MALICIOUS

Classifications: Spyware

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

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll**
ID	#2782913
MD5	784adf3295b7eafe53aa80da302b1b5d
SHA1	c79da77a4d00ec47594e007f9a174de43b5028d3
SHA256	69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4
File Size	2020.00 KB
Report Created	2021-09-28 14:08 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (9 rules, 137 matches)

Score	Category	Operation	Count	Classification
4/5	Injection	Modifies control flow of another process	2	-
	• (Process #2) pcqblvrnr.exe alters context of (process #9) explorer.exe. • (Process #13) pcqblvrnr.exe alters context of (process #9) explorer.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	7	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #2) pcqblvrnr.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #4) pcqblvrnr.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #24) pcqblvrnr.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #29) pcqblvrnr.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #64) pcqblvrnr.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #71) pcqblvrnr.exe as "Gen:Variant.Mikey.113998".			
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
2/5	Masquerade	Creates a new process from a system binary	1	-
	• (Process #9) explorer.exe creates a new explorer.exe process.			
1/5	Discovery	Reads system data	54	-

- (Process #2) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #3) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #4) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #5) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #6) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #7) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #8) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #10) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #12) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #11) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #13) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #14) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #15) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #19) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #17) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #20) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #18) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #24) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #21) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #22) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #29) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #23) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #30) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #27) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #32) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #31) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #34) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #33) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #35) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #38) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #39) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #46) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #40) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #41) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #44) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #45) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #48) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #47) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #53) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #49) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #50) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #51) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #52) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #54) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #55) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #57) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #56) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #63) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #58) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #61) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #67) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #69) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #70) pcqblvrnr.exe reads the Windows installation date from registry.
- (Process #62) pcqblvrnr.exe reads the Windows installation date from registry.

Score	Category	Operation	Count	Classification
1/5	Mutex	Creates mutex	60	-

• (Process #2) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #4) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #3) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #2) pcqblvrnr.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
• (Process #5) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #6) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #7) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #8) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #10) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #12) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #11) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #13) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #13) pcqblvrnr.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
• (Process #14) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #15) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #19) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #17) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #20) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #18) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #17) pcqblvrnr.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
• (Process #24) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #21) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #22) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #29) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #23) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #30) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #27) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #30) pcqblvrnr.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
• (Process #32) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #34) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #31) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #33) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #33) pcqblvrnr.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
• (Process #35) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #38) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #39) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #46) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #40) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #41) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #44) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #45) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #48) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #47) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #53) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #49) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #50) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #52) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #49) pcqblvrnr.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
• (Process #54) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #55) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #57) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #56) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #63) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #58) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #61) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #67) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #69) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #63) pcqblvrnr.exe creates mutex with name "{6fe2e17b-8d7f-b377-077e-4f2681f673a4}".
• (Process #70) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
• (Process #62) pcqblvrnr.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	6	-

- (Process #2) pcqblvrnr.exe reads from (process #9) explorer.exe.
- (Process #13) pcqblvrnr.exe reads from (process #9) explorer.exe.
- (Process #17) pcqblvrnr.exe reads from (process #9) explorer.exe.
- (Process #30) pcqblvrnr.exe reads from (process #9) explorer.exe.
- (Process #33) pcqblvrnr.exe reads from (process #9) explorer.exe.
- (Process #49) pcqblvrnr.exe reads from (process #9) explorer.exe.

1/5	Crash	A monitored process crashed	5	-

- (Process #9) explorer.exe crashed.
- (Process #13) pcqblvrnr.exe crashed.
- (Process #17) pcqblvrnr.exe crashed.
- (Process #30) pcqblvrnr.exe crashed.
- (Process #33) pcqblvrnr.exe crashed.

1/5	Crash	An unmonitored process crashed	1	-

- Unmonitored process dllhost.exe crashed.

Mitre ATT&CK Matrix

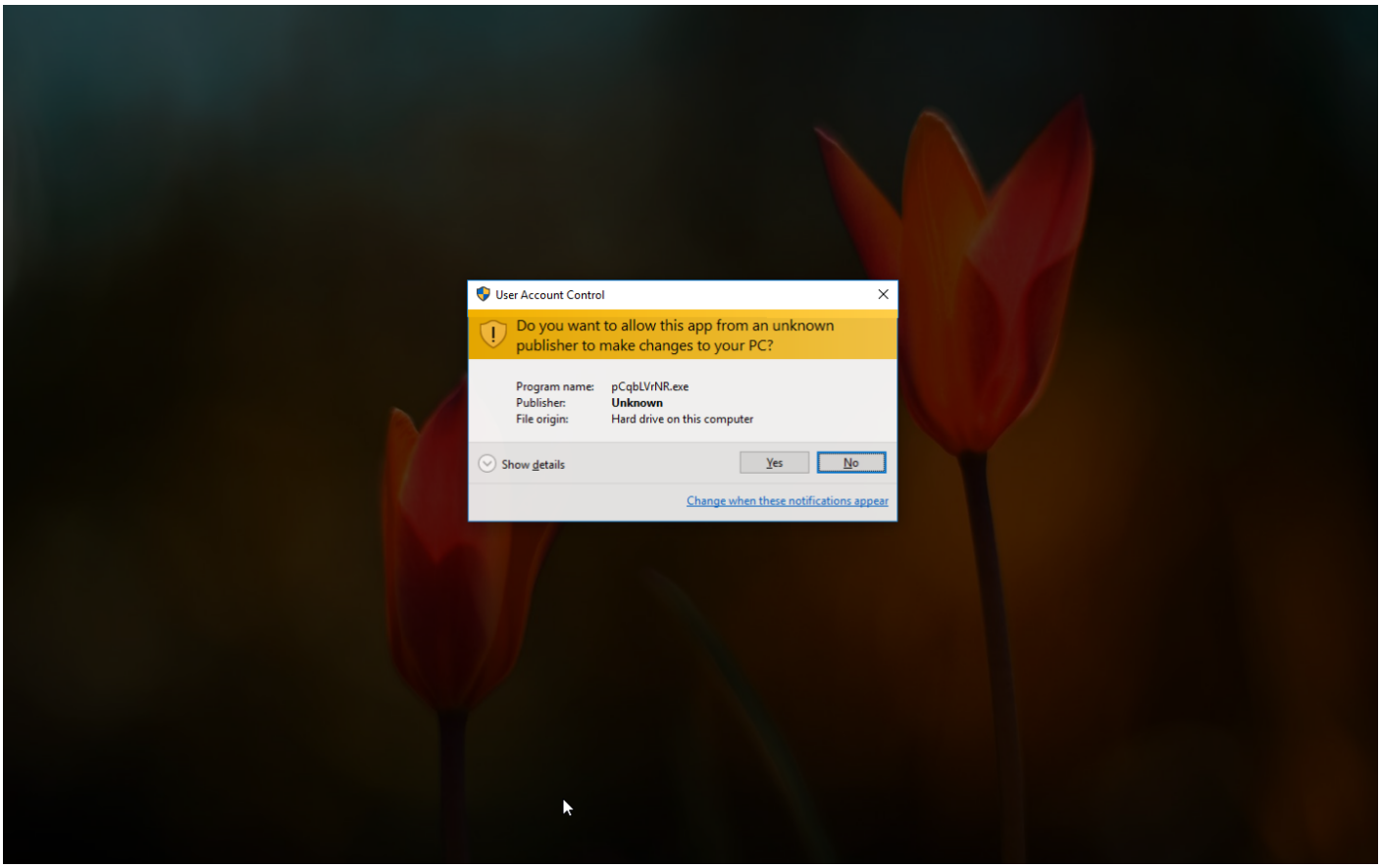
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
						#T1082 System Information Discovery					
						#T1012 Query Registry					

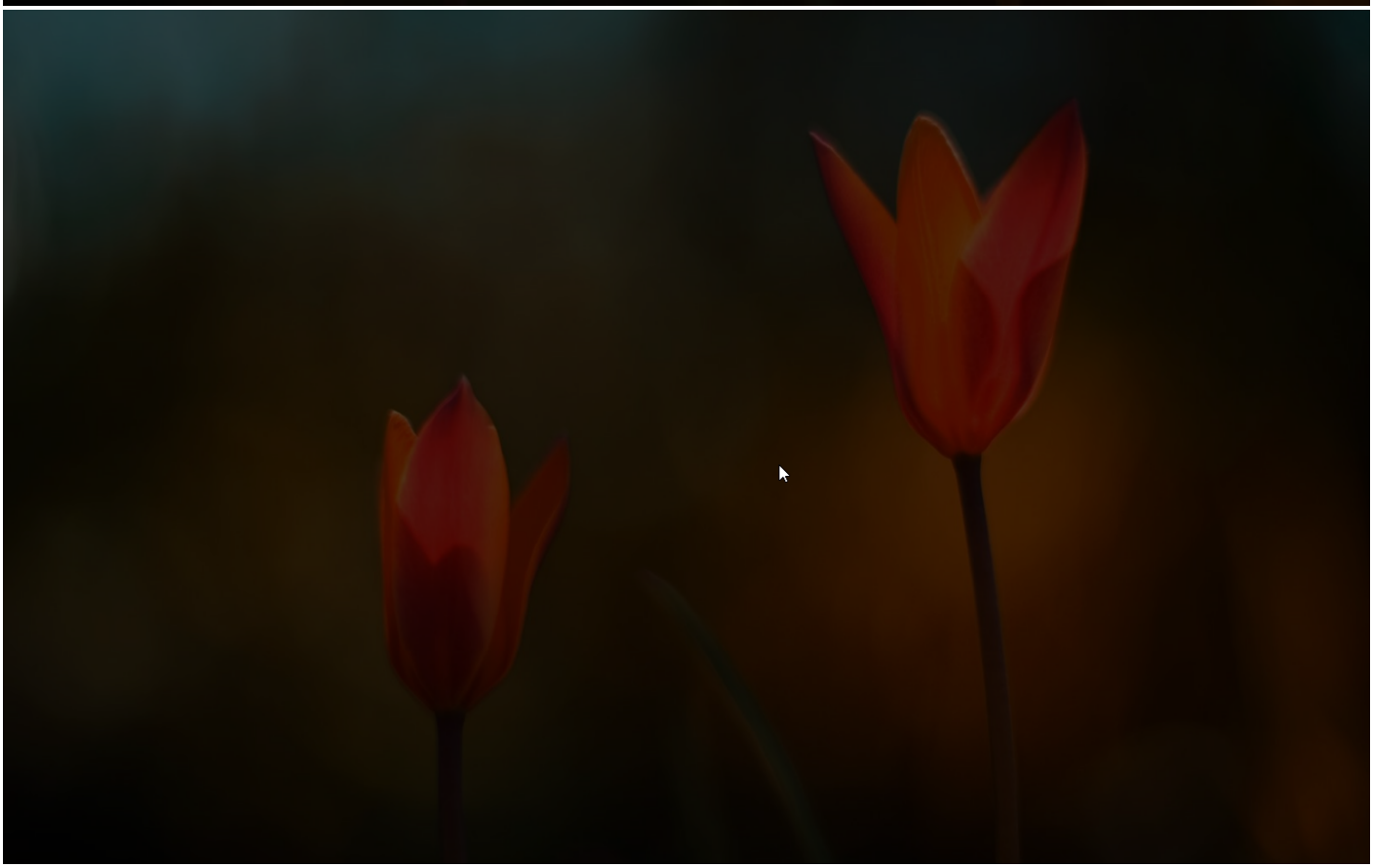
Sample Information

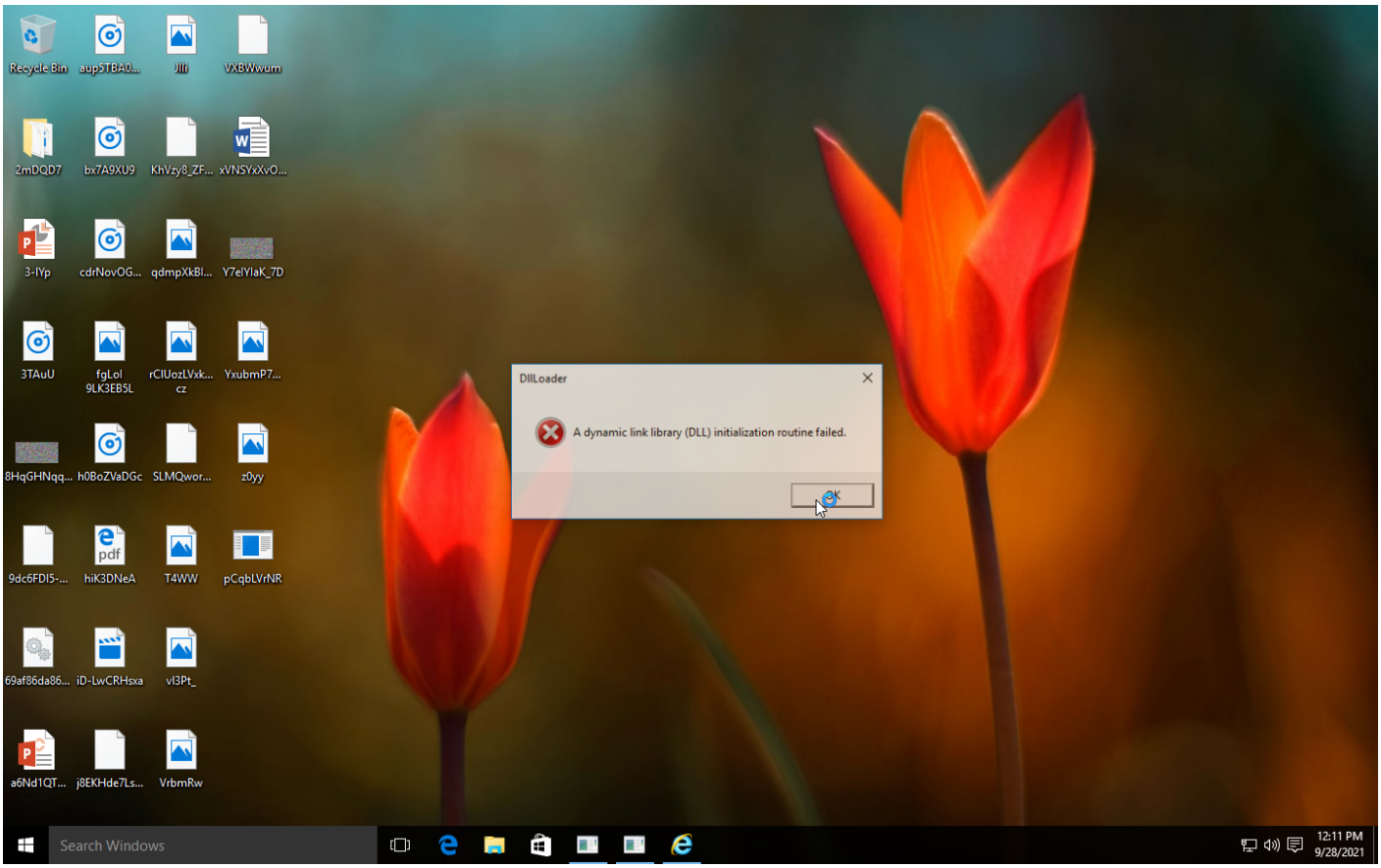
ID	#2782913
MD5	784adf3295b7eafe53aa80da302b1b5d
SHA1	c79da77a4d00ec47594e007f9a174de43b5028d3
SHA256	69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4
SSDeep	12288:YVI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1qxgI:NfP7fWsK5z9A+WGAW+V5SB6Ct4bnbg
ImpHash	6668be91e2c948b183827f040944057f
File Name	69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll
File Size	2020.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

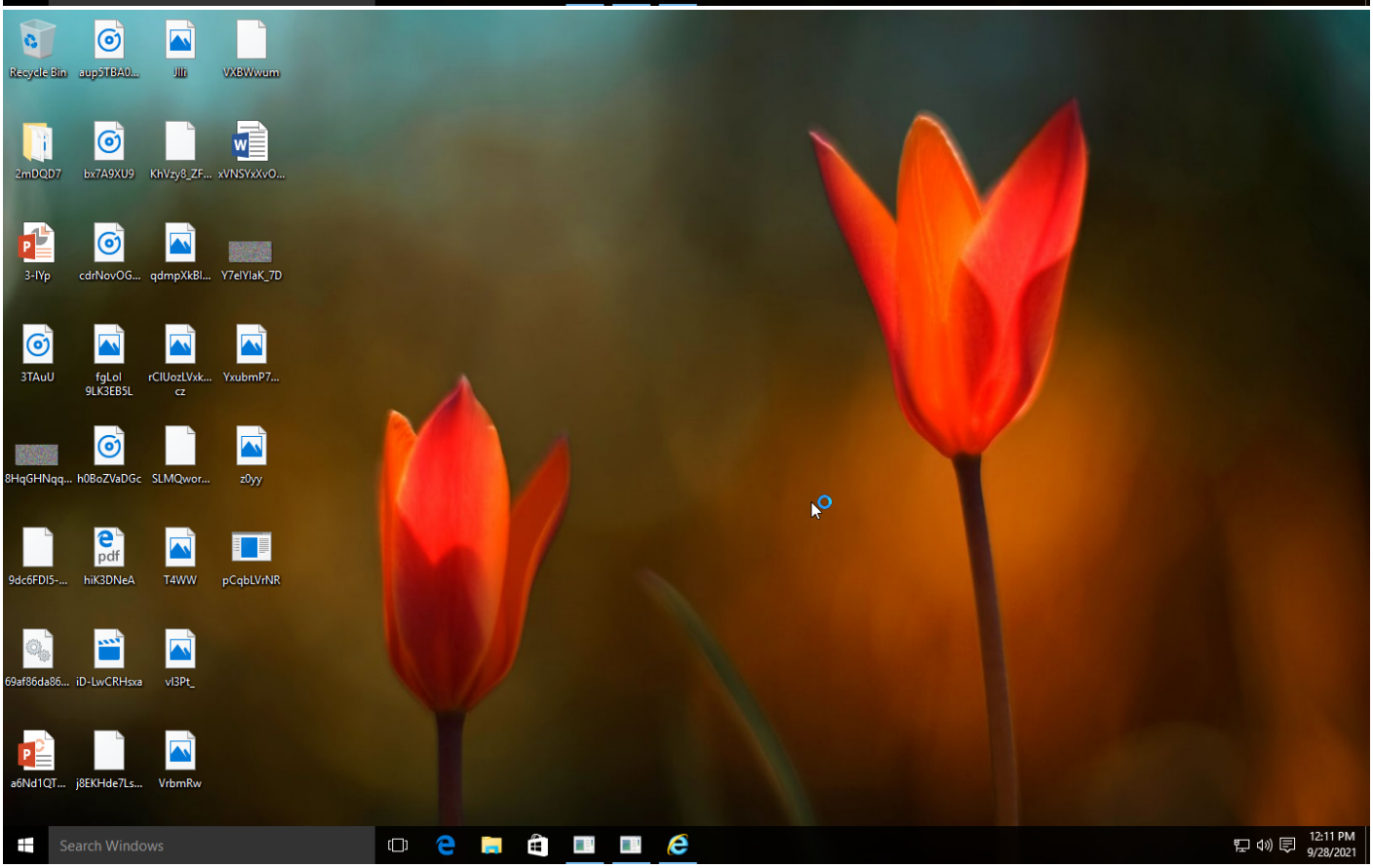
Analysis Information

Creation Time	2021-09-28 14:08 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	76
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	7
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


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







Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

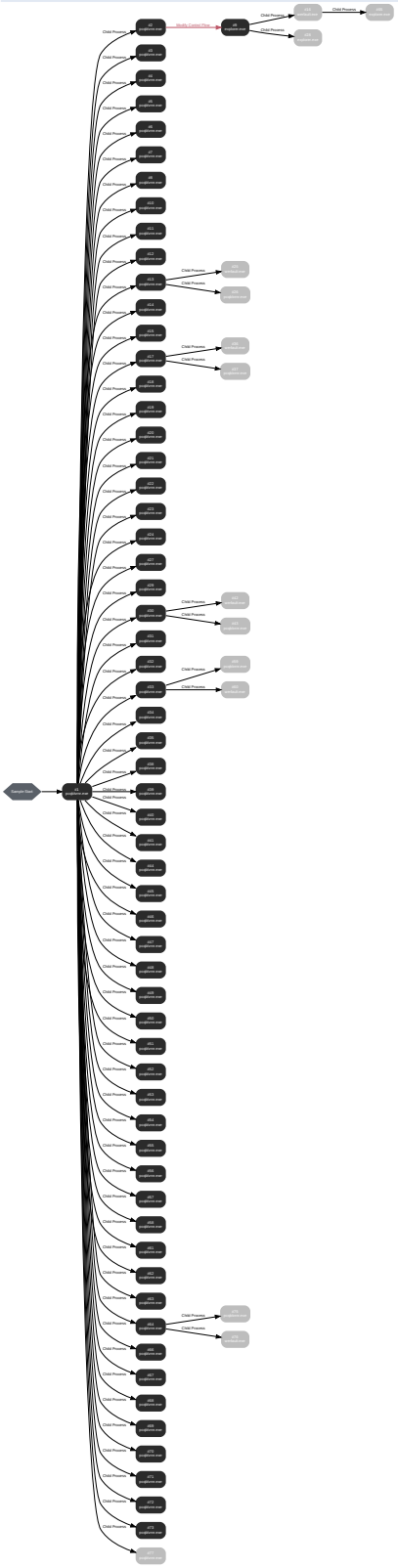
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: pcqblvrnr.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpc61pgs_v" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 76028, Reason: Analysis Target
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	245.67s
Return Code	Unknown
PID	3020
Parent PID	1600
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	7
Environment	1
Process	62

Process #2: pcqblvrnr.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c8... ... 3d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 100042, Reason: Child Process
Unmonitor End Time	End Time: 157654, Reason: Terminated
Monitor duration	57.61s
Return Code	0
PID	1840
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	50
Environment	2
Registry	776
Mutex	6
Process	2
-	100
-	46
-	189

Process #3: pcqblvrnr.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 101938, Reason: Child Process
Unmonitor End Time	End Time: 121161, Reason: Terminated
Monitor duration	19.22s
Return Code	0
PID	1792
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #4: pcqblvrnr.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 103506, Reason: Child Process
Unmonitor End Time	End Time: 120315, Reason: Terminated
Monitor duration	16.81s
Return Code	0
PID	3216
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	768
Mutex	7

Process #5: pcqblvrnr.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $PatternProvider@VInvokeProvider@DirectUI@@UIInvokeProvider@@$0A@@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 106633, Reason: Child Process
Unmonitor End Time	End Time: 129511, Reason: Terminated
Monitor duration	22.88s
Return Code	0
PID	1164
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #6: pcqblvrnr.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $PatternProvider@VRangeValueProvider@DirectUI@@UIRangeValueProvider@@$03@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 112173, Reason: Child Process
Unmonitor End Time	End Time: 135662, Reason: Terminated
Monitor duration	23.49s
Return Code	0
PID	3568
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #7: pcqblvrnr.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $PatternProvider@VScrollItemProvider@DirectUI@@UIScrollItemProvider@@$05@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 117863, Reason: Child Process
Unmonitor End Time	End Time: 143965, Reason: Terminated
Monitor duration	26.10s
Return Code	0
PID	2476
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #8: pcqblvrnr.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $PatternProvider@VScrollProvider@DirectUI@@UIScrollProvider@@$04@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 123268, Reason: Child Process
Unmonitor End Time	End Time: 146678, Reason: Terminated
Monitor duration	23.41s
Return Code	0
PID	4076
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	4
Environment	2
Registry	766
Mutex	7

Process #9: explorer.exe

ID	9
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 127126, Reason: Injection
Unmonitor End Time	End Time: 311646, Reason: Crashed
Monitor duration	184.52s
Return Code	255
PID	1600
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (150)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x644	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x684	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6b8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6c8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6d0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6f0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x710	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x728	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x73c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x75c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x764	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x768	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x774	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x7a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x7b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x7bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xa9c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xb94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xbf8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xbfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x8b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x5d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x8bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x928	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xe14	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xe7c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xc20	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xa94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xb14	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x560	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xc98	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xd04	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xcbc	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xbc4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x12a0	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x12bc	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x12c0	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x12cc	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x12d4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x135c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x139c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x564	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb28bab580(140716696843648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x644	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x684	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6b8	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6c8	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6d0	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6d4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x6f0	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x710	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x728	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x73c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x75c	0x7ffb28ba4f00(140716696817408)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x764	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x768	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x774	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x7a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x7b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x7bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xa9c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xb94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xbf8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xbfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x8b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x5d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x8bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x928	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xe14	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xe7c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xc20	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xa94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xb14	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x560	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xc98	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xd04	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xcbc	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0xbc4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x12a0	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x12bc	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x12c0	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x12cc	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x12d4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x135c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x139c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x564	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x688	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb28bab580(140716696843648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x760 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#13: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x13cc / 0x644	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#13: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x13cc / 0x684	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#13: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x13cc / 0x688	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#13: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x13cc / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#13: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x13cc / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#13: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x13cc / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#13: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x13cc / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#13: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x13cc / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#13: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x13cc / 0x6b8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#13: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x13cc / 0x6c8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#13: c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe	0x13cc / 0x6d0	0x7ffb28ba4f00(140716696817408)	-	✓	1

Host Behavior

Type	Count
Module	2

Process #10: pcqblvrnr.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $PatternProvider@VSelectionItemProvider@DirectUI@@UISelectionItemProvider@@$06@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 130149, Reason: Child Process
Unmonitor End Time	End Time: 150287, Reason: Terminated
Monitor duration	20.14s
Return Code	0
PID	5036
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	784
Mutex	7

Process #11: pcqblvrnr.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $PatternProvider@VSelectionProvider@DirectUI@@UISelectionProvider@@$07@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 134172, Reason: Child Process
Unmonitor End Time	End Time: 151388, Reason: Terminated
Monitor duration	17.22s
Return Code	0
PID	3924
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	768
Mutex	7

Process #12: pcqblvrnr.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $PatternProvider@VTableItemProvider@DirectUI@@UITableItemProvider@@$09@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 138893, Reason: Child Process
Unmonitor End Time	End Time: 151376, Reason: Terminated
Monitor duration	12.48s
Return Code	0
PID	3684
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #13: pcqblvrnr.exe

ID	13
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $PatternProvider@VTableProvider@DirectUI@@UITableProvider@@$08@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 145041, Reason: Child Process
Unmonitor End Time	End Time: 220666, Reason: Crashed
Monitor duration	75.62s
Return Code	1114
PID	3396
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	43
File	118
System	8
Environment	2
Registry	788
Mutex	6
Process	2
-	52
-	1
-	100
Window	1

Process #14: pcqblvrnr.exe

ID	14
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $PatternProvider@VToggleProvider@DirectUI@@UIToggleProvider@@$0L@@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 149339, Reason: Child Process
Unmonitor End Time	End Time: 178185, Reason: Terminated
Monitor duration	28.85s
Return Code	0
PID	5056
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #15: pcqblvrnr.exe

ID	15
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $PatternProvider@VValueProvider@DirectUI@@UIValueProvider@@$0M@@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 151495, Reason: Child Process
Unmonitor End Time	End Time: 185062, Reason: Terminated
Monitor duration	33.57s
Return Code	0
PID	3128
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	7
Environment	2
Registry	786
Mutex	7

Process #16: werfault.exe

ID	16
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 1600 -s 4368
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 156009, Reason: Child Process
Unmonitor End Time	End Time: 300424, Reason: Terminated
Monitor duration	144.41s
Return Code	0
PID	1644
Parent PID	1600
Bitness	64 Bit

Process #17: pcqblvrnr.exe

ID	17
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $SafeArrayAccessor@H@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 156049, Reason: Child Process
Unmonitor End Time	End Time: 243972, Reason: Crashed
Monitor duration	87.92s
Return Code	1114
PID	3800
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	43
File	118
System	8
Environment	2
Registry	786
Mutex	6
Process	2
-	52
-	1
-	100
Window	1

Process #18: pcqblvrnr.exe

ID	18
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0AccessibleButton@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 162778, Reason: Child Process
Unmonitor End Time	End Time: 200244, Reason: Terminated
Monitor duration	37.47s
Return Code	0
PID	4844
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #19: pcqblvrnr.exe

ID	19
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0AccessibleButton@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 165409, Reason: Child Process
Unmonitor End Time	End Time: 185919, Reason: Terminated
Monitor duration	20.51s
Return Code	0
PID	2816
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #20: pcqblvrnr.exe

ID	20
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0AccessibleButton@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 168051, Reason: Child Process
Unmonitor End Time	End Time: 193234, Reason: Terminated
Monitor duration	25.18s
Return Code	0
PID	4904
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #21: pcqblvrnr.exe

ID	21
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0AnimationStrip@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 170867, Reason: Child Process
Unmonitor End Time	End Time: 210929, Reason: Terminated
Monitor duration	40.06s
Return Code	0
PID	4892
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #22: pcqblvrnr.exe

ID	22
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0AnimationStrip@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 174720, Reason: Child Process
Unmonitor End Time	End Time: 215170, Reason: Terminated
Monitor duration	40.45s
Return Code	0
PID	4772
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #23: pcqblvrnr.exe

ID	23
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 178174, Reason: Child Process
Unmonitor End Time	End Time: 217259, Reason: Terminated
Monitor duration	39.09s
Return Code	0
PID	1472
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #24: pcqblvrnr.exe

ID	24
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0AutoButton@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 181975, Reason: Child Process
Unmonitor End Time	End Time: 207160, Reason: Terminated
Monitor duration	25.18s
Return Code	0
PID	2656
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #25: werfault.exe

ID	25
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 3396 -s 668
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 185343, Reason: Child Process
Unmonitor End Time	End Time: 215286, Reason: Terminated
Monitor duration	29.94s
Return Code	0
PID	4140
Parent PID	3396
Bitness	64 Bit

Process #26: pcqblvrnr.exe

ID	26
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $PatternProvider@VTableProvider@DirectUI@@UITableProvider@@$08@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 185776, Reason: Child Process
Unmonitor End Time	End Time: 215885, Reason: Terminated
Monitor duration	30.11s
Return Code	259
PID	4116
Parent PID	3396
Bitness	64 Bit

Process #27: pcqblvrnr.exe

ID	27
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 186635, Reason: Child Process
Unmonitor End Time	End Time: 223175, Reason: Terminated
Monitor duration	36.54s
Return Code	0
PID	4180
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #28: explorer.exe

ID	28
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 190838, Reason: Child Process
Unmonitor End Time	End Time: 298941, Reason: Terminated
Monitor duration	108.10s
Return Code	259
PID	4240
Parent PID	1600
Bitness	64 Bit

Process #29: pcqblvrnr.exe

ID	29
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0AutoLock@DirectUI@@QEAA@PEAU_RTL_CRITICAL_SECTION@@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 191782, Reason: Child Process
Unmonitor End Time	End Time: 217274, Reason: Terminated
Monitor duration	25.49s
Return Code	0
PID	4264
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #30: pcqblvrnr.exe

ID	30
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AutoThread@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 198526, Reason: Child Process
Unmonitor End Time	End Time: 274950, Reason: Crashed
Monitor duration	76.42s
Return Code	1114
PID	4364
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	43
File	118
System	8
Environment	2
Registry	786
Mutex	6
Process	2
-	52
-	1
-	100
Window	1

Process #31: pcqblvrnr.exe

ID	31
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AutoVariant@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 203996, Reason: Child Process
Unmonitor End Time	End Time: 231640, Reason: Terminated
Monitor duration	27.64s
Return Code	0
PID	4548
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #32: pcqblvrnr.exe

ID	32
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0BaseScrollBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 208494, Reason: Child Process
Unmonitor End Time	End Time: 227426, Reason: Terminated
Monitor duration	18.93s
Return Code	0
PID	4612
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #33: pcqblvrnr.exe

ID	33
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0BaseScrollBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 213636, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Crashed
Monitor duration	108.06s
Return Code	Unknown
PID	4740
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	43
File	118
System	8
Environment	2
Registry	786
Mutex	6
Process	2
-	52
-	1
-	100
Window	1

Process #34: pcqblvrnr.exe

ID	34
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0BaseScrollBar@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 216711, Reason: Child Process
Unmonitor End Time	End Time: 232013, Reason: Terminated
Monitor duration	15.30s
Return Code	0
PID	4756
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #35: pcqblvrnr.exe

ID	35
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0BaseScrollViewer@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 220433, Reason: Child Process
Unmonitor End Time	End Time: 253094, Reason: Terminated
Monitor duration	32.66s
Return Code	0
PID	3772
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	7
Environment	2
Registry	786
Mutex	7

Process #36: werfault.exe

ID	36
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 3800 -s 668
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 220497, Reason: Child Process
Unmonitor End Time	End Time: 237675, Reason: Terminated
Monitor duration	17.18s
Return Code	0
PID	3928
Parent PID	3800
Bitness	64 Bit

Process #37: pcqblvrnr.exe

ID	37
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0? $SafeArrayAccessor@H@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 220858, Reason: Child Process
Unmonitor End Time	End Time: 238726, Reason: Terminated
Monitor duration	17.87s
Return Code	259
PID	3468
Parent PID	3800
Bitness	64 Bit

Process #38: pcqblvrnr.exe

ID	38
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0BaseScrollViewer@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 225333, Reason: Child Process
Unmonitor End Time	End Time: 257718, Reason: Terminated
Monitor duration	32.38s
Return Code	0
PID	2424
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #39: pcqblvrnr.exe

ID	39
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 228549, Reason: Child Process
Unmonitor End Time	End Time: 266288, Reason: Terminated
Monitor duration	37.74s
Return Code	0
PID	1812
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #40: pcqblvrnr.exe

ID	40
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0Bind@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 232209, Reason: Child Process
Unmonitor End Time	End Time: 270935, Reason: Terminated
Monitor duration	38.73s
Return Code	0
PID	3876
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #41: pcqblvrnr.exe

ID	41
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 234824, Reason: Child Process
Unmonitor End Time	End Time: 275563, Reason: Terminated
Monitor duration	40.74s
Return Code	0
PID	3580
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #42: werfault.exe

ID	42
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 4364 -s 668
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 236620, Reason: Child Process
Unmonitor End Time	End Time: 265032, Reason: Terminated
Monitor duration	28.41s
Return Code	0
PID	5000
Parent PID	4364
Bitness	64 Bit

Process #43: pcqblvrnr.exe

ID	43
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AutoThread@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 237215, Reason: Child Process
Unmonitor End Time	End Time: 267503, Reason: Terminated
Monitor duration	30.29s
Return Code	259
PID	2220
Parent PID	4364
Bitness	64 Bit

Process #44: pcqblvrnr.exe

ID	44
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0BorderLayout@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 237216, Reason: Child Process
Unmonitor End Time	End Time: 276848, Reason: Terminated
Monitor duration	39.63s
Return Code	0
PID	2652
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #45: pcqblvrnr.exe

ID	45
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0BorderLayout@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 238904, Reason: Child Process
Unmonitor End Time	End Time: 280123, Reason: Terminated
Monitor duration	41.22s
Return Code	0
PID	3092
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #46: pcqblvrnr.exe

ID	46
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 239513, Reason: Child Process
Unmonitor End Time	End Time: 270942, Reason: Terminated
Monitor duration	31.43s
Return Code	0
PID	3480
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	7
Environment	2
Registry	786
Mutex	7

Process #47: pcqblvrnr.exe

ID	47
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0Browser@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 241831, Reason: Child Process
Unmonitor End Time	End Time: 286071, Reason: Terminated
Monitor duration	44.24s
Return Code	0
PID	2580
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #48: pcqblvrnr.exe

ID	48
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 242534, Reason: Child Process
Unmonitor End Time	End Time: 284724, Reason: Terminated
Monitor duration	42.19s
Return Code	0
PID	2932
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #49: pcqblvrnr.exe

ID	49
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0BrowserSelectionProxy@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 246962, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	74.73s
Return Code	Unknown
PID	4076
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	7
Environment	2
Registry	786
Mutex	5
Process	2
-	2
-	1

Process #50: pcqblvrnr.exe

ID	50
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0BrowserSelectionProxy@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 251744, Reason: Child Process
Unmonitor End Time	End Time: 293096, Reason: Terminated
Monitor duration	41.35s
Return Code	0
PID	3416
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	7
Environment	2
Registry	786
Mutex	7

Process #51: pcqblvrnr.exe

ID	51
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0BrowserSelectionProxy@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 256037, Reason: Child Process
Unmonitor End Time	End Time: 293308, Reason: Terminated
Monitor duration	37.27s
Return Code	0
PID	5036
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	8

Process #52: pcqblvrnr.exe

ID	52
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0Button@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 257388, Reason: Child Process
Unmonitor End Time	End Time: 293308, Reason: Terminated
Monitor duration	35.92s
Return Code	0
PID	2148
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #53: pcqblvrnr.exe

ID	53
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0Button@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 258112, Reason: Child Process
Unmonitor End Time	End Time: 287016, Reason: Terminated
Monitor duration	28.90s
Return Code	0
PID	1000
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #54: pcqblvrnr.exe

ID	54
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 258885, Reason: Child Process
Unmonitor End Time	End Time: 294852, Reason: Terminated
Monitor duration	35.97s
Return Code	0
PID	3016
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #55: pcqblvrnr.exe

ID	55
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCAVI@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 268227, Reason: Child Process
Unmonitor End Time	End Time: 302528, Reason: Terminated
Monitor duration	34.30s
Return Code	0
PID	1824
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #56: pcqblvrnr.exe

ID	56
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 274606, Reason: Child Process
Unmonitor End Time	End Time: 308506, Reason: Terminated
Monitor duration	33.90s
Return Code	0
PID	1888
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	7
Environment	2
Registry	786
Mutex	7

Process #57: pcqblvrnr.exe

ID	57
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCBase@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 282049, Reason: Child Process
Unmonitor End Time	End Time: 303549, Reason: Terminated
Monitor duration	21.50s
Return Code	0
PID	1144
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #58: pcqblvrnr.exe

ID	58
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCBase@DirectUI@@QEAA@KPEBG@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 286560, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	35.14s
Return Code	Unknown
PID	3840
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	705
Mutex	3

Process #59: pcqblvrnr.exe

ID	59
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0BaseScrollBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 286779, Reason: Child Process
Unmonitor End Time	End Time: 312330, Reason: Terminated
Monitor duration	25.55s
Return Code	259
PID	1244
Parent PID	4740
Bitness	64 Bit

Process #60: werfault.exe

ID	60
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 4740 -s 668
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 286926, Reason: Child Process
Unmonitor End Time	End Time: 311629, Reason: Terminated
Monitor duration	24.70s
Return Code	0
PID	3544
Parent PID	4740
Bitness	64 Bit

Process #61: pcqblvrnr.exe

ID	61
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCBaseCheckRadioButton@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 288557, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	33.14s
Return Code	Unknown
PID	2500
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	5
Environment	2
Registry	560
Mutex	3

Process #62: pcqblvrnr.exe

ID	62
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCBaseCheckRadioButton@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 291491, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	30.20s
Return Code	Unknown
PID	1312
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	1
Environment	2
Registry	226
Mutex	3

Process #63: pcqblvrnr.exe

ID	63
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCBaseCheckRadioButton@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 292654, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	29.04s
Return Code	Unknown
PID	5044
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	31
File	117
System	6
Environment	2
Registry	786
Mutex	5
Process	1
-	1

Process #64: pcqblvrnr.exe

ID	64
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCBaseScrollBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 295570, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	26.13s
Return Code	Unknown
PID	4008
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #65: explorer.exe

ID	65
File Name	c:\windows\explorer.exe
Command Line	"C:\Windows\Explorer.EXE" /LOADSAVEDWINDOWS
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 295726, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	25.97s
Return Code	Unknown
PID	4776
Parent PID	1644
Bitness	64 Bit

Process #66: pcqblvrnr.exe

ID	66
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCBaseScrollBar@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 298057, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	23.64s
Return Code	Unknown
PID	4204
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #67: pcqblvrnr.exe

ID	67
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCBaseScrollBar@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 299437, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	22.26s
Return Code	Unknown
PID	4288
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	5
Environment	2
Registry	560
Mutex	3

Process #68: pcqblvrnr.exe

ID	68
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCCheckBox@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 300426, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	21.27s
Return Code	Unknown
PID	3680
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #69: pcqblvrnr.exe

ID	69
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCCheckBox@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 301441, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	20.25s
Return Code	Unknown
PID	4060
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	2
Environment	2
Registry	281
Mutex	3

Process #70: pcqblvrnr.exe

ID	70
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCCheckBox@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 302644, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	19.05s
Return Code	Unknown
PID	4480
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	2
Environment	2
Registry	248
Mutex	3

Process #71: pcqblvrnr.exe

ID	71
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCCommandLink@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 305105, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	16.59s
Return Code	Unknown
PID	4896
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #72: pcqblvrnr.exe

ID	72
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCCommandLink@DirectUI@@QEAA@AEBV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 310242, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	11.45s
Return Code	Unknown
PID	4660
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	3
Environment	1

Process #73: pcqblvrnr.exe

ID	73
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCCommandLink@DirectUI@@QEAA@K@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 313428, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	8.27s
Return Code	Unknown
PID	3044
Parent PID	3020
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #75: pcqblvrnr.exe

ID	75
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCBaseScrollBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 319014, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	2.68s
Return Code	Unknown
PID	760
Parent PID	4008
Bitness	64 Bit

Process #76: werfault.exe

ID	76
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 4008 -s 360
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319628, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	2.07s
Return Code	Unknown
PID	2972
Parent PID	4008
Bitness	64 Bit

Process #77: pcqblvrnr.exe

ID	77
File Name	c:\users\rdhj0cnfevzx\desktop\pcqblvrnr.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C: \Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=?? 0CCHScrollBar@DirectUI@@QEAA@$$QEAV01@@Z
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 320744, Reason: Child Process
Unmonitor End Time	End Time: 321696, Reason: Terminated by Timeout
Monitor duration	0.95s
Return Code	Unknown
PID	1920
Parent PID	3020
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4	C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll, C:\Users\RDhJ0CNFevzX\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll	Sample File	2020.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpc61pgs_v	Accessed File	Access, Read	CLEAN
C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll	Accessed File	Access, Read	CLEAN
System Paging File	Accessed File	Access	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{0aa26147-58aa-e888-6782-4bac88c336bd}	access	pcqblvrnr.exe	CLEAN
{54137ce8-d76d-e7fc-dec3-c85f290e5b98}	access	pcqblvrnr.exe	CLEAN
{6fe2e17b-8d7f-b377-077e-4f2681f673a4}	access	pcqblvrnr.exe	CLEAN

Registry

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

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\EnableLUA	access, read	pcqblvrnr.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ConsentPromptBehaviorAdmin	access, read	pcqblvrnr.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\PromptOnSecureDesktop	access, read	pcqblvrnr.exe	CLEAN

Process

Process Name	Commandline	Verdict
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpc61pgs_v" /s	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c8... ...3d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VInvokeProvider@DirectUI@@UIInvokeProvider@@$0A@@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VRangeValueProvider@DirectUI@@UIRangeValueProvider@@$03@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VScrollItemProvider@DirectUI@@UIScrollItemProvider@@$05@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VScrollProvider@DirectUI@@UIScrollProvider@@$04@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VSelectionItemProvider@DirectUI@@UISelectionItemProvider@@$06@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VSelectionProvider@DirectUI@@UISelectionProvider@@$07@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VTableItemProvider@DirectUI@@UITableItemProvider@@$09@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VTableProvider@DirectUI@@UITableProvider@@$08@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VToggleProvider@DirectUI@@UIToggleProvider@@$0L@@DirectUI@@QEAA@XZ	CLEAN

Process Name	Commandline	Verdict
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0?$PatternProvider@VValueProvider@DirectUI@@UIValueProvider@@$0M@@DirectUI@@QEAA@XZ	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 1600 -s 4368	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0?$SafeArrayAccessor@H@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AccessibleButton@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AccessibleButton@DirectUI@@QEAA@AEBV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AccessibleButton@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AnimationStrip@DirectUI@@QEAA@AEBV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AnimationStrip@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@AEBV01@@Z	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 3396 -s 668	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AutoButton@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AutoLock@DirectUI@@QEAA@PEAU_RTL_CRITICAL_SECTION@@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AutoThread@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0AutoVariant@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0BaseScrollBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0BaseScrollBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0BaseScrollBar@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0BaseScrollViewer@DirectUI@@QEAA@AEBV01@@Z	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 3800 -s 668	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0BaseScrollViewer@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@AEBV01@@Z	CLEAN

Process Name	Commandline	Verdict
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0Bind@DirectUI@@QEAA@XZ	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 4364 -s 668	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0BorderLayout@DirectUI@@QEAA@AEBV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0BorderLayout@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@AEBV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0Browser@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0BrowserSelectionProxy@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0BrowserSelectionProxy@DirectUI@@QEAA@AEBV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0BrowserSelectionProxy@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0Button@DirectUI@@QEAA@AEBV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0Button@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@AEBV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCAVI@DirectUI@@QEAA@XZ	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCBase@DirectUI@@QEAA@AEBV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCBase@DirectUI@@QEAA@KPEBG@Z	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 4740 -s 668	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCBaseCheckRadioButton@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCBaseCheckRadioButton@DirectUI@@QEAA@AEBV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCBaseCheckRadioButton@DirectUI@@QEAA@K@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCBaseScrollBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
explorer.exe	"C:\Windows\Explorer.EXE" /LOADSAVEDWINDOWS	CLEAN

Process Name	Commandline	Verdict
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCBaseScrollBar@DirectUI@@QEAA@AEBV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCBaseScrollBar@DirectUI@@QEAA@K@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCCheckBox@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCCheckBox@DirectUI@@QEAA@AEBV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCCheckBox@DirectUI@@QEAA@K@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCCommandLink@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCCommandLink@DirectUI@@QEAA@AEBV01@@Z	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCCommandLink@DirectUI@@QEAA@K@Z	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 4008 -s 360	CLEAN
pcqblvrnr.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pCqbLVrNR.exe" /dll="C:\Users\RDHJ0C~1\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll" /fn_id=??0CCHScrollBar@DirectUI@@QEAA@$$QEAV01@@Z	CLEAN

YARA / AV

Antivirus (7)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\Desktop\69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4.exe.dll	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
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	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB

User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows