MALICIOUS

Classifications: Spyware

Threat Names: Trojan.GenericKDZ.75562

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll**
ID	#2783013
MD5	d49772c85d426ce5fe41cf8c5529a5ff
SHA1	4eaa4a005cd6825706634cf5fb9b95c4f546778e
SHA256	73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da
File Size	1336.00 KB
Report Created	2021-09-28 14:54 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (8 rules, 88 matches)

Score	Category	Operation	Count	Classification
4/5	Injection	Modifies control flow of another process	6	-
	• (Process #4) xnczqh.exe alters context of (process #34) explorer.exe. • (Process #3) xnczqh.exe alters context of (process #94) explorer.exe. • (Process #4) xnczqh.exe alters context of (process #94) explorer.exe. • (Process #6) xnczqh.exe alters context of (process #154) explorer.exe. • (Process #29) xnczqh.exe alters context of (process #194) explorer.exe. • (Process #4) xnczqh.exe alters context of (process #226) explorer.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	2	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.75562". • Built-in AV detected a memory dump of (process #226) explorer.exe as "Trojan.GenericKDZ.75562".			
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #226) explorer.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #226) explorer.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
1/5	Discovery	Reads system data	45	-

Score	Category	Operation	Count	Classification
		• (Process #3) xnczqh.exe reads the Windows installation date from registry. • (Process #4) xnczqh.exe reads the Windows installation date from registry. • (Process #5) xnczqh.exe reads the Windows installation date from registry. • (Process #2) xnczqh.exe reads the Windows installation date from registry. • (Process #6) xnczqh.exe reads the Windows installation date from registry. • (Process #7) xnczqh.exe reads the Windows installation date from registry. • (Process #15) xnczqh.exe reads the Windows installation date from registry. • (Process #8) xnczqh.exe reads the Windows installation date from registry. • (Process #12) xnczqh.exe reads the Windows installation date from registry. • (Process #9) xnczqh.exe reads the Windows installation date from registry. • (Process #10) xnczqh.exe reads the Windows installation date from registry. • (Process #11) xnczqh.exe reads the Windows installation date from registry. • (Process #13) xnczqh.exe reads the Windows installation date from registry. • (Process #22) xnczqh.exe reads the Windows installation date from registry. • (Process #14) xnczqh.exe reads the Windows installation date from registry. • (Process #18) xnczqh.exe reads the Windows installation date from registry. • (Process #17) xnczqh.exe reads the Windows installation date from registry. • (Process #20) xnczqh.exe reads the Windows installation date from registry. • (Process #16) xnczqh.exe reads the Windows installation date from registry. • (Process #21) xnczqh.exe reads the Windows installation date from registry. • (Process #19) xnczqh.exe reads the Windows installation date from registry. • (Process #24) xnczqh.exe reads the Windows installation date from registry. • (Process #23) xnczqh.exe reads the Windows installation date from registry. • (Process #25) xnczqh.exe reads the Windows installation date from registry. • (Process #27) xnczqh.exe reads the Windows installation date from registry. • (Process #29) xnczqh.exe reads the Windows installation date from registry. • (Process #26) xnczqh.exe reads the Windows installation date from registry. • (Process #28) xnczqh.exe reads the Windows installation date from registry. • (Process #53) xnczqh.exe reads the Windows installation date from registry. • (Process #82) xnczqh.exe reads the Windows installation date from registry. • (Process #38) xnczqh.exe reads the Windows installation date from registry. • (Process #47) xnczqh.exe reads the Windows installation date from registry. • (Process #125) xnczqh.exe reads the Windows installation date from registry. • (Process #79) xnczqh.exe reads the Windows installation date from registry. • (Process #144) xnczqh.exe reads the Windows installation date from registry. • (Process #121) xnczqh.exe reads the Windows installation date from registry. • (Process #64) xnczqh.exe reads the Windows installation date from registry. • (Process #135) xnczqh.exe reads the Windows installation date from registry. • (Process #88) xnczqh.exe reads the Windows installation date from registry. • (Process #97) xnczqh.exe reads the Windows installation date from registry. • (Process #129) xnczqh.exe reads the Windows installation date from registry. • (Process #78) xnczqh.exe reads the Windows installation date from registry. • (Process #114) xnczqh.exe reads the Windows installation date from registry. • (Process #169) xnczqh.exe reads the Windows installation date from registry. • (Process #226) explorer.exe reads the Windows installation date from registry.		
1/5	Mutex	Creates mutex	30	-

Score	Category	Operation	Count	Classification
		• (Process #4) xnczqh.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{ba62725d-6184-50d2-b706-2d7b865dd82b}". • (Process #3) xnczqh.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{ba62725d-6184-50d2-b706-2d7b865dd82b}". • (Process #3) xnczqh.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{4d4723f4-3231-c9f6-01c4-c1d27a4c4bd8}". • (Process #5) xnczqh.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{4d4723f4-3231-c9f6-01c4-c1d27a4c4bd8}". • (Process #4) xnczqh.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{4d4723f4-3231-c9f6-01c4-c1d27a4c4bd8}". • (Process #6) xnczqh.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{ef578541-399a-fd9e-e289-8a7de092f1e1}". • (Process #29) xnczqh.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{b03188d9-dc52-62a0-6542-6a36e85abcdc}". • (Process #4) xnczqh.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{d548238c-0931-accf-c0f6-d7d58fdc9b42}". • (Process #14) xnczqh.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{d548238c-0931-accf-c0f6-d7d58fdc9b42}". • (Process #226) explorer.exe creates mutex with name "0". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{bbfa96fb-03e2-244a-e13e-86541d1b182b}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{6ae03f50-7a2d-c6e9-ca75-492d6e54c058}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{65c8ac9c-25ba-82f3-37f2-3fe3857eeb82}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{e2bfdadf-a2b6-e661-1346-e3045decc346}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{121b3c01-c2b9-8fd6-4a33-a81c9e5ad022}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{4e86d667-f880-8524-1916-7c7287b1331b}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{4cb4b2d7-d443-0d31-d657-2e588d0f0847}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{35a5844a-04c4-2b9e-20b5-1ed3474b1b1b}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{6bc7ca6d-1ff4-948e-acb8-8ace0ff7d262}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{9699601a-11d0-e0ff-28f5-ad601c034e07}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{ecd35ed5-f792-4a36-e2f9-1c720c8c8b37}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{b5d19349-ced1-2973-477a-88f731ebad8b}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{f207e615-5c45-d37b-bead-454e78cb105c}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{9da07381-49bd-fcd5-49f0-db565310a644}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{042b3ca8-0f60-256b-21a6-0d7a28a1ea42}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{675f95d3-f1a9-8553-af59-6580116ac42b}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{65b97bfc-3a12-e27a-fd30-cf51840b6a30}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{3f101a0b-5225-9c23-d36f-0f50cf5d6f94}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{40c6472e-ca6c-f949-442f-1331c5545e04}". • (Process #226) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{3031726c-f468-1cec-44d7-c5ae97544a09}".		
1/5	Obfuscation	Reads from memory of another process	2	-
		• (Process #3) xnczqh.exe reads from (process #94) explorer.exe. • (Process #4) xnczqh.exe reads from (process #154) explorer.exe.		
-	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

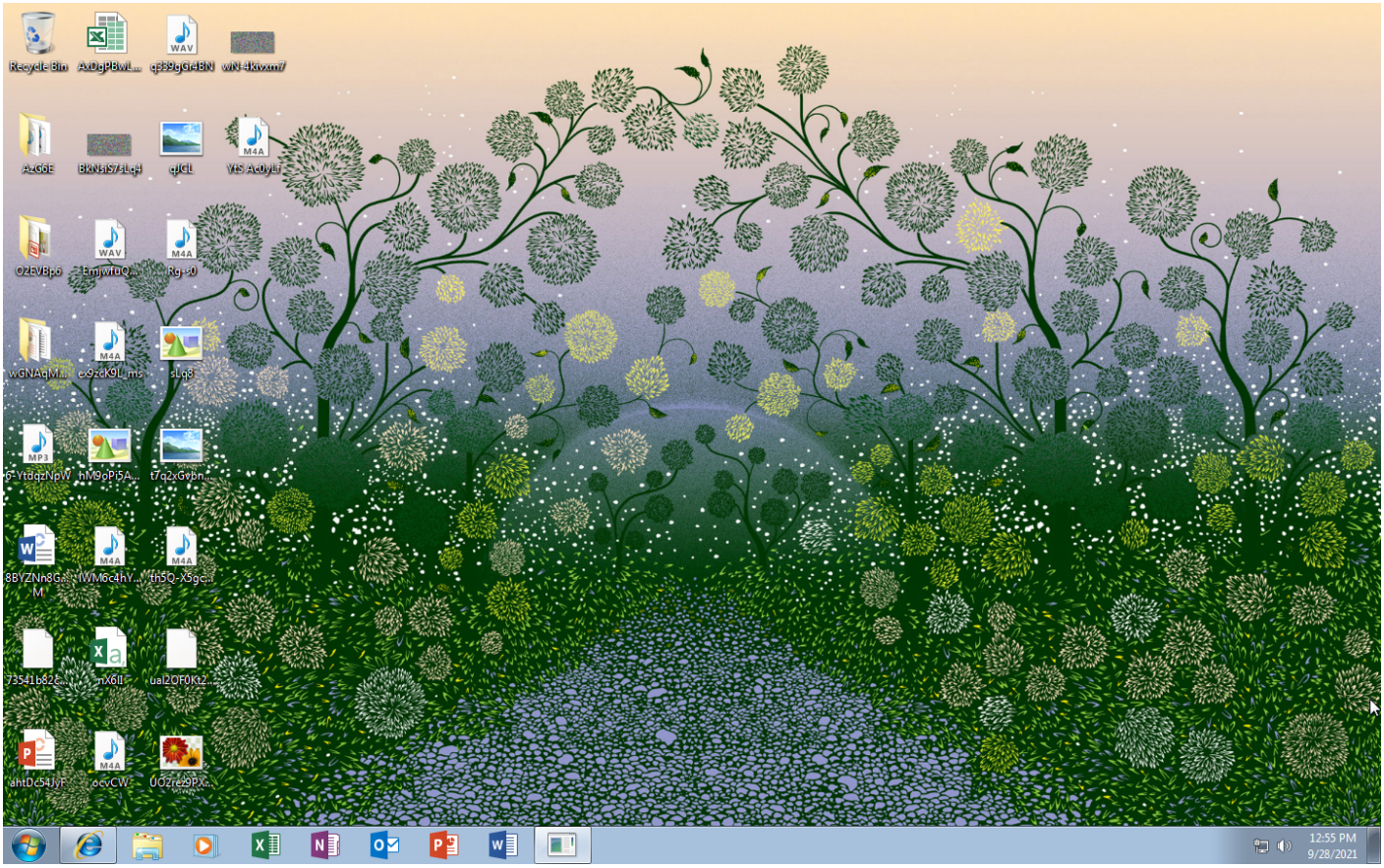
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
					#T1081 Credentials in Files	#T1082 System Information Discovery		#T1119 Automated Collection			
						#T1012 Query Registry		#T1005 Data from Local System			
						#T1083 File and Directory Discovery					

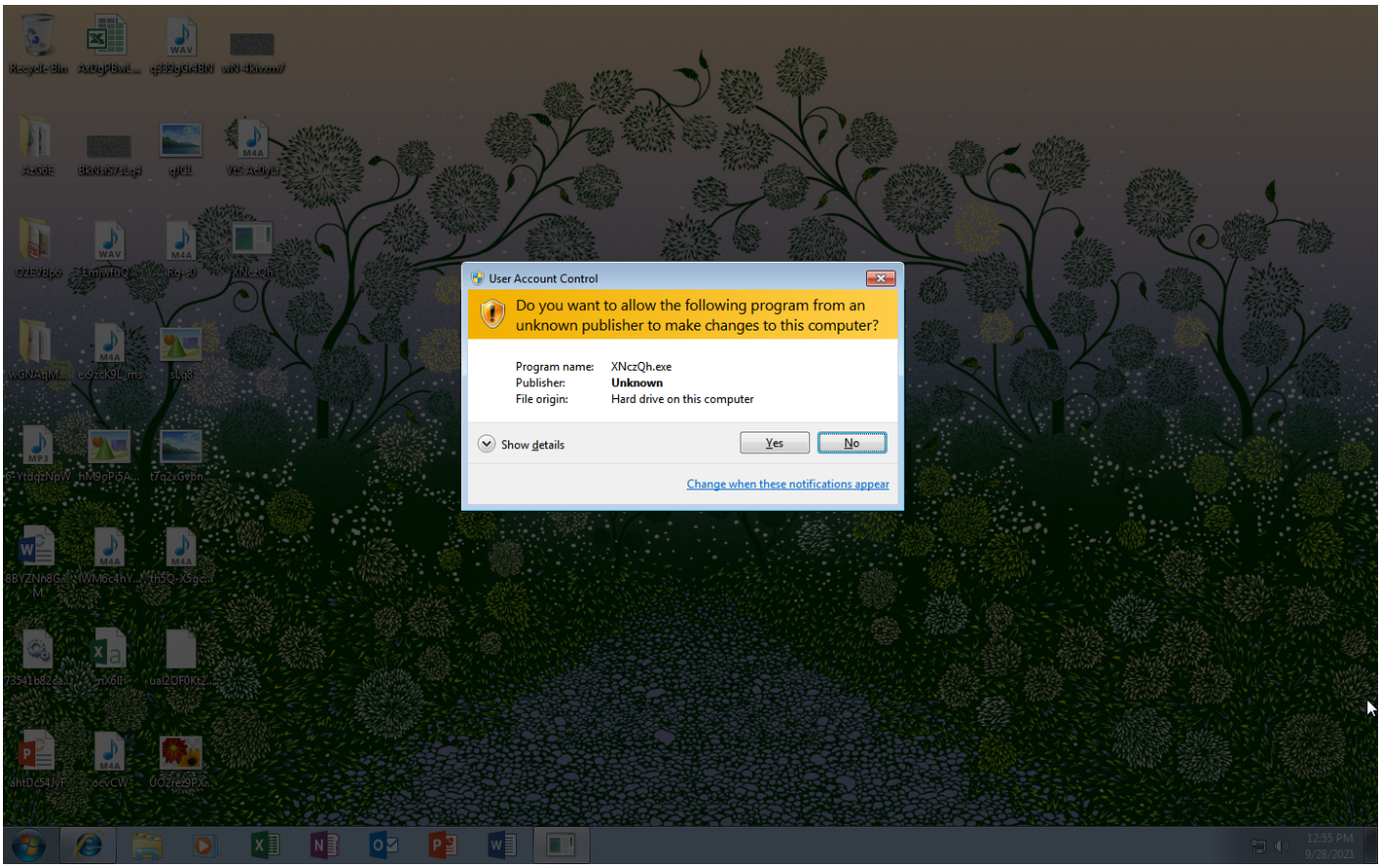
Sample Information

ID	#2783013
MD5	d49772c85d426ce5fe41cf8c5529a5ff
SHA1	4eaa4a005cd6825706634cf5fb9b95c4f546778e
SHA256	73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da
SSDeep	12288:NdMIwS97wJs6tSKDXEabXaC+jhc1S8XXk7CZzHsZH9dq0TbEA:jMIJxSDX3bqjhcfHk7MzH6zn
ImpHash	c6b4c2eec8a93016c63563421e15f011
File Name	73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll
File Size	1336.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 14:54 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	239
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	2
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0





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

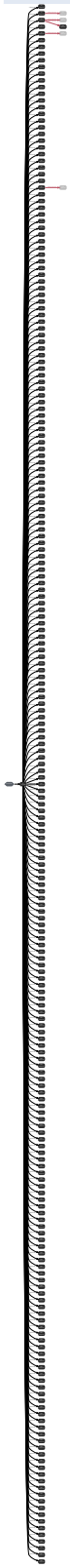
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: xnczqh.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmpuwvadihb" /s
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 42807, Reason: Analysis Target
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	250.01s
Return Code	Unknown
PID	3820
Parent PID	1116
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	16
File	10
Environment	1
Process	234

Process #2: xnczqh.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.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: 59380, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	233.44s
Return Code	Unknown
PID	3848
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	491
Module	28
File	14
Environment	1
Registry	416
User	1
Mutex	482

Process #3: xnczqh.exe

ID	3
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.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: 60421, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	232.40s
Return Code	Unknown
PID	3860
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	274
Module	33
File	14
Environment	1
Process	8
Registry	416
User	1
Mutex	243
-	15
-	63

Process #4: xnczqh.exe

ID	4
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.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: 60553, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	232.27s
Return Code	Unknown
PID	3876
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	302
Module	46
File	14
Environment	1
Process	3
Registry	416
User	1
Mutex	213
-	192
-	34

Process #5: xnczqh.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.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: 60863, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	231.96s
Return Code	Unknown
PID	3888
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	523
Module	28
File	14
Environment	1
Process	6
Registry	416
User	1
Mutex	484

Process #6: xnczqh.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.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: 61139, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	231.68s
Return Code	Unknown
PID	3900
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	493
Module	33
File	14
Environment	1
Registry	416
User	1
Mutex	458
-	37

Process #7: xnczqh.exe

ID	7
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.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: 62874, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	229.94s
Return Code	Unknown
PID	3916
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	615
Module	28
File	14
Environment	1
Registry	416
User	1
Mutex	598

Process #8: xnczqh.exe

ID	8
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.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: 63741, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	229.08s
Return Code	Unknown
PID	3928
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	336
Module	28
File	14
Environment	1
Process	6
Registry	416
User	1
Mutex	294

Process #9: xnczqh.exe

ID	9
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.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: 64355, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	228.46s
Return Code	Unknown
PID	3944
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	568
Module	28
File	14
Environment	1
Process	3
Registry	416
User	1
Mutex	561

Process #10: xnczqh.exe

ID	10
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.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: 65496, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	227.32s
Return Code	Unknown
PID	3956
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	343
Module	28
File	14
Environment	1
Process	4
Registry	416
User	1
Mutex	310

Process #11: xnczqh.exe

ID	11
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.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: 67147, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	225.67s
Return Code	Unknown
PID	3976
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	445
Module	28
File	14
Environment	1
Process	3
Registry	416
User	1
Mutex	437

Process #12: xnczqh.exe

ID	12
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.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: 69327, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	223.49s
Return Code	Unknown
PID	3988
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	573
Module	28
File	14
Environment	1
Process	8
Registry	416
User	1
Mutex	564

Process #13: xnczqh.exe

ID	13
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.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: 69952, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	222.87s
Return Code	Unknown
PID	4000
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	117
Module	28
File	14
Environment	1
Process	1
Registry	416
User	1
Mutex	110

Process #14: xnczqh.exe

ID	14
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.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: 70648, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	222.17s
Return Code	Unknown
PID	4012
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	109
Module	29
File	14
Environment	1
Registry	416
User	1
Mutex	104

Process #15: xnczqh.exe

ID	15
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0? $SafeArrayAccessor@H@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 71400, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	221.42s
Return Code	Unknown
PID	4028
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	622
Module	28
File	14
Environment	1
Registry	416
User	1
Mutex	615

Process #16: xnczqh.exe

ID	16
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0AccessibleButton@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 75394, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	217.43s
Return Code	Unknown
PID	4044
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	21
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #17: xnczqh.exe

ID	17
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0AccessibleButton@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 76096, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	216.72s
Return Code	Unknown
PID	4056
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	11
Environment	1
Registry	416
User	1
Mutex	1

Process #18: xnczqh.exe

ID	18
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0AccessibleButton@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 76986, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	215.83s
Return Code	Unknown
PID	4068
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	12
Module	28
File	14
Environment	1
Registry	416
User	1
Mutex	1

Process #19: xnczqh.exe

ID	19
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0AnimationStrip@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82059, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	210.76s
Return Code	Unknown
PID	4080
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	110
Module	21
File	14
Environment	1
Registry	416
User	1
Mutex	102

Process #20: xnczqh.exe

ID	20
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0AnimationStrip@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82995, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	209.82s
Return Code	Unknown
PID	4092
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	22
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #21: xnczqh.exe

ID	21
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83907, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	208.91s
Return Code	Unknown
PID	2928
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	342
Module	28
File	14
Environment	1
Registry	416
User	1
Mutex	335

Process #22: xnczqh.exe

ID	22
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0AutoButton@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87737, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	205.08s
Return Code	Unknown
PID	2916
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	14
Environment	1
Registry	416
User	1
Mutex	1

Process #23: xnczqh.exe

ID	23
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 88723, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	204.10s
Return Code	Unknown
PID	2904
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #24: xnczqh.exe

ID	24
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0AutoLock@DirectUI@@QEAA@PEAU_RTL_CRITICAL_SECTION@@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89815, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	203.00s
Return Code	Unknown
PID	2892
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1

Process #25: xnczqh.exe

ID	25
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0AutoThread@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 96082, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	196.74s
Return Code	Unknown
PID	2872
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	22
Module	28
File	14
Environment	1
Registry	416
User	1
Mutex	16

Process #26: xnczqh.exe

ID	26
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0AutoVariant@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 97089, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	195.73s
Return Code	Unknown
PID	2860
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #27: xnczqh.exe

ID	27
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0BaseScrollBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 99173, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	193.65s
Return Code	Unknown
PID	2844
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	129
Module	28
File	14
Environment	1
Registry	416
User	1
Mutex	122

Process #28: xnczqh.exe

ID	28
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0BaseScrollBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 101374, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	191.44s
Return Code	Unknown
PID	2828
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #29: xnczqh.exe

ID	29
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0BaseScrollBar@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 103070, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	189.75s
Return Code	Unknown
PID	2816
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	70
Module	38
File	14
Environment	1
Registry	416
User	1
Mutex	26
-	75

Process #30: xnczqh.exe

ID	30
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0BaseScrollViewer@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 103674, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	189.15s
Return Code	Unknown
PID	2804
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #31: xnczqh.exe

ID	31
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0BaseScrollViewer@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 106422, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	186.40s
Return Code	Unknown
PID	2792
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #32: xnczqh.exe

ID	32
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@$ $QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 106834, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	185.99s
Return Code	Unknown
PID	2780
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #33: xnczqh.exe

ID	33
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0Bind@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 107231, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	185.59s
Return Code	Unknown
PID	2768
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #34: explorer.exe

ID	34
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 107393, Reason: Injection
Unmonitor End Time	End Time: 140505, Reason: Terminated
Monitor duration	33.11s
Return Code	0
PID	1116
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (119)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x460	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x4bc	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x4cc	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x4d4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x52c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x534	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x540	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x5d8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x478	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x510	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x514	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x51c	0x777313f0(2004030448)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x53c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x350	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x354	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x5a4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x790	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x5b8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x5b0	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x7bc	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x2f4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x5f8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x338	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x718	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xa14	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xac8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xd5c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xd68	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xd80	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xdf0	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77732ed0(2004037328)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x460	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x4bc	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x4cc	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x4d4	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x52c	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x534	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x540	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x5d8	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x478	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x510	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x514	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x51c	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x53c	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x350	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x354	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x5a4	0x777313f0(2004030448)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x790	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x5b8	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x5b0	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x7bc	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x2f4	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x5f8	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x338	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x718	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xa14	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xac8	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xd5c	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xd68	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xd80	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xdf0	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xd1c	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x474	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77732ed0(2004037328)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✖	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✖	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0x50c	0x77526a30(2001889840)	-	✖	1

Process #35: xnczqh.exe

ID	35
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 108912, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	183.91s
Return Code	Unknown
PID	2940
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #36: xnczqh.exe

ID	36
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0BorderLayout@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 111853, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	180.97s
Return Code	Unknown
PID	3248
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #37: xnczqh.exe

ID	37
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0BorderLayout@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 112339, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	180.48s
Return Code	Unknown
PID	3332
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #38: xnczqh.exe

ID	38
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 112741, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	180.08s
Return Code	Unknown
PID	3368
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #39: xnczqh.exe

ID	39
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0Browser@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 113111, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	179.71s
Return Code	Unknown
PID	3180
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #40: xnczqh.exe

ID	40
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 113667, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	179.15s
Return Code	Unknown
PID	3176
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #41: xnczqh.exe

ID	41
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0BrowserSelectionProxy@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 117810, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	175.01s
Return Code	Unknown
PID	3380
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #42: xnczqh.exe

ID	42
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0BrowserSelectionProxy@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 118594, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	174.22s
Return Code	Unknown
PID	3364
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #43: xnczqh.exe

ID	43
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0BrowserSelectionProxy@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 119224, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	173.59s
Return Code	Unknown
PID	3344
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #44: xnczqh.exe

ID	44
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0Button@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 121639, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	171.18s
Return Code	Unknown
PID	3392
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #45: xnczqh.exe

ID	45
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Button@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 122417, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	170.40s
Return Code	Unknown
PID	3408
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #46: xnczqh.exe

ID	46
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 123037, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	169.78s
Return Code	Unknown
PID	3404
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #47: xnczqh.exe

ID	47
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCAVI@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 124637, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	168.18s
Return Code	Unknown
PID	384
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	14
Environment	1
Registry	416
User	1
Mutex	1

Process #48: xnczqh.exe

ID	48
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 126238, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	166.58s
Return Code	Unknown
PID	3252
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #49: xnczqh.exe

ID	49
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCBase@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 126440, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	166.38s
Return Code	Unknown
PID	2092
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #50: xnczqh.exe

ID	50
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCBase@DirectUI@@QEAA@KPEBG@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 126745, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	166.07s
Return Code	Unknown
PID	2228
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #51: xnczqh.exe

ID	51
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCBaseCheckRadioButton@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 127481, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	165.34s
Return Code	Unknown
PID	2240
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #52: xnczqh.exe

ID	52
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCBaseCheckRadioButton@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 127591, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	165.23s
Return Code	Unknown
PID	2252
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #53: xnczqh.exe

ID	53
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCBaseCheckRadioButton@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 127749, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	165.07s
Return Code	Unknown
PID	2264
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #54: xnczqh.exe

ID	54
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCBaseScrollBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 128390, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	164.43s
Return Code	Unknown
PID	2276
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #55: xnczqh.exe

ID	55
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCBaseScrollBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 128501, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	164.32s
Return Code	Unknown
PID	2288
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #56: xnczqh.exe

ID	56
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCBaseScrollBar@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 128610, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	164.21s
Return Code	Unknown
PID	2588
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #57: xnczqh.exe

ID	57
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCCheckBox@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 128793, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	164.03s
Return Code	Unknown
PID	2600
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #58: xnczqh.exe

ID	58
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCCheckBox@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 129496, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	163.32s
Return Code	Unknown
PID	2612
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #59: xnczqh.exe

ID	59
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCCheckBox@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 129856, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	162.96s
Return Code	Unknown
PID	2624
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #60: xnczqh.exe

ID	60
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCCommandLink@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 130277, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	162.54s
Return Code	Unknown
PID	2636
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #61: xnczqh.exe

ID	61
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCCommandLink@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 130733, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	162.09s
Return Code	Unknown
PID	2648
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #62: xnczqh.exe

ID	62
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCCommandLink@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 131154, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	161.66s
Return Code	Unknown
PID	2660
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #63: xnczqh.exe

ID	63
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCHScrollBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 131621, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	161.20s
Return Code	Unknown
PID	2672
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	25
File	3
Environment	1

Process #64: xnczqh.exe

ID	64
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCHScrollBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 132061, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	160.76s
Return Code	Unknown
PID	2684
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #65: xnczqh.exe

ID	65
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCHScrollBar@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 132640, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	160.18s
Return Code	Unknown
PID	2696
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #66: xnczqh.exe

ID	66
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCListBox@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 132860, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	159.96s
Return Code	Unknown
PID	2708
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #67: xnczqh.exe

ID	67
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCListBox@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 133143, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	159.68s
Return Code	Unknown
PID	2720
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #68: xnczqh.exe

ID	68
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCListBox@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 133318, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	159.50s
Return Code	Unknown
PID	2732
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #69: xnczqh.exe

ID	69
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCListView@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 133924, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	158.90s
Return Code	Unknown
PID	2744
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #70: xnczqh.exe

ID	70
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCListView@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 134039, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	158.78s
Return Code	Unknown
PID	2756
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #71: xnczqh.exe

ID	71
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCListView@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 134178, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	158.64s
Return Code	Unknown
PID	3320
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #72: xnczqh.exe

ID	72
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCProgressBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 134370, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	158.45s
Return Code	Unknown
PID	796
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #73: xnczqh.exe

ID	73
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCProgressBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 135113, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	157.71s
Return Code	Unknown
PID	3560
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #74: xnczqh.exe

ID	74
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCProgressBar@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 135270, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	157.55s
Return Code	Unknown
PID	3576
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #75: xnczqh.exe

ID	75
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCPushButton@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 135538, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	157.28s
Return Code	Unknown
PID	1036
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #76: xnczqh.exe

ID	76
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCPushButton@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 136147, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	156.67s
Return Code	Unknown
PID	1032
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #77: xnczqh.exe

ID	77
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCPushButton@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 136271, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	156.55s
Return Code	Unknown
PID	3532
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #78: xnczqh.exe

ID	78
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCRadioButton@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 136400, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	156.42s
Return Code	Unknown
PID	3520
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #79: xnczqh.exe

ID	79
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCRadioButton@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 136570, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	156.25s
Return Code	Unknown
PID	3464
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	11
Environment	1
Registry	416
User	1
Mutex	1

Process #80: xnczqh.exe

ID	80
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCRadioButton@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 137424, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	155.40s
Return Code	Unknown
PID	3504
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #81: xnczqh.exe

ID	81
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCSysLink@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 138314, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	154.50s
Return Code	Unknown
PID	3716
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #82: xnczqh.exe

ID	82
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCSysLink@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 138751, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	154.07s
Return Code	Unknown
PID	3784
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	12
Module	28
File	14
Environment	1
Registry	416
User	1
Mutex	1

Process #83: xnczqh.exe

ID	83
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCSysLink@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 139040, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	153.78s
Return Code	Unknown
PID	3640
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #84: xnczqh.exe

ID	84
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCTrackBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 139345, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	153.47s
Return Code	Unknown
PID	800
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #85: xnczqh.exe

ID	85
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCTrackBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 140431, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	152.39s
Return Code	Unknown
PID	1588
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #86: xnczqh.exe

ID	86
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCTrackBar@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 141030, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	151.79s
Return Code	Unknown
PID	3884
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	25
File	8
Environment	1

Process #87: xnczqh.exe

ID	87
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCTreeView@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 141313, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	151.51s
Return Code	Unknown
PID	3448
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #88: xnczqh.exe

ID	88
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCTreeView@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 141905, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	150.91s
Return Code	Unknown
PID	3424
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #89: xnczqh.exe

ID	89
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCTreeView@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 142146, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	150.67s
Return Code	Unknown
PID	3936
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #90: xnczqh.exe

ID	90
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCVScrollBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 142445, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	150.37s
Return Code	Unknown
PID	3968
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #91: xnczqh.exe

ID	91
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCVScrollBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 143131, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	149.69s
Return Code	Unknown
PID	3776
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #92: xnczqh.exe

ID	92
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CCVScrollBar@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 144767, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	148.05s
Return Code	Unknown
PID	3744
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #93: xnczqh.exe

ID	93
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CallstackTracker@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 146539, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	146.28s
Return Code	Unknown
PID	2932
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #94: explorer.exe

ID	94
File Name	c:\windows\explorer.exe
Command Line	explorer.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 148589, Reason: Injection
Unmonitor End Time	End Time: 186397, Reason: Terminated
Monitor duration	37.81s
Return Code	0
PID	3708
Parent PID	420
Bitness	64 Bit

Injection Information (45)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xe80	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0x530	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf54	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xe2c	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xed4	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xed8	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77732ed0(2004037328)	-	✔	1
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#3: c: \users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xe80	0x777313f0(2004030448)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0x530	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf54	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xe2c	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xed4	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xed8	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf7c	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xeb4	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf90	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xfa8	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xfb4	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xda8	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xfd4	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xfec	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0x7b0	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0x6e4	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x777313f0(2004030448)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✗	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✗	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf48	0x77526a30(2001889840)	-	✗	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0xf90	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#3: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf18 / 0x524	0x777313f0(2004030448)	-	✗	1
Modify Control Flow	#4: c:\users\keecfmwgj\desktop\xnczqh.exe	0xf28 / 0xf90	0x777313f0(2004030448)	-	✓	1

Process #95: xnczqh.exe

ID	95
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CheckBoxGlyph@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 153230, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	139.59s
Return Code	Unknown
PID	2908
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #96: xnczqh.exe

ID	96
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CheckBoxGlyph@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 153607, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	139.21s
Return Code	Unknown
PID	604
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #97: xnczqh.exe

ID	97
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ClassInfoBase@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 153945, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	138.87s
Return Code	Unknown
PID	1408
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1

Process #98: xnczqh.exe

ID	98
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ClassInfoBase@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 156571, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	136.25s
Return Code	Unknown
PID	1412
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #99: xnczqh.exe

ID	99
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Clipper@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 158767, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	134.05s
Return Code	Unknown
PID	1004
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	25
File	3
Environment	1

Process #100: xnczqh.exe

ID	100
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0Clipper@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 160600, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	132.22s
Return Code	Unknown
PID	2820
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #101: xnczqh.exe

ID	101
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Clipper@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 162953, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	129.87s
Return Code	Unknown
PID	2096
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	25
File	3
Environment	1

Process #102: xnczqh.exe

ID	102
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0Combobox@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 163200, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	129.62s
Return Code	Unknown
PID	896
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #103: xnczqh.exe

ID	103
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Combobox@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 163615, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	129.20s
Return Code	Unknown
PID	1208
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #104: xnczqh.exe

ID	104
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0CritSecLock@DirectUI@@QEAA@PEAU_RTL_CRITICAL_SECTION@@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 165678, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	127.14s
Return Code	Unknown
PID	3336
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #106: xnczqh.exe

ID	106
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0DCSurface@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 165865, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	126.95s
Return Code	Unknown
PID	3192
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #107: xnczqh.exe

ID	107
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0DCSurface@DirectUI@@QEAA@PEAUHDC__@@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 166025, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	126.79s
Return Code	Unknown
PID	1976
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #108: xnczqh.exe

ID	108
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0DUIFactory@DirectUI@@QEAA@PEAUHWND__@@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 166228, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	126.59s
Return Code	Unknown
PID	3312
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #109: xnczqh.exe

ID	109
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0DUIXmlParser@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 167563, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	125.26s
Return Code	Unknown
PID	548
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #110: xnczqh.exe

ID	110
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0DUIXmlParser@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 167879, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	124.94s
Return Code	Unknown
PID	1872
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #111: xnczqh.exe

ID	111
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0DialogElement@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 168030, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	124.79s
Return Code	Unknown
PID	3216
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #112: xnczqh.exe

ID	112
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0DialogElement@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 168336, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	124.48s
Return Code	Unknown
PID	3228
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #113: xnczqh.exe

ID	113
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0DialogElement@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 169425, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	123.39s
Return Code	Unknown
PID	2964
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #114: xnczqh.exe

ID	114
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0DuiAccessible@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 169742, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	123.08s
Return Code	Unknown
PID	3148
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #115: xnczqh.exe

ID	115
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0Edit@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 169933, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	122.89s
Return Code	Unknown
PID	3136
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #116: xnczqh.exe

ID	116
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Edit@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 170160, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	122.66s
Return Code	Unknown
PID	1304
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #117: xnczqh.exe

ID	117
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0Element@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 170469, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	122.35s
Return Code	Unknown
PID	3200
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #118: xnczqh.exe

ID	118
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Element@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 171436, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	121.38s
Return Code	Unknown
PID	3388
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #119: xnczqh.exe

ID	119
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ElementProvider@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 171859, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	120.96s
Return Code	Unknown
PID	3484
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #120: xnczqh.exe

ID	120
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ElementProxy@DirectUI@@IEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 172881, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	119.94s
Return Code	Unknown
PID	3480
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #121: xnczqh.exe

ID	121
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ElementProxy@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 173108, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	119.71s
Return Code	Unknown
PID	1996
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #122: xnczqh.exe

ID	122
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ElementProxy@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 173500, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	119.32s
Return Code	Unknown
PID	1708
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #123: xnczqh.exe

ID	123
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ElementWithHWND@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 173717, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	119.10s
Return Code	Unknown
PID	2024
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #124: xnczqh.exe

ID	124
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ElementWithHWND@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 174760, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	118.06s
Return Code	Unknown
PID	2224
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #125: xnczqh.exe

ID	125
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ElementWithHWND@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 175308, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	117.51s
Return Code	Unknown
PID	2236
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #126: xnczqh.exe

ID	126
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ExpandCollapseProvider@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 175559, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	117.26s
Return Code	Unknown
PID	2272
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #127: xnczqh.exe

ID	127
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ExpandCollapseProxy@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 176490, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	116.33s
Return Code	Unknown
PID	2584
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #128: xnczqh.exe

ID	128
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ExpandCollapseProxy@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 176634, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	116.19s
Return Code	Unknown
PID	2608
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #129: xnczqh.exe

ID	129
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ExpandCollapseProxy@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 176828, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	115.99s
Return Code	Unknown
PID	2632
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #130: xnczqh.exe

ID	130
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Expandable@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 177117, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	115.70s
Return Code	Unknown
PID	3592
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #131: xnczqh.exe

ID	131
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0Expandable@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 178115, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	114.70s
Return Code	Unknown
PID	2680
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #132: xnczqh.exe

ID	132
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0Expandable@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 179235, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	113.58s
Return Code	Unknown
PID	2716
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #133: xnczqh.exe

ID	133
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Expando@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 180189, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	112.63s
Return Code	Unknown
PID	2752
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #134: xnczqh.exe

ID	134
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0Expando@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 181987, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	110.83s
Return Code	Unknown
PID	3516
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #135: xnczqh.exe

ID	135
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Expando@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 182256, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	110.56s
Return Code	Unknown
PID	3556
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #136: xnczqh.exe

ID	136
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ExpandoButtonGlyph@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 182656, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	110.16s
Return Code	Unknown
PID	3612
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #137: xnczqh.exe

ID	137
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0ExpandoButtonGlyph@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 184469, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	108.35s
Return Code	Unknown
PID	1228
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #138: xnczqh.exe

ID	138
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0FillLayout@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 184700, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	108.12s
Return Code	Unknown
PID	1332
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #139: xnczqh.exe

ID	139
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0FillLayout@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 184953, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	107.87s
Return Code	Unknown
PID	1144
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #140: xnczqh.exe

ID	140
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0FlowLayout@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 186011, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	106.81s
Return Code	Unknown
PID	1340
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #141: xnczqh.exe

ID	141
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0FlowLayout@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 186232, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	106.59s
Return Code	Unknown
PID	1444
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #142: xnczqh.exe

ID	142
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0FontCache@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 186595, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	106.22s
Return Code	Unknown
PID	1980
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #143: xnczqh.exe

ID	143
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0FontCache@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 187629, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	105.19s
Return Code	Unknown
PID	824
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #144: xnczqh.exe

ID	144
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0FontCache@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 187787, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	105.03s
Return Code	Unknown
PID	2760
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	28
File	10
Environment	1
Registry	416
User	1
Mutex	1

Process #145: xnczqh.exe

ID	145
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0FontCheckOut@DirectUI@@QEAA@PEAVElement@1@PEAUHDC__@@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 189293, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	103.53s
Return Code	Unknown
PID	3568
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #146: xnczqh.exe

ID	146
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0GridItemProvider@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 189766, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	103.05s
Return Code	Unknown
PID	1120
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #147: xnczqh.exe

ID	147
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0GridItemProxy@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 190608, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	102.21s
Return Code	Unknown
PID	1904
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #148: xnczqh.exe

ID	148
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0GridItemProxy@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 190873, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	101.95s
Return Code	Unknown
PID	3792
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #149: xnczqh.exe

ID	149
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0GridItemProxy@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 191068, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	101.75s
Return Code	Unknown
PID	3752
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #150: xnczqh.exe

ID	150
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C: \Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=?? 0GridLayout@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 192089, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	100.73s
Return Code	Unknown
PID	3772
Parent PID	3820
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #151: xnczqh.exe

ID	151
File Name	c:\users\keecfmwgj\desktop\xnczqh.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0GridLayout@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 192314, Reason: Child Process
Unmonitor End Time	End Time: 292819, Reason: Terminated by Timeout
Monitor duration	100.50s
Return Code	Unknown
PID	4036
Parent PID	3820
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
73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da	C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll, C:\Users\kEecfMwgj\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll	Sample File	1336.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
8ed2fe1ab8a23c8d75f8765a2f30c9e2987b197e4084dc8518ac46a76d46c2ff	c:\users\keecfmwgj\appdata\local\microsoft\windows\history\history.ie5\index.dat	Modified File	80.00 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
dad87da879bdfbe6a5cc15eb44dc703a2b8daf60e85b33a241bb4a2c58d62c63	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
c9b5be37474586c13713122a68fd66fa42fff4241412cc59e29df82610d8db49	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\XNczQh.exe	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\tmpuwvadihb	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Access, Read	CLEAN
C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll	Accessed File	Access, Read	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\explorer.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Identities\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Identities\{31810C36-5D23-4CCE-A3B4-316DED195C38}\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\AddIns\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Crypto\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Crypto\RSA\	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Document Building Blocks\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Document Building Blocks\1033\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Excel\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Excel\XLSTART\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Internet Explorer\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\ImplicitAppShortcuts\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Network\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Network\Connections\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Network\Connections\Pbk\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Proof\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\SystemCertificates\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\SystemCertificates\My\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Cookies\Low\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\IECompatCache\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\IECompatCache\Low\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\IETldCache\Low\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\NetworkShortcuts\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\PrinterShortcuts\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\PrivacIE\Low\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Templates\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Word\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Word\STARTUP\	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files (x86)\Internet Explorer\iexplore.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\netsh.exe	Accessed File	Access	CLEAN
C:\Windows\system32\TSTheme.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\irftp.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\xpsrchvw.exe	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\Microsoft OneDrive\outlook.exe	Accessed File	Access, Read	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
\Sessions\1\BaseNamedObjects\{bbfa96fb-03e2-244a-e13e-86541d1b182b}	access	xnczqh.exe	CLEAN
\Sessions\1\BaseNamedObjects\{ba62725d-6184-50d2-b706-2d7b865dd82b}	access	xnczqh.exe	CLEAN
\Sessions\1\BaseNamedObjects\{4d4723f4-3231-c9f6-01c4-c1d27a4c4bd8}	access	xnczqh.exe	CLEAN
\Sessions\1\BaseNamedObjects\{ef578541-399a-fd9e-e289-8a7de092f1e1}	access	xnczqh.exe	CLEAN
\Sessions\1\BaseNamedObjects\{b03188d9-dc52-62a0-6542-6a36e85abcdc}	access	xnczqh.exe	CLEAN
\Sessions\1\BaseNamedObjects\{d548238c-0931-accf-c0f6-d7d58fdc9b42}	access	xnczqh.exe	CLEAN
0	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{6ae03f50-7a2d-c6e9-ca75-492d6e54c058}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{65c8ac9c-25ba-82f3-37f2-3fe3857eeb82}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{e2bfdadf-a2b6-e661-1346-e3045decc346}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{121b3c01-c2b9-8fd6-4a33-a81c9e5ad022}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{4e86d667-f880-8524-1916-7c7287b1331b}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{4cb4b2d7-d443-0d31-d657-2e588d0f0847}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{35a5844a-04c4-2b9e-20b5-1ed3474b1b1b}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{6bc7ca6d-1ff4-948e-acb8-8ace0ff7d262}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{9699601a-11d0-e0ff-28f5-ad601c034e07}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{ecd35ed5-f792-4a36-e2f9-1c720c8c8b37}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{b5d19349-ced1-2973-477a-88f731ebad8b}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{f207e615-5c45-d37b-bead-454e78cb105c}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{9da07381-49bd-fcd5-49f0-db565310a644}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{042b3ca8-0f60-256b-21a6-0d7a28a1ea42}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{675f95d3-f1a9-8553-af59-6580116ac42b}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
\Sessions\1\BaseNamedObjects\{65b97bfc-3a12-e27a-fd30-cf51840b6a30}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{3f101a0b-5225-9c23-d36f-0f50cf5d6f94}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{40c6472e-ca6c-f949-442f-1331c5545e04}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{3031726c-f468-1cec-44d7-c5ae97544a09}	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE	access	xnczqh.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE	access	xnczqh.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft	access	xnczqh.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows	access	xnczqh.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion	access	xnczqh.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	access	xnczqh.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	access	xnczqh.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	access, read	xnczqh.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin	access, read	xnczqh.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop	access, read	xnczqh.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT	access	xnczqh.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	xnczqh.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate	access, read	xnczqh.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
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

Registry Key	Operations	Parent Process Name	Verdict
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\{D57BFD99-72FA-EBCF-6359-7D853217D93C}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{961EFF9D-BB8C-3A05-CE8E-AB9FF0211A1C}\ShellFolder\{5C4892CF-0F89-038F-5F0C-6D2729D1B889}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{6637DB77-7BBF-C6DD-642D-230B00070679}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{6637DB77-7BBF-C6DD-642D-230B00070679}\ShellFolder\{A1F8CF23-2EDE-5C4A-00A4-6CF97B7AF725}	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
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

Registry Key	Operations	Parent Process Name	Verdict
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

Process

Process Name	Commandline	Verdict
explorer.exe	explorer.exe	SUSPICIOUS
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmpuwvadihb" /s	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$PatternProvider@VInvokeProvider@DirectUI@@UIInvokeProvider@@$0A@@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$PatternProvider@VRangeValueProvider@DirectUI@@UIRangeValueProvider@@$03@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$PatternProvider@VScrollItemProvider@DirectUI@@UIScrollItemProvider@@$05@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$PatternProvider@VScrollProvider@DirectUI@@UIScrollProvider@@$04@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$PatternProvider@VSelectionItemProvider@DirectUI@@UISelectionItemProvider@@$06@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$PatternProvider@VSelectionProvider@DirectUI@@UISelectionProvider@@$07@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$PatternProvider@VTableItemProvider@DirectUI@@UITableItemProvider@@$09@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$PatternProvider@VTableProvider@DirectUI@@UITableProvider@@$08@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$PatternProvider@VToggleProvider@DirectUI@@UIToggleProvider@@$0L@@DirectUI@@QEAA@XZ	CLEAN

Process Name	Commandline	Verdict
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$PatternProvider@VValueProvider@DirectUI@@UIValueProvider@@$0M@@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0?$SafeArrayAccessor@H@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0AccessibleButton@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0AccessibleButton@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0AccessibleButton@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0AnimationStrip@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0AnimationStrip@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0AutoLock@DirectUI@@QEAA@PEAU_RTL_CRITICAL_SECTION@@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0AutoThread@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0AutoVariant@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0BaseScrollBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0BaseScrollBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0BaseScrollBar@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0BaseScrollViewer@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0BaseScrollViewer@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@AEBV01@@Z	CLEAN
explorer.exe	C:\Windows\Explorer.EXE	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@XZ	CLEAN

Process Name	Commandline	Verdict
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0BorderLayout@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0BorderLayout@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0BrowserSelectionProxy@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0BrowserSelectionProxy@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0BrowserSelectionProxy@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Button@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Button@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCBase@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCBase@DirectUI@@QEAA@KPEBG@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCBaseCheckRadioButton@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCBaseCheckRadioButton@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCBaseCheckRadioButton@DirectUI@@QEAA@K@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCBaseScrollBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCBaseScrollBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCBaseScrollBar@DirectUI@@QEAA@K@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCCheckBox@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN

Process Name	Commandline	Verdict
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCCheckBox@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCCheckBox@DirectUI@@QEAA@K@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCCommandLink@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCCommandLink@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCCommandLink@DirectUI@@QEAA@K@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCHScrollBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCHScrollBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCHScrollBar@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCListBox@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCListBox@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCListBox@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCListView@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCListView@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCListView@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCProgressBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCProgressBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCProgressBar@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCPushButton@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCPushButton@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCPushButton@DirectUI@@QEAA@K@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCRadioButton@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCRadioButton@DirectUI@@QEAA@AEBV01@@Z	CLEAN

Process Name	Commandline	Verdict
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCRadioButton@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCSysLink@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCSysLink@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCSysLink@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCTrackBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCTrackBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCTrackBar@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCTreeView@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCTreeView@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCTreeView@DirectUI@@QEAA@K@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCVScrollBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCVScrollBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CCVScrollBar@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CallstackTracker@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CheckBoxGlyph@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CheckBoxGlyph@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ClassInfoBase@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ClassInfoBase@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Clipper@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Clipper@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Clipper@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Combobox@DirectUI@@QEAA@AEBV01@@Z	CLEAN

Process Name	Commandline	Verdict
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Combobox@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0CritSecLock@DirectUI@@QEAA@PEAU_RTL_CRITICAL_SECTION@@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0DCSurface@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0DCSurface@DirectUI@@QEAA@PEAUHDC__@@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0DUIFactory@DirectUI@@QEAA@PEAUHWND__@@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0DUIXmlParser@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0DUIXmlParser@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0DialogElement@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0DialogElement@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0DialogElement@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0DuiAccessible@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Edit@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Edit@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Element@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Element@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ElementProvider@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ElementProxy@DirectUI@@IEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ElementProxy@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ElementProxy@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ElementWithHWND@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ElementWithHWND@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ElementWithHWND@DirectUI@@QEAA@XZ	CLEAN

Process Name	Commandline	Verdict
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ExpandCollapseProvider@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ExpandCollapseProxy@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ExpandCollapseProxy@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ExpandCollapseProxy@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Expandable@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Expandable@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Expandable@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Expando@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Expando@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0Expando@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ExpandoButtonGlyph@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0ExpandoButtonGlyph@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0FillLayout@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0FillLayout@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0FlowLayout@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0FlowLayout@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0FontCache@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0FontCache@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0FontCache@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0FontCheckOut@DirectUI@@QEAA@PEAVElement@1@PEAUHDC__@@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0GridItemProvider@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0GridItemProxy@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN

Process Name	Commandline	Verdict
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0GridItemProxy@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0GridItemProxy@DirectUI@@QEAA@XZ	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0GridLayout@DirectUI@@QEAA@AEBV01@@Z	CLEAN
xnczqh.exe	"C:\Users\kEecfMwgj\Desktop\XNczQh.exe" /dll="C:\Users\KEECFM~1\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll" /fn_id=??0GridLayout@DirectUI@@QEAA@XZ	CLEAN

Reduced dataset

YARA / AV

Antivirus (2)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.75562	C:\Users\kEecfMwgj\Desktop\73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da.exe.dll	MALICIOUS
Memory Dump	Trojan.GenericKDZ.75562	-	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