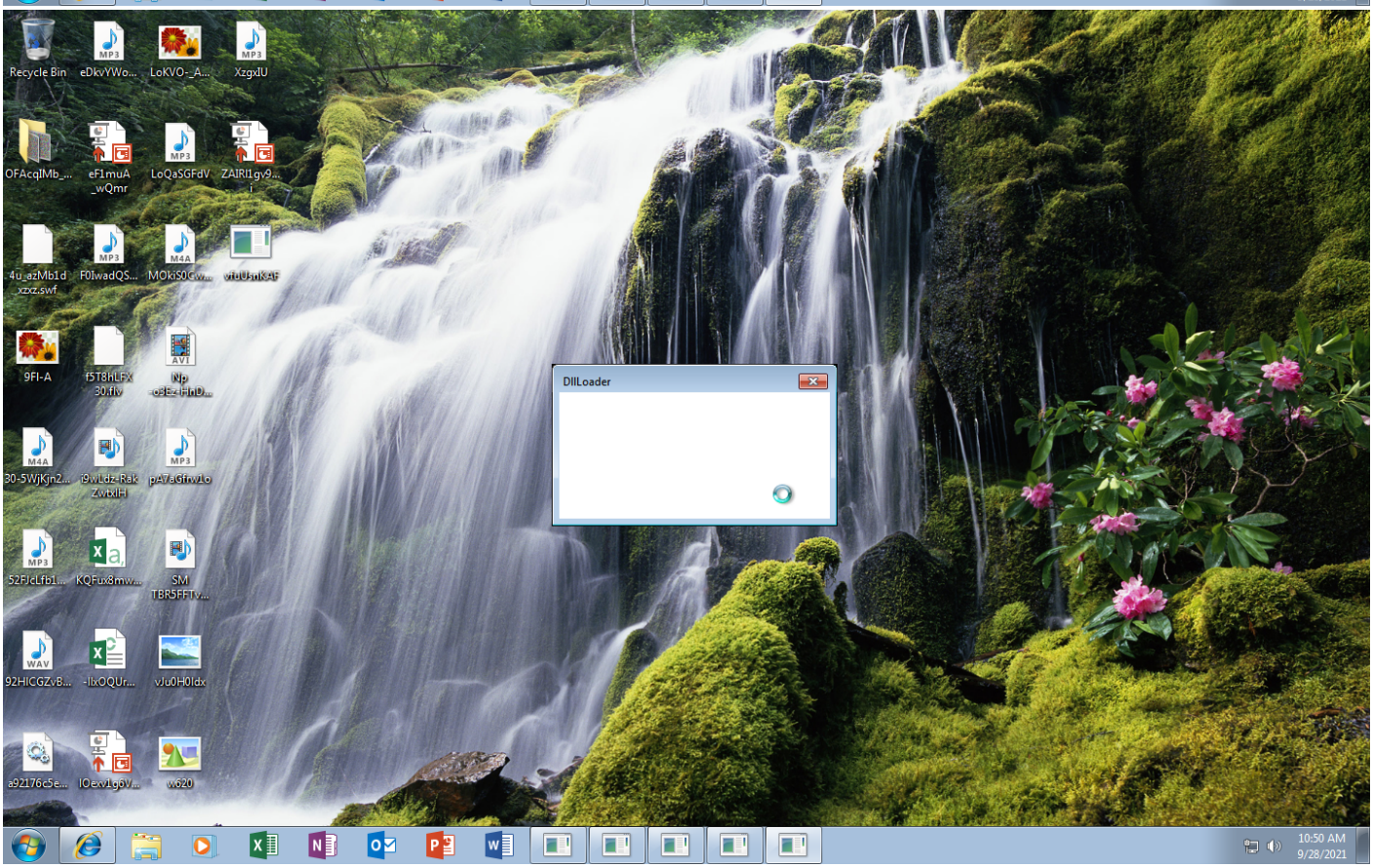
Sample Information

ID	#2782665
MD5	2cd9944b4c51630053a486adf9ba7928
SHA1	fbbe87d4587c694c6b44870bb99e30e1d48d1c06
SHA256	a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca
SSDeep	12288:i5VI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1MVedA:i4fP7fWsK5z9A+WGAW+V5SB6Ct4bnbg
ImpHash	6668be91e2c948b183827f040944057f
File Name	a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll
File Size	2276.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 12:49 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	273
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	4
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: vfuUsnKAF.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

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

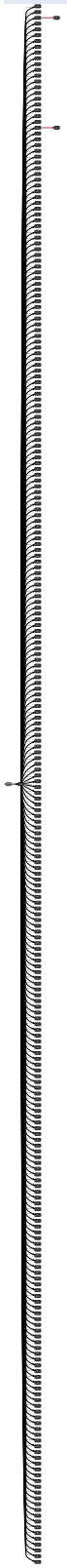
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: vfuusnkaf.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmp2h7i6jr7" /s
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 52439, Reason: Analysis Target
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	242.32s
Return Code	Unknown
PID	3844
Parent PID	1116
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	16
File	11
Environment	1
Process	271

Process #2: vfuusnkaf.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 70709, Reason: Child Process
Unmonitor End Time	End Time: 90780, Reason: Terminated
Monitor duration	20.07s
Return Code	0
PID	3872
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #3: vfuusnkaf.exe

ID	3
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 71004, Reason: Child Process
Unmonitor End Time	End Time: 92019, Reason: Terminated
Monitor duration	21.02s
Return Code	0
PID	3884
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #4: vfuusnkaf.exe

ID	4
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 71186, Reason: Child Process
Unmonitor End Time	End Time: 113102, Reason: Terminated
Monitor duration	41.92s
Return Code	998
PID	3900
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	40
Module	44
File	118
Environment	2
Registry	589
Mutex	6
Process	2
-	2
-	36
-	63
Window	1

Process #5: vfuusnkaf.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $PatternProvider@VInvokeProvider@DirectUI@@UIInvokeProvider@@$0A@@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 71564, Reason: Child Process
Unmonitor End Time	End Time: 96069, Reason: Terminated
Monitor duration	24.50s
Return Code	0
PID	3912
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #6: vfuusnkaf.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $PatternProvider@VRangeValueProvider@DirectUI@@UIRangeValueProvider@@$03@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 71776, Reason: Child Process
Unmonitor End Time	End Time: 96630, Reason: Terminated
Monitor duration	24.85s
Return Code	0
PID	3924
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #7: vfuusnkaf.exe

ID	7
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $PatternProvider@VScrollItemProvider@DirectUI@@UIScrollItemProvider@@$05@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 72724, Reason: Child Process
Unmonitor End Time	End Time: 87596, Reason: Terminated
Monitor duration	14.87s
Return Code	0
PID	3940
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #8: vfuusnkaf.exe

ID	8
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $PatternProvider@VScrollProvider@DirectUI@@UIScrollProvider@@$04@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 74385, Reason: Child Process
Unmonitor End Time	End Time: 98337, Reason: Terminated
Monitor duration	23.95s
Return Code	0
PID	3952
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #9: vfuusnkaf.exe

ID	9
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $PatternProvider@VSelectionItemProvider@DirectUI@@UISelectionItemProvider@@$06@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 74755, Reason: Child Process
Unmonitor End Time	End Time: 100427, Reason: Terminated
Monitor duration	25.67s
Return Code	0
PID	3964
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #10: vfuusnkaf.exe

ID	10
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $PatternProvider@VSelectionProvider@DirectUI@@UISelectionProvider@@$07@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77241, Reason: Child Process
Unmonitor End Time	End Time: 101027, Reason: Terminated
Monitor duration	23.79s
Return Code	0
PID	3980
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #11: vfuusnkaf.exe

ID	11
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $PatternProvider@VTableItemProvider@DirectUI@@UITableItemProvider@@$09@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77699, Reason: Child Process
Unmonitor End Time	End Time: 98961, Reason: Terminated
Monitor duration	21.26s
Return Code	0
PID	3992
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #12: vfuusnkaf.exe

ID	12
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $PatternProvider@VTableProvider@DirectUI@@UITableProvider@@$08@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81081, Reason: Child Process
Unmonitor End Time	End Time: 137475, Reason: Terminated
Monitor duration	56.39s
Return Code	998
PID	4024
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	17
Module	44
File	118
Environment	2
Registry	589
Mutex	6
Process	2
-	68
-	7
-	106
Window	1

Process #13: vfuusnkaf.exe

ID	13
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $PatternProvider@VToggleProvider@DirectUI@@UIToggleProvider@@$0L@@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82830, Reason: Child Process
Unmonitor End Time	End Time: 153615, Reason: Terminated
Monitor duration	70.78s
Return Code	0
PID	4036
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #14: vfuusnkaf.exe

ID	14
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $PatternProvider@VValueProvider@DirectUI@@UIValueProvider@@$0M@@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 84716, Reason: Child Process
Unmonitor End Time	End Time: 147726, Reason: Terminated
Monitor duration	63.01s
Return Code	998
PID	4052
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	10
Module	44
File	118
Environment	2
Registry	589
Mutex	6
Process	2
-	35
-	1
-	66
Window	1

Process #15: vfuusnkaf.exe

ID	15
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0? $SafeArrayAccessor@H@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85797, Reason: Child Process
Unmonitor End Time	End Time: 203384, Reason: Terminated
Monitor duration	117.59s
Return Code	0
PID	4064
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #16: vfuusnkaf.exe

ID	16
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0AccessibleButton@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87187, Reason: Child Process
Unmonitor End Time	End Time: 168416, Reason: Terminated
Monitor duration	81.23s
Return Code	998
PID	4084
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	9
Module	44
File	118
Environment	2
Registry	589
Mutex	6
Process	2
-	3
-	1
-	12
Window	1

Process #17: vfuusnkaf.exe

ID	17
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0AccessibleButton@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87652, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	207.11s
Return Code	Unknown
PID	2764
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	117
Environment	2
Registry	171
Mutex	3

Process #18: vfuusnkaf.exe

ID	18
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0AccessibleButton@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89054, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	205.71s
Return Code	Unknown
PID	2812
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	114
Environment	2
Registry	171
Mutex	3

Process #19: vfuusnkaf.exe

ID	19
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0AnimationStrip@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89902, Reason: Child Process
Unmonitor End Time	End Time: 259540, Reason: Terminated
Monitor duration	169.64s
Return Code	0
PID	2768
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #20: explorer.exe

ID	20
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 89908, Reason: Injection
Unmonitor End Time	End Time: 164884, Reason: Crashed
Monitor duration	74.98s
Return Code	3221225477
PID	1116
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (137)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77732ed0(2004037328)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xf40 / 0x474	0x77526a60(2001889888)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x460	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x474	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x4b8	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x4bc	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x4cc	0x777313f0(2004030448)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x4d4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x50c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x52c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x534	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x540	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x5d8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x478	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x510	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x514	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x51c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x53c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x350	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x354	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x5a4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x36c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x310	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x338	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x12c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x698	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x240	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x880	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x884	0x777313f0(2004030448)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x8a8	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0xd5c	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0xd64	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0xd68	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0xdcc	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0xd48	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x474	0x77732ed0(2004037328)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x460	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x4b8	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x4bc	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x4cc	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x4d4	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x50c	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x52c	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x534	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x540	0x777313f0(2004030448)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x5d8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x478	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x510	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x514	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x51c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x53c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x350	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x354	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x5a4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x36c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x310	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x338	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x12c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x698	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x240	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x880	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x884	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x8a8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0xd5c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0xd64	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0xd68	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0xdcc	0x777313f0(2004030448)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0xd48	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#12: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfbc / 0x474	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x460	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x474	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x4b8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x4bc	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x4cc	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x4d4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x50c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x52c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x534	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x540	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x5d8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x478	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x510	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x514	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x51c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x53c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x350	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x354	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x5a4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x36c	0x777313f0(2004030448)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x310	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x338	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x12c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x698	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x240	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x880	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x884	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0x8a8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0xd5c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0xd64	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0xd68	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0xdcc	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#14: c:\users\keecfmwgj\desktop\vfuusnkaf.exe	0xfd8 / 0xd48	0x777313f0(2004030448)	-	✓	1

Host Behavior

Type	Count
Module	1

Process #21: vfuusnkaf.exe

ID	21
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0AnimationStrip@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89996, Reason: Child Process
Unmonitor End Time	End Time: 167571, Reason: Terminated
Monitor duration	77.58s
Return Code	998
PID	2792
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	34
File	117
Environment	2
Registry	589
Mutex	6
Process	1
Window	1

Process #22: vfuusnkaf.exe

ID	22
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@$ $QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 91223, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	203.54s
Return Code	Unknown
PID	2780
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #23: vfuusnkaf.exe

ID	23
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0AutoButton@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 91333, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	203.43s
Return Code	Unknown
PID	3016
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	117
Environment	2
Registry	171
Mutex	3

Process #24: vfuusnkaf.exe

ID	24
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0AutoButton@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 91768, Reason: Child Process
Unmonitor End Time	End Time: 284936, Reason: Terminated
Monitor duration	193.17s
Return Code	0
PID	3000
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	98
Module	41
File	118
Environment	2
Registry	589
Mutex	6
Process	2
-	116
-	91
-	224

Process #25: vfuusnkaf.exe

ID	25
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0AutoLock@DirectUI@@QEAA@PEAU_RTL_CRITICAL_SECTION@@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 91879, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	202.88s
Return Code	Unknown
PID	2960
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #26: vfuusnkaf.exe

ID	26
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0AutoThread@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 92392, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	202.37s
Return Code	Unknown
PID	2948
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #27: vfuusnkaf.exe

ID	27
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0AutoVariant@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 92504, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	202.26s
Return Code	Unknown
PID	2344
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #28: vfuusnkaf.exe

ID	28
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0BaseScrollBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 92736, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	202.03s
Return Code	Unknown
PID	2352
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #29: vfuusnkaf.exe

ID	29
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0BaseScrollBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 92845, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	201.92s
Return Code	Unknown
PID	2348
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #30: vfuusnkaf.exe

ID	30
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0BaseScrollBar@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 93234, Reason: Child Process
Unmonitor End Time	End Time: 246812, Reason: Terminated
Monitor duration	153.58s
Return Code	0
PID	2000
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #31: vfuusnkaf.exe

ID	31
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0BaseScrollViewer@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 93297, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	201.47s
Return Code	Unknown
PID	1916
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #32: vfuusnkaf.exe

ID	32
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0BaseScrollViewer@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 93475, Reason: Child Process
Unmonitor End Time	End Time: 274642, Reason: Terminated
Monitor duration	181.17s
Return Code	0
PID	3232
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #33: vfuusnkaf.exe

ID	33
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@$ $QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 93597, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	201.17s
Return Code	Unknown
PID	3312
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	117
Environment	2
Registry	171
Mutex	3

Process #34: vfuusnkaf.exe

ID	34
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0Bind@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 93790, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	200.97s
Return Code	Unknown
PID	2196
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #35: vfuusnkaf.exe

ID	35
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 93878, Reason: Child Process
Unmonitor End Time	End Time: 246499, Reason: Terminated
Monitor duration	152.62s
Return Code	0
PID	2184
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #36: vfuusnkaf.exe

ID	36
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0BorderLayout@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 93974, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	200.79s
Return Code	Unknown
PID	3320
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	114
Environment	2
Registry	171
Mutex	3

Process #37: vfuusnkaf.exe

ID	37
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0BorderLayout@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 94548, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	200.22s
Return Code	Unknown
PID	2132
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	114
Environment	2
Registry	171
Mutex	3

Process #38: vfuusnkaf.exe

ID	38
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@$ $QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 94657, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	200.11s
Return Code	Unknown
PID	2148
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #39: vfuusnkaf.exe

ID	39
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0Browser@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 94939, Reason: Child Process
Unmonitor End Time	End Time: 261950, Reason: Terminated
Monitor duration	167.01s
Return Code	0
PID	3332
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #40: vfuusnkaf.exe

ID	40
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 95047, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	199.72s
Return Code	Unknown
PID	3372
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	117
Environment	2
Registry	171
Mutex	3

Process #41: vfuusnkaf.exe

ID	41
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0BrowserSelectionProxy@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 95464, Reason: Child Process
Unmonitor End Time	End Time: 239530, Reason: Terminated
Monitor duration	144.07s
Return Code	0
PID	3376
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #42: vfuusnkaf.exe

ID	42
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0BrowserSelectionProxy@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 95571, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	199.19s
Return Code	Unknown
PID	3360
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #43: vfuusnkaf.exe

ID	43
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0BrowserSelectionProxy@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 95827, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	198.94s
Return Code	Unknown
PID	3352
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #44: vfuusnkaf.exe

ID	44
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0Button@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 95936, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	198.83s
Return Code	Unknown
PID	3388
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #45: vfuusnkaf.exe

ID	45
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Button@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 96348, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	198.41s
Return Code	Unknown
PID	3424
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	117
Environment	2
Registry	171
Mutex	3

Process #46: vfuusnkaf.exe

ID	46
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@$ $QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 96482, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	198.28s
Return Code	Unknown
PID	3436
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #47: vfuusnkaf.exe

ID	47
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCAVI@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 96872, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	197.89s
Return Code	Unknown
PID	3272
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #48: vfuusnkaf.exe

ID	48
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 97174, Reason: Child Process
Unmonitor End Time	End Time: 275358, Reason: Terminated
Monitor duration	178.18s
Return Code	0
PID	1640
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #49: vfuusnkaf.exe

ID	49
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCBase@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 97571, Reason: Child Process
Unmonitor End Time	End Time: 261950, Reason: Terminated
Monitor duration	164.38s
Return Code	0
PID	2240
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #50: vfuusnkaf.exe

ID	50
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCBase@DirectUI@@QEAA@KPEBG@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 97679, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	197.08s
Return Code	Unknown
PID	2252
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #51: vfuusnkaf.exe

ID	51
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCBaseCheckRadioButton@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 98399, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	196.36s
Return Code	Unknown
PID	2264
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	117
Environment	2
Registry	171
Mutex	3

Process #52: vfuusnkaf.exe

ID	52
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCBaseCheckRadioButton@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 98636, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	196.13s
Return Code	Unknown
PID	2276
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #53: vfuusnkaf.exe

ID	53
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCBaseCheckRadioButton@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 99487, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	195.28s
Return Code	Unknown
PID	2292
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	114
Environment	2
Registry	171
Mutex	3

Process #54: vfuusnkaf.exe

ID	54
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCBaseScrollBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 99885, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	194.88s
Return Code	Unknown
PID	2304
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #55: vfuusnkaf.exe

ID	55
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCBaseScrollBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 101846, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	192.92s
Return Code	Unknown
PID	2632
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #56: vfuusnkaf.exe

ID	56
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCBaseScrollBar@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 102226, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	192.54s
Return Code	Unknown
PID	2644
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	114
Environment	2
Registry	171
Mutex	3

Process #57: vfuusnkaf.exe

ID	57
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCCheckBox@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 103231, Reason: Child Process
Unmonitor End Time	End Time: 240836, Reason: Terminated
Monitor duration	137.60s
Return Code	0
PID	2696
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #58: vfuusnkaf.exe

ID	58
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCCheckBox@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 103438, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	191.32s
Return Code	Unknown
PID	2708
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	117
Environment	2
Registry	171
Mutex	3

Process #59: vfuusnkaf.exe

ID	59
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCCheckBox@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 104680, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	190.08s
Return Code	Unknown
PID	2720
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #60: vfuusnkaf.exe

ID	60
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCCommandLink@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 104937, Reason: Child Process
Unmonitor End Time	End Time: 243733, Reason: Terminated
Monitor duration	138.80s
Return Code	0
PID	2732
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	9
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #61: vfuusnkaf.exe

ID	61
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCCommandLink@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 106154, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	188.61s
Return Code	Unknown
PID	2748
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #62: vfuusnkaf.exe

ID	62
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCCommandLink@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 106355, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	188.41s
Return Code	Unknown
PID	2824
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #63: vfuusnkaf.exe

ID	63
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCHScrollBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 107681, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	187.08s
Return Code	Unknown
PID	2836
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	117
Environment	2
Registry	171
Mutex	3

Process #64: vfuusnkaf.exe

ID	64
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCHScrollBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 107890, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	186.87s
Return Code	Unknown
PID	2848
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #65: vfuusnkaf.exe

ID	65
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCHScrollBar@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 108137, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	186.63s
Return Code	Unknown
PID	2864
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #66: vfuusnkaf.exe

ID	66
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCListBox@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 109853, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	184.91s
Return Code	Unknown
PID	2880
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #67: vfuusnkaf.exe

ID	67
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCListBox@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 110106, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	184.66s
Return Code	Unknown
PID	2328
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #68: vfuusnkaf.exe

ID	68
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCListBox@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 110836, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	183.93s
Return Code	Unknown
PID	2340
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #69: vfuusnkaf.exe

ID	69
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCListView@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 111474, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	183.29s
Return Code	Unknown
PID	3324
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #70: vfuusnkaf.exe

ID	70
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCListView@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 112121, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	182.64s
Return Code	Unknown
PID	1676
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #71: vfuusnkaf.exe

ID	71
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCListView@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 112200, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	182.56s
Return Code	Unknown
PID	3548
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #72: vfuusnkaf.exe

ID	72
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCProgressBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 112310, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	182.45s
Return Code	Unknown
PID	3560
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #73: vfuusnkaf.exe

ID	73
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCProgressBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 112559, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	182.20s
Return Code	Unknown
PID	3596
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #74: vfuusnkaf.exe

ID	74
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCProgressBar@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 112926, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	181.84s
Return Code	Unknown
PID	3540
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #75: vfuusnkaf.exe

ID	75
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCPushButton@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 113296, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	181.47s
Return Code	Unknown
PID	3608
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #76: vfuusnkaf.exe

ID	76
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCPushButton@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 113414, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	181.35s
Return Code	Unknown
PID	3476
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #77: vfuusnkaf.exe

ID	77
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCPushButton@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 113576, Reason: Child Process
Unmonitor End Time	End Time: 261584, Reason: Terminated
Monitor duration	148.01s
Return Code	0
PID	3740
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #78: vfuusnkaf.exe

ID	78
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCRadioButton@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 114474, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	180.29s
Return Code	Unknown
PID	3668
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #79: vfuusnkaf.exe

ID	79
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCRadioButton@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 114653, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	180.11s
Return Code	Unknown
PID	3660
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #80: vfuusnkaf.exe

ID	80
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCRadioButton@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 114841, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	179.92s
Return Code	Unknown
PID	3652
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #81: vfuusnkaf.exe

ID	81
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCSysLink@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 115157, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	179.61s
Return Code	Unknown
PID	3636
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #82: vfuusnkaf.exe

ID	82
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCSysLink@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 117012, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	177.75s
Return Code	Unknown
PID	3852
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #83: vfuusnkaf.exe

ID	83
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCSysLink@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 117356, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	177.41s
Return Code	Unknown
PID	3908
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #84: vfuusnkaf.exe

ID	84
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCTrackBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 118068, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	176.69s
Return Code	Unknown
PID	3508
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #85: vfuusnkaf.exe

ID	85
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCTrackBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 118890, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	175.87s
Return Code	Unknown
PID	3504
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #86: vfuusnkaf.exe

ID	86
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCTrackBar@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 119031, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	175.73s
Return Code	Unknown
PID	3960
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #87: vfuusnkaf.exe

ID	87
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCTreeView@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 119800, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	174.96s
Return Code	Unknown
PID	3836
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #88: vfuusnkaf.exe

ID	88
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCTreeView@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 119956, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	174.81s
Return Code	Unknown
PID	3832
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #89: vfuusnkaf.exe

ID	89
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCTreeView@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 120878, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	173.88s
Return Code	Unknown
PID	3828
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #90: vfuusnkaf.exe

ID	90
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCVScrollBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 121219, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	173.54s
Return Code	Unknown
PID	3800
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #91: vfuusnkaf.exe

ID	91
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCVScrollBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 122500, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	172.26s
Return Code	Unknown
PID	3784
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #92: vfuusnkaf.exe

ID	92
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CCVScrollBar@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 122658, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	172.10s
Return Code	Unknown
PID	3780
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #93: vfuusnkaf.exe

ID	93
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CallstackTracker@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 123014, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	171.75s
Return Code	Unknown
PID	772
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #94: vfuusnkaf.exe

ID	94
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CheckBoxGlyph@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 125060, Reason: Child Process
Unmonitor End Time	End Time: 278244, Reason: Terminated
Monitor duration	153.18s
Return Code	0
PID	4092
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #95: vfuusnkaf.exe

ID	95
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CheckBoxGlyph@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 125464, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	169.30s
Return Code	Unknown
PID	3872
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #96: vfuusnkaf.exe

ID	96
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ClassInfoBase@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 125916, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	168.85s
Return Code	Unknown
PID	4016
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #97: vfuusnkaf.exe

ID	97
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ClassInfoBase@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 128454, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	166.31s
Return Code	Unknown
PID	3004
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	117
Environment	2
Registry	171
Mutex	3

Process #98: vfuusnkaf.exe

ID	98
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Clipper@DirectUI@@QEAA@$ $QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 128880, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	165.88s
Return Code	Unknown
PID	2940
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #99: vfuusnkaf.exe

ID	99
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0Clipper@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 136423, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	158.34s
Return Code	Unknown
PID	3012
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #100: vfuusnkaf.exe

ID	100
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Clipper@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 136712, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	158.05s
Return Code	Unknown
PID	1928
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #101: vfuusnkaf.exe

ID	101
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0Combobox@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 137848, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	156.91s
Return Code	Unknown
PID	604
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #102: vfuusnkaf.exe

ID	102
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0Combobox@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 138069, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	156.69s
Return Code	Unknown
PID	3952
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #103: vfuusnkaf.exe

ID	103
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0CritSecLock@DirectUI@@QEAA@PEAU_RTL_CRITICAL_SECTION@@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 139096, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	155.67s
Return Code	Unknown
PID	3924
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #104: vfuusnkaf.exe

ID	104
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0DCSurface@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 139606, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	155.16s
Return Code	Unknown
PID	4048
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #105: vfuusnkaf.exe

ID	105
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0DCSurface@DirectUI@@QEAA@PEAUHDC__@@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 140997, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	153.77s
Return Code	Unknown
PID	2228
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #106: vfuusnkaf.exe

ID	106
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0DUIFactory@DirectUI@@QEAA@PEAUHWND__@@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 141173, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	153.59s
Return Code	Unknown
PID	792
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #107: vfuusnkaf.exe

ID	107
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0DUIXmlParser@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 141371, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	153.39s
Return Code	Unknown
PID	1268
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #108: vfuusnkaf.exe

ID	108
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0DUIXmlParser@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 143173, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	151.59s
Return Code	Unknown
PID	1660
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #109: vfuusnkaf.exe

ID	109
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0DialogElement@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 143727, Reason: Child Process
Unmonitor End Time	End Time: 280896, Reason: Terminated
Monitor duration	137.17s
Return Code	0
PID	2704
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #110: vfuusnkaf.exe

ID	110
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0DialogElement@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 144491, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	150.27s
Return Code	Unknown
PID	3980
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #111: vfuusnkaf.exe

ID	111
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0DialogElement@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 145828, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	148.94s
Return Code	Unknown
PID	2740
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #112: vfuusnkaf.exe

ID	112
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0DuiAccessible@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 145945, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	148.82s
Return Code	Unknown
PID	2844
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #113: vfuusnkaf.exe

ID	113
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0Edit@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 146247, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	148.52s
Return Code	Unknown
PID	1960
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #114: vfuusnkaf.exe

ID	114
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Edit@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 146355, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	148.41s
Return Code	Unknown
PID	892
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #115: vfuusnkaf.exe

ID	115
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0Element@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 146527, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	148.24s
Return Code	Unknown
PID	4012
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #116: vfuusnkaf.exe

ID	116
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Element@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 146720, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	148.04s
Return Code	Unknown
PID	3568
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #117: vfuusnkaf.exe

ID	117
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ElementProvider@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 146899, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	147.86s
Return Code	Unknown
PID	3484
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #118: vfuusnkaf.exe

ID	118
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ElementProxy@DirectUI@@IEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 146952, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	147.81s
Return Code	Unknown
PID	3480
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #119: vfuusnkaf.exe

ID	119
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ElementProxy@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 147109, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	147.65s
Return Code	Unknown
PID	3444
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #120: vfuusnkaf.exe

ID	120
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ElementProxy@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 147190, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	147.57s
Return Code	Unknown
PID	3268
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #121: vfuusnkaf.exe

ID	121
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ElementWithHWND@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 147354, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	147.41s
Return Code	Unknown
PID	3860
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	117
Environment	2
Registry	171
Mutex	3

Process #122: vfuusnkaf.exe

ID	122
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ElementWithHWND@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 147511, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	147.25s
Return Code	Unknown
PID	3920
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #123: vfuusnkaf.exe

ID	123
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ElementWithHWND@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 147571, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	147.19s
Return Code	Unknown
PID	3496
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #124: vfuusnkaf.exe

ID	124
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ExpandCollapseProvider@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 147654, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	147.11s
Return Code	Unknown
PID	936
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #125: vfuusnkaf.exe

ID	125
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ExpandCollapseProxy@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 147935, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	146.83s
Return Code	Unknown
PID	1836
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #126: vfuusnkaf.exe

ID	126
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ExpandCollapseProxy@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 148001, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	146.76s
Return Code	Unknown
PID	3976
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #127: vfuusnkaf.exe

ID	127
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ExpandCollapseProxy@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 148159, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	146.60s
Return Code	Unknown
PID	3824
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #128: vfuusnkaf.exe

ID	128
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Expandable@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 148340, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	146.42s
Return Code	Unknown
PID	1860
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #129: vfuusnkaf.exe

ID	129
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0Expandable@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 148522, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	146.24s
Return Code	Unknown
PID	1436
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #130: vfuusnkaf.exe

ID	130
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0Expandable@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 148617, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	146.15s
Return Code	Unknown
PID	4032
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #131: vfuusnkaf.exe

ID	131
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Expando@DirectUI@@QEAA@$ $QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 148865, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	145.90s
Return Code	Unknown
PID	1980
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #132: vfuusnkaf.exe

ID	132
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0Expando@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 148941, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	145.82s
Return Code	Unknown
PID	2024
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	114
Environment	2
Registry	171
Mutex	3

Process #133: vfuusnkaf.exe

ID	133
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Expando@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 149289, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	145.47s
Return Code	Unknown
PID	3256
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #134: vfuusnkaf.exe

ID	134
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ExpandoButtonGlyph@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 149361, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	145.40s
Return Code	Unknown
PID	2620
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	30
File	117
Environment	2
Registry	589
Mutex	5
Process	1

Process #135: vfuusnkaf.exe

ID	135
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0ExpandoButtonGlyph@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 149545, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	145.22s
Return Code	Unknown
PID	3236
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #136: vfuusnkaf.exe

ID	136
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0FillLayout@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 149767, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	145.00s
Return Code	Unknown
PID	3248
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #137: vfuusnkaf.exe

ID	137
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0FillLayout@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 150105, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	144.66s
Return Code	Unknown
PID	2612
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #138: vfuusnkaf.exe

ID	138
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0FlowLayout@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 150172, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	144.59s
Return Code	Unknown
PID	3316
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #139: vfuusnkaf.exe

ID	139
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0FlowLayout@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 150279, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	144.48s
Return Code	Unknown
PID	1036
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #140: vfuusnkaf.exe

ID	140
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0FontCache@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 150623, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	144.14s
Return Code	Unknown
PID	3940
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #141: vfuusnkaf.exe

ID	141
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0FontCache@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 150685, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	144.08s
Return Code	Unknown
PID	4028
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #142: vfuusnkaf.exe

ID	142
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0FontCache@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 150919, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	143.84s
Return Code	Unknown
PID	1388
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #143: vfuusnkaf.exe

ID	143
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0FontCheckOut@DirectUI@@QEAA@PEAVElement@1@PEAUHDC__@@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 152544, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	142.22s
Return Code	Unknown
PID	1216
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #144: vfuusnkaf.exe

ID	144
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0GridItemProvider@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 152735, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	142.03s
Return Code	Unknown
PID	3456
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #145: vfuusnkaf.exe

ID	145
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0GridItemProxy@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 153111, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	141.65s
Return Code	Unknown
PID	3416
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #146: vfuusnkaf.exe

ID	146
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0GridItemProxy@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 153183, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	141.58s
Return Code	Unknown
PID	2144
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #147: vfuusnkaf.exe

ID	147
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0GridItemProxy@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 153376, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	141.39s
Return Code	Unknown
PID	3672
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #148: vfuusnkaf.exe

ID	148
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0GridLayout@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 153575, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	141.19s
Return Code	Unknown
PID	1820
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #149: vfuusnkaf.exe

ID	149
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0GridLayout@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 154134, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	140.63s
Return Code	Unknown
PID	732
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #150: vfuusnkaf.exe

ID	150
File Name	c:\users\keecfmwgj\desktop\vfuusnkaf.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C: \Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=?? 0GridProvider@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 154285, Reason: Child Process
Unmonitor End Time	End Time: 294763, Reason: Terminated by Timeout
Monitor duration	140.48s
Return Code	Unknown
PID	1432
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca	C:\Users\kEecfMwgj\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll, C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll	Sample File	2276.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
71cbfcc21bb572d6f6532470ff98d3b5ce7ed7fa7d560ae7d11b19383c2309c4	c:\users\keecfmwgj\appdata\local\microsoft\windows\history\history.ie5\index.dat	Modified File	64.00 KB	application/octet-stream	-	CLEAN
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
b1c2cf3e6204e607ff1b0a9162151e8aa36decab7f833bb852e9ef706454eaad	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
35d16e47abd7e21621f47fdcf045370fd546f316ff63a98fda3fbb759b8642c2	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\vfuUsnKAF.exe	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\tmp2h7i6jr7	Accessed File	Access, Read	CLEAN
C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll	Accessed File	Access, Read	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\explorer.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Internet Explorer\iexplore.exe	Accessed File	Access, Read	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{bbfa96fb-03e2-244a-e13e-86541d1b182b}	access	vfuusnkaf.exe	CLEAN
{ba62725d-6184-50d2-b706-2d7b865dd82b}	access	vfuusnkaf.exe	CLEAN
{712d24f9-647f-9b8f-21cf-5266fada45a5}	access	vfuusnkaf.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

Name	Operations	Parent Process Name	Verdict
{65c8ac9c-25ba-82f3-37f2-3fe3857eeb82}	access	explorer.exe	CLEAN
{0a551681-1dc9-107d-38f7-af9fb1aa17f3}	access	explorer.exe	CLEAN
{13aead68-664f-350c-c7cb-a05c41ca6d91}	access	explorer.exe	CLEAN
{2ca9ea5d-c35c-c94c-fe63-9aa486cb1267}	access	explorer.exe	CLEAN
{02d851a8-f7cd-b455-df45-71a402a6edbc}	access	explorer.exe	CLEAN
{6ba32bba-4e96-f5a2-050a-03757c53defe}	access	explorer.exe	CLEAN
{c048b0eb-b8ca-7103-8f33-90bb9cc094e1}	access	explorer.exe	CLEAN
{c7dddfcc-fb68-9c80-b7a6-092779936187}	access	explorer.exe	CLEAN
{b59073af-3f1e-9c2e-af6d-076c62047c1a}	access	explorer.exe	CLEAN
{7f2d86d4-0955-2066-882a-14cbed49896d}	access	explorer.exe	CLEAN
{018d1282-98a9-7481-13d2-c8f764fa5048}	access	explorer.exe	CLEAN

Registry

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

Registry Key	Operations	Parent Process Name	Verdict
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\{E042EE63-C260-8CF6-B219-B4DB821C2E12}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{961EFF9D-BB8C-3A05-CE8E-AB9FF0211A1C}\ShellFolder\{3AA9A263-6EED-2333-7FE8-27102917E617}	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
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

Registry Key	Operations	Parent Process Name	Verdict
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\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-PnrpSvc-UDP-OUT-Active	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-PnrpSvc-UDP-In-EdgeScope-Active	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-SSDPSrv-Out-TCP-Active	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-SSDPSrv-In-TCP-Active	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-SSDPSrv-Out-UDP-Active	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-SSDPSrv-In-UDP-Active	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-Out-TCP-Active	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-In-TCP-EdgeScope-Active	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-DCOM-In-TCP-NoScope-Active	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-RAServer-Out-TCP-NoScope-Active	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-RAServer-In-TCP-NoScope-Active	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-PnrpSvc-UDP-OUT	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-PnrpSvc-UDP-In-EdgeScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-Out-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteAssistance-In-TCP-EdgeScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteFwAdmin-RPCSS-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteFwAdmin-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteFwAdmin-RPCSS-In-TCP-NoScope	access, read	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteFwAdmin-In-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\WINRM-HTTP-Compat-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\WINRM-HTTP-Compat-In-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\WINRM-HTTP-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\WINRM-HTTP-In-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteEventLogSvc-RPCSS-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteEventLogSvc-NP-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteEventLogSvc-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteEventLogSvc-RPCSS-In-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteEventLogSvc-NP-In-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteEventLogSvc-In-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\MSDTC-RPCSS-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\MSDTC-KTMRM-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\MSDTC-Out-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\MSDTC-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\MSDTC-RPCSS-In-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\MSDTC-KTMRM-In-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\MSDTC-Out-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\MSDTC-In-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteTask-RPCSS-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteTask-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteTask-RPCSS-In-TCP-NoScope	access, read	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteTask-In-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteSvcAdmin-RPCSS-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteSvcAdmin-NP-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteSvcAdmin-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteSvcAdmin-RPCSS-In-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteSvcAdmin-NP-In-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\RemoteSvcAdmin-In-TCP-NoScope	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-WSDEVNT-Out-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-WSDEVNT-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-WSDEVNTS-Out-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-WSDEVNTS-In-TCP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-FDRESPUB-WSD-Out-UDP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-FDRESPUB-WSD-In-UDP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-LLMNR-Out-UDP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-LLMNR-In-UDP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-FDPHOST-Out-UDP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-FDPHOST-In-UDP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-NB_Datagram-Out-UDP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-NB_Datagram-In-UDP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-NB_Name-Out-UDP	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-NB_Name-In-UDP	access, read	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
explorer.exe	explorer.exe	SUSPICIOUS
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmp2h7i6jr7" /s	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$PatternProvider@VInvokeProvider@DirectUI@@UIInvokeProvider@@$0A@@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$PatternProvider@VRangeValueProvider@DirectUI@@UIRangeValueProvider@@$03@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$PatternProvider@VScrollItemProvider@DirectUI@@UIScrollItemProvider@@$05@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$PatternProvider@VScrollProvider@DirectUI@@UIScrollProvider@@$04@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$PatternProvider@VSelectionItemProvider@DirectUI@@UISelectionItemProvider@@$06@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$PatternProvider@VSelectionProvider@DirectUI@@UISelectionProvider@@$07@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$PatternProvider@VTableItemProvider@DirectUI@@UITableItemProvider@@$09@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$PatternProvider@VTableProvider@DirectUI@@UITableProvider@@$08@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$PatternProvider@VToggleProvider@DirectUI@@UIToggleProvider@@$0L@@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$PatternProvider@VValueProvider@DirectUI@@UIValueProvider@@$0M@@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0?$SafeArrayAccessor@H@DirectUI@@QEAA@XZ	CLEAN

Process Name	Commandline	Verdict
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0AccessibleButton@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0AccessibleButton@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0AccessibleButton@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0AnimationStrip@DirectUI@@QEAA@AEBV01@@Z	CLEAN
explorer.exe	C:\Windows\Explorer.EXE	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0AnimationStrip@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0AutoLock@DirectUI@@QEAA@PEAU_RTL_CRITICAL_SECTION@@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0AutoThread@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0AutoVariant@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0BaseScrollBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0BaseScrollBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0BaseScrollBar@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0BaseScrollViewer@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0BaseScrollViewer@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0BorderLayout@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0BorderLayout@DirectUI@@QEAA@XZ	CLEAN

Process Name	Commandline	Verdict
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0BrowserSelectionProxy@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0BrowserSelectionProxy@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0BrowserSelectionProxy@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Button@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Button@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCBase@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCBase@DirectUI@@QEAA@KPEBG@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCBaseCheckRadioButton@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCBaseCheckRadioButton@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCBaseCheckRadioButton@DirectUI@@QEAA@K@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCBaseScrollBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCBaseScrollBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCBaseScrollBar@DirectUI@@QEAA@K@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCCheckBox@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCCheckBox@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCCheckBox@DirectUI@@QEAA@K@Z	CLEAN

Process Name	Commandline	Verdict
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCCommandLink@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCCommandLink@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCCommandLink@DirectUI@@QEAA@K@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCHScrollBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCHScrollBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCHScrollBar@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCListBox@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCListBox@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCListBox@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCListView@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCListView@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCListView@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCProgressBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCProgressBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCProgressBar@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCPushButton@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCPushButton@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCPushButton@DirectUI@@QEAA@K@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCRadioButton@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCRadioButton@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCRadioButton@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCSysLink@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN

Process Name	Commandline	Verdict
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCSysLink@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCSysLink@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCTrackBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCTrackBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCTrackBar@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCTreeView@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCTreeView@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCTreeView@DirectUI@@QEAA@K@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCVScrollBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCVScrollBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CCVScrollBar@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CallstackTracker@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CheckBoxGlyph@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CheckBoxGlyph@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ClassInfoBase@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ClassInfoBase@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Clipper@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Clipper@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Clipper@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Combobox@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Combobox@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0CritSecLock@DirectUI@@QEAA@PEAU_RTL_CRITICAL_SECTION@@@Z	CLEAN

Process Name	Commandline	Verdict
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0DCSurface@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0DCSurface@DirectUI@@QEAA@PEAUHDC__@@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0DUIFactory@DirectUI@@QEAA@PEAUHWND__@@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0DUIXmlParser@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0DUIXmlParser@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0DialogElement@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0DialogElement@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0DialogElement@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0DuiAccessible@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Edit@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Edit@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Element@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Element@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ElementProvider@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ElementProxy@DirectUI@@IEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ElementProxy@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ElementProxy@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ElementWithHWND@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ElementWithHWND@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ElementWithHWND@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ExpandCollapseProvider@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ExpandCollapseProxy@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN

Process Name	Commandline	Verdict
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ExpandCollapseProxy@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ExpandCollapseProxy@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Expandable@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Expandable@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Expandable@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Expando@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Expando@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0Expando@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ExpandoButtonGlyph@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0ExpandoButtonGlyph@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0FillLayout@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0FillLayout@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0FlowLayout@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0FlowLayout@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0FontCache@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0FontCache@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0FontCache@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0FontCheckOut@DirectUI@@QEAA@PEAVElement@1@PEAUHDC__@@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0GridItemProvider@DirectUI@@QEAA@XZ	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0GridItemProxy@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0GridItemProxy@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0GridItemProxy@DirectUI@@QEAA@XZ	CLEAN

Process Name	Commandline	Verdict
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0GridLayout@DirectUI@@QEAA@AEBV01@@Z	CLEAN
vfuusnkaf.exe	"C:\Users\kEecfMwgj\Desktop\vfuUsnKAF.exe" /dll="C:\Users\KEECFM~1\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll" /fn_id=??0GridLayout@DirectUI@@QEAA@XZ	CLEAN

Reduced dataset

YARA / AV

Antivirus (4)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\kEecfMwgj\Desktop\a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca.exe.dll	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	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