MALICIOUS

Classifications: Spyware

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

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll**
ID	#2782710
MD5	5edd6ba336c4de29f55cadfd2167a67e
SHA1	af181a8f3fe25a515a8fe2a02559e5daceecf976
SHA256	eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d
File Size	2116.00 KB
Report Created	2021-09-28 13:02 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (8 rules, 111 matches)

Score	Category	Operation	Count	Classification
4/5	Antivirus	Malicious content was detected by heuristic scan	6	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #3) gcgcuoqb.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #22) gcgcuoqb.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #27) gcgcuoqb.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #56) gcgcuoqb.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #23) explorer.exe as "Trojan.GenericKDZ.76753".			
4/5	Injection	Modifies control flow of another process	12	-
	• (Process #2) gcgcuoqb.exe alters context of (process #23) explorer.exe. • (Process #20) gcgcuoqb.exe alters context of (process #23) explorer.exe. • (Process #28) gcgcuoqb.exe alters context of (process #23) explorer.exe. • (Process #2) gcgcuoqb.exe alters context of (process #24) active-charge.exe. • (Process #20) gcgcuoqb.exe alters context of (process #24) active-charge.exe. • (Process #28) gcgcuoqb.exe alters context of (process #24) active-charge.exe. • (Process #38) gcgcuoqb.exe alters context of (process #24) active-charge.exe. • (Process #2) gcgcuoqb.exe alters context of (process #25) yahoomessenger.exe. • (Process #2) gcgcuoqb.exe alters context of (process #26) omnipos.exe. • (Process #20) gcgcuoqb.exe alters context of (process #26) omnipos.exe. • (Process #28) gcgcuoqb.exe alters context of (process #26) omnipos.exe. • (Process #38) gcgcuoqb.exe alters context of (process #26) omnipos.exe.			
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 #23) explorer.exe creates a new explorer.exe process.			
1/5	Discovery	Reads system data	40	-

Score	Category	Operation	Count	Classification
		• (Process #2) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #3) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #4) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #5) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #6) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #7) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #8) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #9) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #10) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #11) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #12) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #13) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #14) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #15) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #16) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #17) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #18) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #19) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #20) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #21) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #22) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #27) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #28) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #30) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #31) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #32) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #36) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #35) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #34) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #33) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #37) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #38) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #46) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #39) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #43) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #45) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #44) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #47) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #48) gcgcuoqb.exe reads the Windows installation date from registry. • (Process #50) gcgcuoqb.exe reads the Windows installation date from registry.		
1/5	Mutex	Creates mutex	42	-

Score	Category	Operation	Count	Classification
		• (Process #2) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #3) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #4) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #5) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #2) gcgcuoqb.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}". • (Process #6) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #7) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #8) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #9) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #10) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #11) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #12) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #13) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #14) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #15) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #16) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #17) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #18) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #19) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #20) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #21) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #20) gcgcuoqb.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}". • (Process #22) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #27) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #28) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #30) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #28) gcgcuoqb.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}". • (Process #31) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #32) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #36) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #35) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #37) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #38) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #46) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #39) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #43) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #38) gcgcuoqb.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}". • (Process #44) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #47) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #48) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #47) gcgcuoqb.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}". • (Process #50) gcgcuoqb.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".		
1/5	Obfuscation	Reads from memory of another process	5	-
		• (Process #2) gcgcuoqb.exe reads from (process #23) explorer.exe. • (Process #20) gcgcuoqb.exe reads from (process #23) explorer.exe. • (Process #28) gcgcuoqb.exe reads from (process #23) explorer.exe. • (Process #38) gcgcuoqb.exe reads from (process #23) explorer.exe. • (Process #47) gcgcuoqb.exe reads from (process #23) explorer.exe.		
1/5	Crash	A monitored process crashed	4	-

Score	Category	Operation	Count	Classification
		• (Process #23) explorer.exe crashed. • (Process #20) gcgcuoqb.exe crashed. • (Process #28) gcgcuoqb.exe crashed. • (Process #38) gcgcuoqb.exe crashed.		

Mitre ATT&CK Matrix

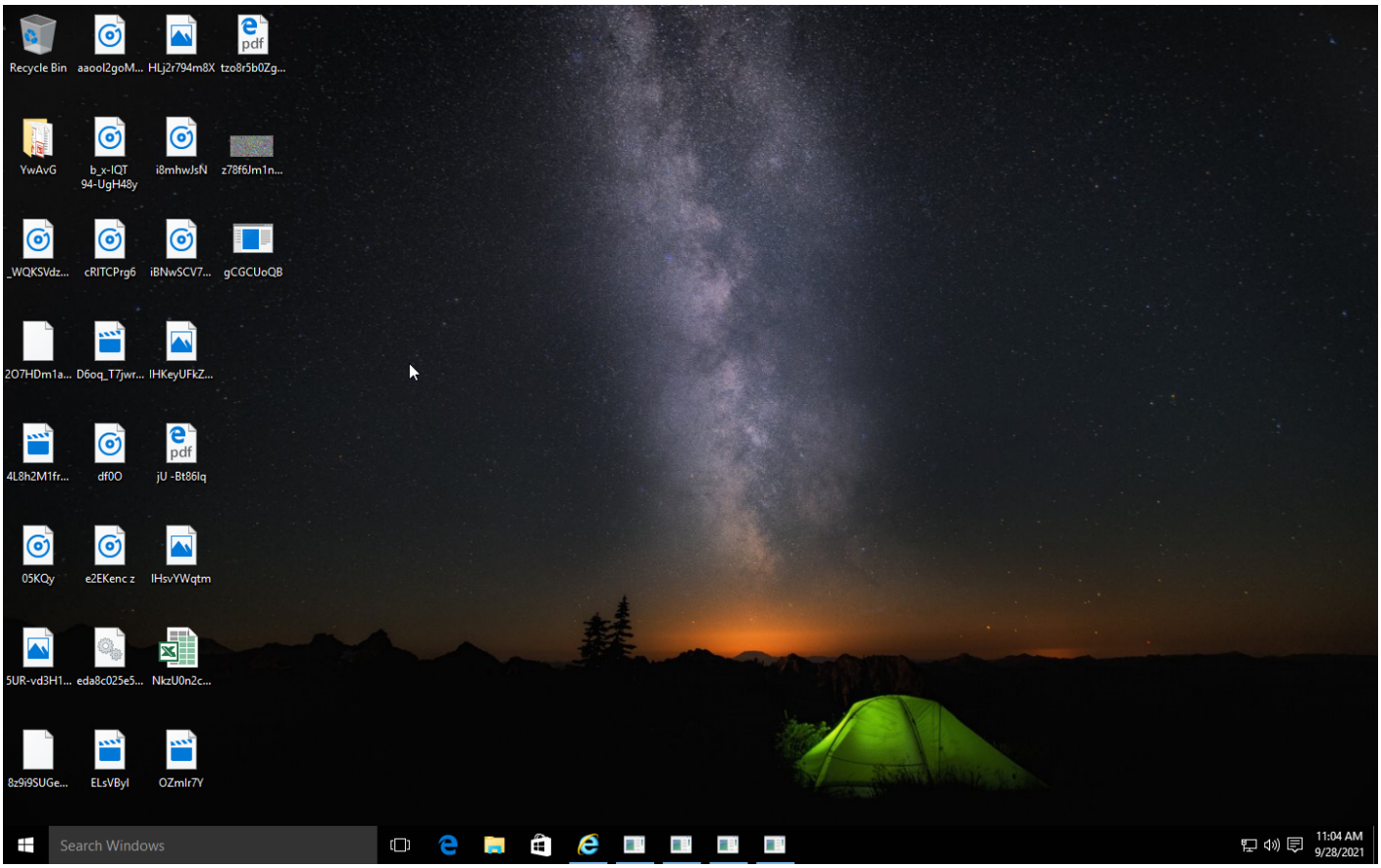
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
						#T1082 System Information Discovery					
						#T1012 Query Registry					

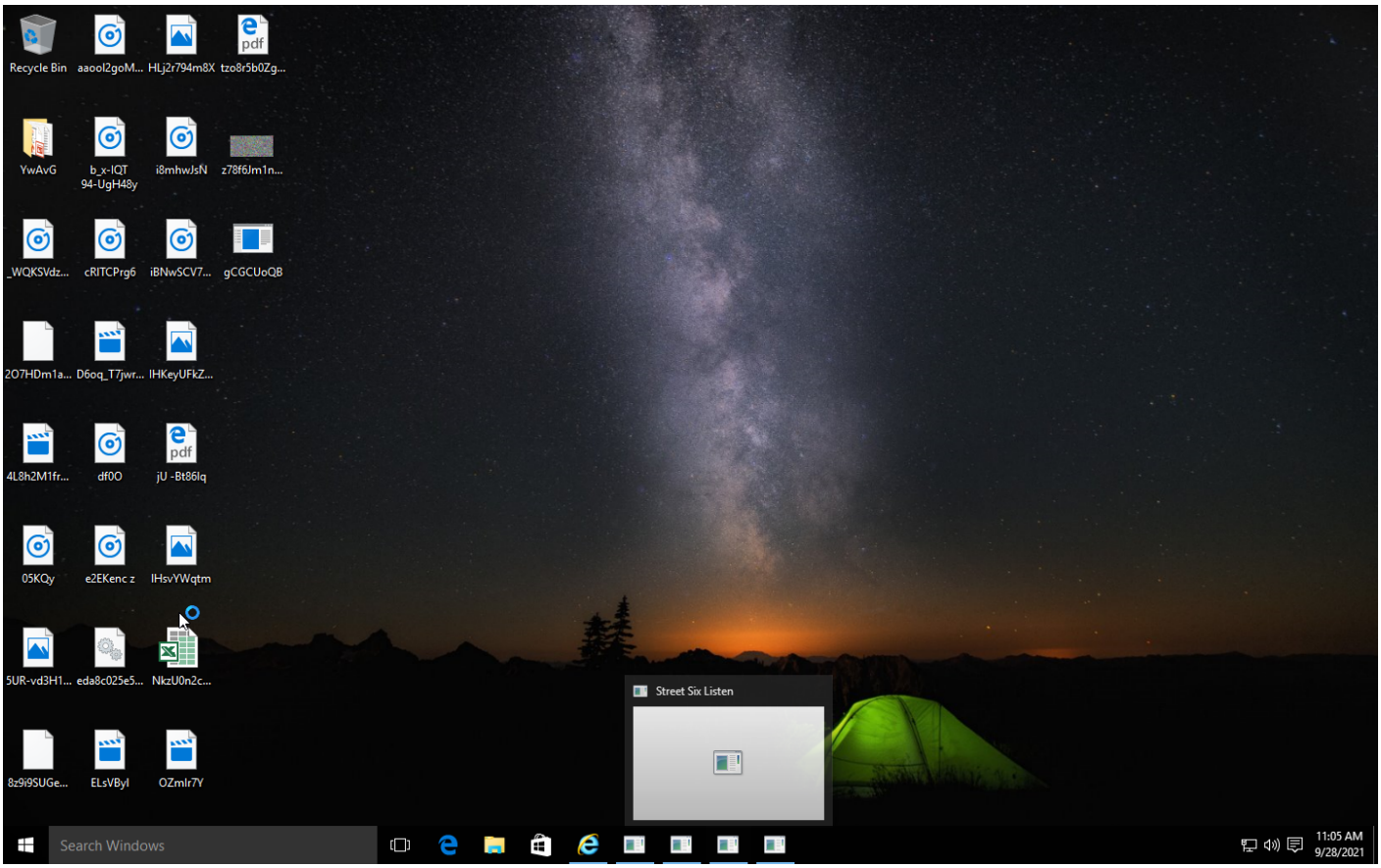
Sample Information

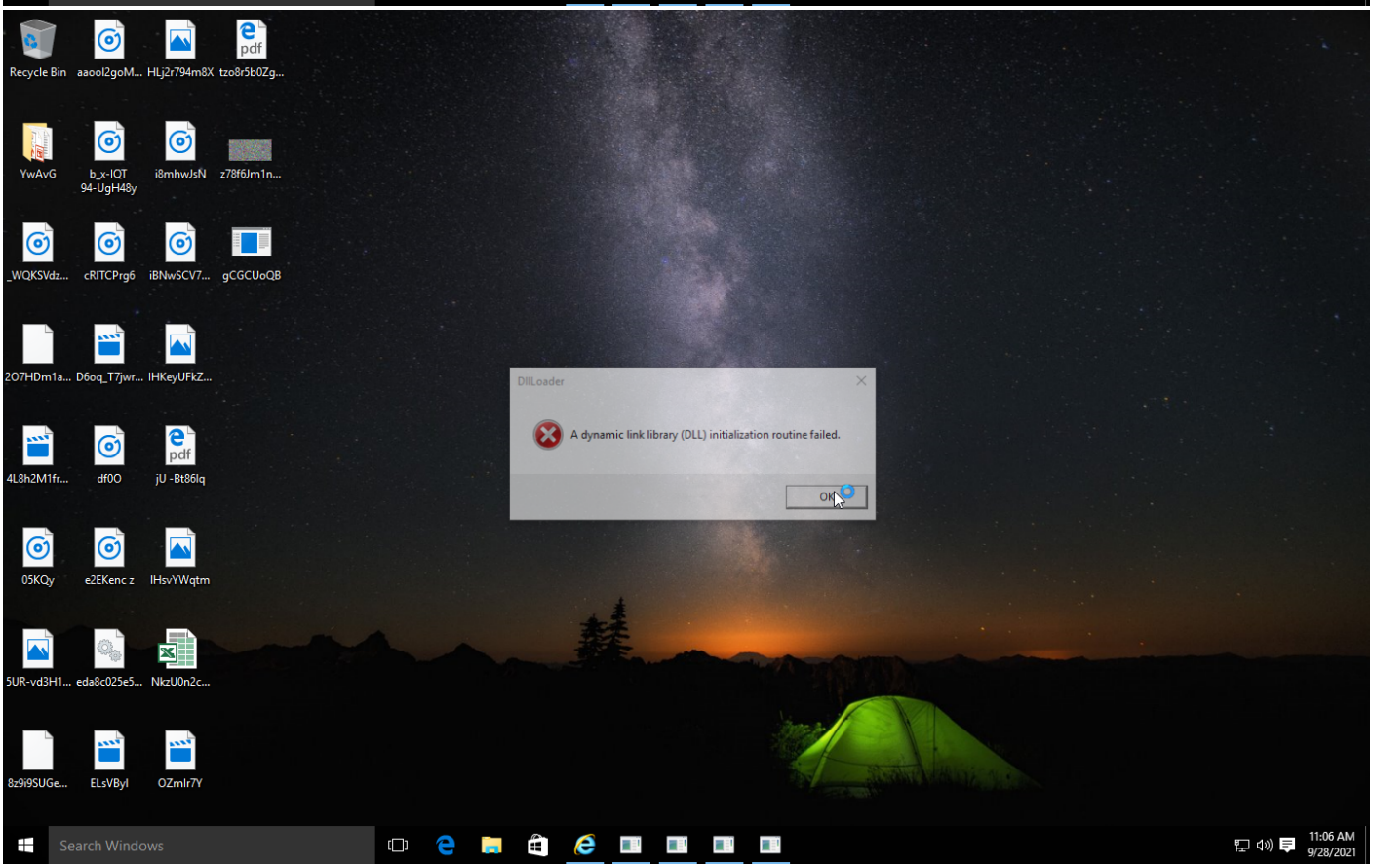
ID	#2782710
MD5	5edd6ba336c4de29f55cadfd2167a67e
SHA1	af181a8f3fe25a515a8fe2a02559e5daceecf976
SHA256	eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d
SSDeep	12288:JVI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:ofP7fWsK5z9A+WGAW+V5SB6Ct4bnb
ImpHash	6668be91e2c948b183827f040944057f
File Name	eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll
File Size	2116.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 13:02 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	61
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	6
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
aaool2goM...
HLj2r794m8X
tzo8r5b0Zg...
YwAvG
b_x-lQT 94-UgH48y
i8mhwJsN
z78f6Jm1n...
_WQKSVdz...
cRITCPrg6
iBNwSCV7...
gCGCUoQB
2O7HDm1a...
D6oq_T7jwr...
IHKeyUFkZ...
4L8h2M1fr...
df0O
jU -Bt86lq
05KQy
e2EKenc z
IHsvYWqtm
5UR-vd3H1...
eda8c025e5...
NkzU0n2c...
8z9i9SUGe...
ELsVByI
OZmlr7Y
Search Windows
11:04 AM
9/28/2021





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

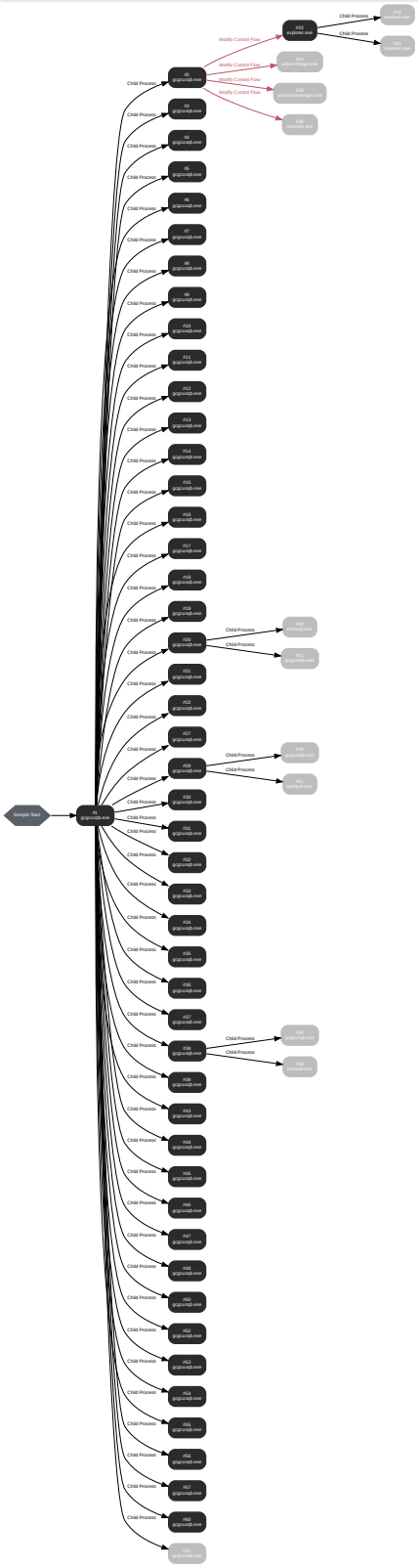
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: gcgcuoqb.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpfppy89vx" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 75480, Reason: Analysis Target
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	246.05s
Return Code	Unknown
PID	5052
Parent PID	1600
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	6
Environment	1
Process	49

Process #2: gcgcuoqb.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=LogonIdFromWinStationNameA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 101836, Reason: Child Process
Unmonitor End Time	End Time: 240540, Reason: Terminated
Monitor duration	138.70s
Return Code	0
PID	3292
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	35
Environment	2
Registry	789
Mutex	6
Process	2
-	49
-	32
-	123

Process #3: gcgcuoqb.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=LogonIdFromWinStationNameW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 102467, Reason: Child Process
Unmonitor End Time	End Time: 158660, Reason: Terminated
Monitor duration	56.19s
Return Code	0
PID	3300
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #4: gcgcuoqb.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=RemoteAssistancePrepareSystemRestore
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 104825, Reason: Child Process
Unmonitor End Time	End Time: 169276, Reason: Terminated
Monitor duration	64.45s
Return Code	0
PID	2524
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	788
Mutex	7

Process #5: gcgcuoqb.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerGetInternetConnectorStatus
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 105827, Reason: Child Process
Unmonitor End Time	End Time: 175717, Reason: Terminated
Monitor duration	69.89s
Return Code	0
PID	2712
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	788
Mutex	7

Process #6: gcgcuoqb.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingClose
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 107844, Reason: Child Process
Unmonitor End Time	End Time: 181717, Reason: Terminated
Monitor duration	73.87s
Return Code	0
PID	1900
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	787
Mutex	7

Process #7: gcgcuoqb.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingDeactivateCurrentPolicy
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 109744, Reason: Child Process
Unmonitor End Time	End Time: 189768, Reason: Terminated
Monitor duration	80.02s
Return Code	0
PID	2508
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	787
Mutex	7

Process #8: gcgcuoqb.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingFreePolicyInformation
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 111964, Reason: Child Process
Unmonitor End Time	End Time: 190732, Reason: Terminated
Monitor duration	78.77s
Return Code	0
PID	1948
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	787
Mutex	7

Process #9: gcgcuoqb.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingGetAvailablePolicyIds
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 114250, Reason: Child Process
Unmonitor End Time	End Time: 198798, Reason: Terminated
Monitor duration	84.55s
Return Code	0
PID	1992
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #10: gcgcuoqb.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingGetPolicy
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 114934, Reason: Child Process
Unmonitor End Time	End Time: 201505, Reason: Terminated
Monitor duration	86.57s
Return Code	0
PID	336
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #11: gcgcuoqb.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingGetPolicyInformationA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 116141, Reason: Child Process
Unmonitor End Time	End Time: 203464, Reason: Terminated
Monitor duration	87.32s
Return Code	0
PID	2872
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #12: gcgcuoqb.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingGetPolicyInformationW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 117697, Reason: Child Process
Unmonitor End Time	End Time: 202337, Reason: Terminated
Monitor duration	84.64s
Return Code	0
PID	1308
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #13: gcgcuoqb.exe

ID	13
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingLoadPolicy
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 122231, Reason: Child Process
Unmonitor End Time	End Time: 205713, Reason: Terminated
Monitor duration	83.48s
Return Code	0
PID	3764
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #14: gcgcuoqb.exe

ID	14
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingOpenA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 127479, Reason: Child Process
Unmonitor End Time	End Time: 205699, Reason: Terminated
Monitor duration	78.22s
Return Code	0
PID	2748
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #15: gcgcuoqb.exe

ID	15
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingOpenW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 136274, Reason: Child Process
Unmonitor End Time	End Time: 215843, Reason: Terminated
Monitor duration	79.57s
Return Code	0
PID	3684
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #16: gcgcuoqb.exe

ID	16
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingSetPolicy
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 150616, Reason: Child Process
Unmonitor End Time	End Time: 222671, Reason: Terminated
Monitor duration	72.06s
Return Code	0
PID	5024
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #17: gcgcuoqb.exe

ID	17
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingUnloadPolicy
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 164860, Reason: Child Process
Unmonitor End Time	End Time: 228680, Reason: Terminated
Monitor duration	63.82s
Return Code	0
PID	5116
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #18: gcgcuoqb.exe

ID	18
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerQueryInetConnectorInformationA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 179344, Reason: Child Process
Unmonitor End Time	End Time: 232862, Reason: Terminated
Monitor duration	53.52s
Return Code	0
PID	4536
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #19: gcgcuoqb.exe

ID	19
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerQueryInetConnectorInformationW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 189985, Reason: Child Process
Unmonitor End Time	End Time: 234218, Reason: Terminated
Monitor duration	44.23s
Return Code	0
PID	2752
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #20: gcgcuoqb.exe

ID	20
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerSetInternetConnectorStatus
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 202542, Reason: Child Process
Unmonitor End Time	End Time: 303482, Reason: Crashed
Monitor duration	100.94s
Return Code	1114
PID	5108
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	43
File	118
System	8
Environment	2
Registry	786
Mutex	6
Process	2
-	51
-	1
-	98
Window	1

Process #21: gcgcuoqb.exe

ID	21
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WTSRegisterSessionNotificationEx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 209117, Reason: Child Process
Unmonitor End Time	End Time: 250021, Reason: Terminated
Monitor duration	40.90s
Return Code	0
PID	5056
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #22: gcgcuoqb.exe

ID	22
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WTSUnRegisterSessionNotificationEx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 215615, Reason: Child Process
Unmonitor End Time	End Time: 254443, Reason: Terminated
Monitor duration	38.83s
Return Code	0
PID	3372
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #23: explorer.exe

ID	23
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 220582, Reason: Injection
Unmonitor End Time	End Time: 321532, Reason: Crashed
Monitor duration	100.95s
Return Code	Unknown
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\gcgcuoqb.exe	0x74c / 0x644	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x688	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x6b8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x6c8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x6d0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x6d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x6f0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x710	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x728	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x73c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x75c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x764	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x768	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x774	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x7a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x7b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0xa9c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0xb94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0xbf8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0xbfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x8b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x5d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x8bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x928	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0xd7c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0xdc0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0xf14	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0xf40	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0xfe8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0xff4	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0xff8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0xa30	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x180	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x574	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x258	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0xd10	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x1d0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x314	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb28bab580(140716696843648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb28bab580(140716696843648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x684	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x644	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x684	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x688	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x6b8	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x6c8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x6d0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x6d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x6f0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x710	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x728	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x73c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x75c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x764	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x768	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x774	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x7a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x7b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xa9c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xb94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xbf8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xbfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x8b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x5d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x8bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x928	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xd7c	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xdc0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xf14	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xf40	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xfe8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xff4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xff8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xa30	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x180	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x574	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x258	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xd10	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x1d0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x314	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x650	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x1304	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0xc28	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x644	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x684	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x688	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x6b8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x6c8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x6d0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x6d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x6f0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x710	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x728	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x73c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x75c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x764	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x768	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x774	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x7a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x7b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0xa9c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0xb94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0xbf8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0xbfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x8b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x5d4	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x8bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x928	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0xd7c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0xdc0	0x7ffb28ba4f00(140716696817408)	-	✓	1

Host Behavior

Type	Count
Module	9

Process #24: active-charge.exe

ID	24
File Name	c:\program files (x86)\msbuild\active-charge.exe
Command Line	"C:\Program Files (x86)\MSBuild\active-charge.exe"
Initial Working Directory	C:\Program Files (x86)\MSBuild\
Monitor Start Time	Start Time: 223038, Reason: Injection
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	98.49s
Return Code	Unknown
PID	4396
Parent PID	1600
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x11e4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x11e4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x11e4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#38: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1170 / 0x11e4	0x7ffb28ba4f00(140716696817408)	-	✓	1

Process #25: yahoomessenger.exe

ID	25
File Name	c:\program files\windows journal\yahoomessenger.exe
Command Line	"C:\Program Files\Windows Journal\yahoomessenger.exe"
Initial Working Directory	C:\Program Files\Windows Journal\
Monitor Start Time	Start Time: 223039, Reason: Injection
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	98.49s
Return Code	Unknown
PID	4404
Parent PID	1600
Bitness	32 Bit

Injection Information (1)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x11e8	0x7ffb28ba4f00(140716696817408)	-	✓	1

Process #26: omnipos.exe

ID	26
File Name	c:\program files (x86)\common files\omnipos.exe
Command Line	"C:\Program Files (x86)\Common Files\omnipos.exe"
Initial Working Directory	C:\Program Files (x86)\Common Files\
Monitor Start Time	Start Time: 223041, Reason: Injection
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	98.49s
Return Code	Unknown
PID	4588
Parent PID	1600
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x74c / 0x1200	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#20: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1024 / 0x1200	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#28: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0xd6c / 0x1200	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#38: c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe	0x1170 / 0x1200	0x7ffb28ba4f00(140716696817408)	-	✓	1

Process #27: gcgcuoqb.exe

ID	27
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationActivateLicense
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 224330, Reason: Child Process
Unmonitor End Time	End Time: 261748, Reason: Terminated
Monitor duration	37.42s
Return Code	0
PID	484
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #28: gcgcuoqb.exe

ID	28
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationAutoReconnect
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 231274, Reason: Child Process
Unmonitor End Time	End Time: 319301, Reason: Crashed
Monitor duration	88.03s
Return Code	1114
PID	3920
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	43
File	118
System	8
Environment	2
Registry	786
Mutex	6
Process	2
-	51
-	1
-	98
Window	1

Process #29: werfault.exe

ID	29
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 1600 -s 3604
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 236512, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	85.02s
Return Code	Unknown
PID	1588
Parent PID	1600
Bitness	64 Bit

Process #30: gcgcuoqb.exe

ID	30
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationBroadcastSystemMessage
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 239641, Reason: Child Process
Unmonitor End Time	End Time: 274769, Reason: Terminated
Monitor duration	35.13s
Return Code	0
PID	3916
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #31: gcgcuoqb.exe

ID	31
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationCheckAccess
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 243823, Reason: Child Process
Unmonitor End Time	End Time: 281396, Reason: Terminated
Monitor duration	37.57s
Return Code	0
PID	3896
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #32: gcgcuoqb.exe

ID	32
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationCheckLoopBack
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 246464, Reason: Child Process
Unmonitor End Time	End Time: 285558, Reason: Terminated
Monitor duration	39.09s
Return Code	0
PID	3388
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #33: gcgcuoqb.exe

ID	33
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationCloseServer
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 250708, Reason: Child Process
Unmonitor End Time	End Time: 289336, Reason: Terminated
Monitor duration	38.63s
Return Code	0
PID	3224
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #34: gcgcuoqb.exe

ID	34
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationConnectA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 251222, Reason: Child Process
Unmonitor End Time	End Time: 290088, Reason: Terminated
Monitor duration	38.87s
Return Code	0
PID	1060
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #35: gcgcuoqb.exe

ID	35
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationConnectAndLockDesktop
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 251640, Reason: Child Process
Unmonitor End Time	End Time: 289954, Reason: Terminated
Monitor duration	38.31s
Return Code	0
PID	4300
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #36: gcgcuoqb.exe

ID	36
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationConnectCallback
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 252359, Reason: Child Process
Unmonitor End Time	End Time: 289546, Reason: Terminated
Monitor duration	37.19s
Return Code	0
PID	4348
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #37: gcgcuoqb.exe

ID	37
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationConnectEx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 253779, Reason: Child Process
Unmonitor End Time	End Time: 294156, Reason: Terminated
Monitor duration	40.38s
Return Code	0
PID	4376
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #38: gcgcuoqb.exe

ID	38
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationConnectW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 260654, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Crashed
Monitor duration	60.88s
Return Code	Unknown
PID	4460
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	9
Environment	2
Registry	786
Mutex	6
Process	2
-	51
-	1
-	98

Process #39: gcgcuoqb.exe

ID	39
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationCreateChildSessionTransport
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 266306, Reason: Child Process
Unmonitor End Time	End Time: 301145, Reason: Terminated
Monitor duration	34.84s
Return Code	0
PID	4748
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #40: werfault.exe

ID	40
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 5108 -s 664
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 268183, Reason: Child Process
Unmonitor End Time	End Time: 297701, Reason: Terminated
Monitor duration	29.52s
Return Code	0
PID	4624
Parent PID	5108
Bitness	64 Bit

Process #41: gcgcuoqb.exe

ID	41
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerSetInternetConnectorStatus
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 268404, Reason: Child Process
Unmonitor End Time	End Time: 298188, Reason: Terminated
Monitor duration	29.78s
Return Code	259
PID	3912
Parent PID	5108
Bitness	64 Bit

Process #42: explorer.exe

ID	42
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 268405, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	53.13s
Return Code	Unknown
PID	4620
Parent PID	1600
Bitness	64 Bit

Process #43: gcgcuoqb.exe

ID	43
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationDisconnect
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 269691, Reason: Child Process
Unmonitor End Time	End Time: 302160, Reason: Terminated
Monitor duration	32.47s
Return Code	0
PID	4684
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #44: gcgcuoqb.exe

ID	44
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnableChildSessions
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 273043, Reason: Child Process
Unmonitor End Time	End Time: 305335, Reason: Terminated
Monitor duration	32.29s
Return Code	0
PID	4880
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #45: gcgcuoqb.exe

ID	45
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerateA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 277967, Reason: Child Process
Unmonitor End Time	End Time: 302173, Reason: Terminated
Monitor duration	24.21s
Return Code	0
PID	3272
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #46: gcgcuoqb.exe

ID	46
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerateExW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 284609, Reason: Child Process
Unmonitor End Time	End Time: 300019, Reason: Terminated
Monitor duration	15.41s
Return Code	0
PID	1860
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #47: gcgcuoqb.exe

ID	47
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerateLicenses
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 289953, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	31.58s
Return Code	Unknown
PID	1424
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	9
Environment	2
Registry	766
Mutex	5
Process	2
-	2
-	1

Process #48: gcgcuoqb.exe

ID	48
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerateProcesses
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 293962, Reason: Child Process
Unmonitor End Time	End Time: 320890, Reason: Terminated
Monitor duration	26.93s
Return Code	0
PID	2760
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #49: gcgcuoqb.exe

ID	49
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationAutoReconnect
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 295704, Reason: Child Process
Unmonitor End Time	End Time: 313662, Reason: Terminated
Monitor duration	17.96s
Return Code	259
PID	1968
Parent PID	3920
Bitness	64 Bit

Process #50: gcgcuoqb.exe

ID	50
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerateW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 296501, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	25.03s
Return Code	Unknown
PID	2060
Parent PID	5052
Bitness	64 Bit

Host Behavior

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

Process #51: werfault.exe

ID	51
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 3920 -s 664
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 296554, Reason: Child Process
Unmonitor End Time	End Time: 313045, Reason: Terminated
Monitor duration	16.49s
Return Code	0
PID	2672
Parent PID	3920
Bitness	64 Bit

Process #52: gcgcuoqb.exe

ID	52
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerate_IndexedA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 300369, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	21.16s
Return Code	Unknown
PID	2580
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #53: gcgcuoqb.exe

ID	53
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerate_IndexedW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 303939, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	17.59s
Return Code	Unknown
PID	3188
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	3

Process #54: gcgcuoqb.exe

ID	54
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationFreeConsoleNotification
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 306917, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	14.62s
Return Code	Unknown
PID	2524
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #55: gcgcuoqb.exe

ID	55
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationFreeEXECENVDATAEX
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 308266, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	13.27s
Return Code	Unknown
PID	4756
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #56: gcgcuoqb.exe

ID	56
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationFreeGAPMemory
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 309791, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	11.74s
Return Code	Unknown
PID	4776
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #57: gcgcuoqb.exe

ID	57
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationFreeMemory
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 311765, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	9.77s
Return Code	Unknown
PID	2712
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #58: gcgcuoqb.exe

ID	58
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationConnectW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 312954, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	8.58s
Return Code	Unknown
PID	4504
Parent PID	4460
Bitness	64 Bit

Process #59: werfault.exe

ID	59
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 4460 -s 664
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 313017, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	8.52s
Return Code	Unknown
PID	4500
Parent PID	4460
Bitness	64 Bit

Process #60: gcgcuoqb.exe

ID	60
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationFreePropertyValue
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 316655, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	4.88s
Return Code	Unknown
PID	1264
Parent PID	5052
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #61: gcgcuoqb.exe

ID	61
File Name	c:\users\rdhj0cnfevzx\desktop\gcgcuoqb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationFreeUserCertificates
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 320296, Reason: Child Process
Unmonitor End Time	End Time: 321532, Reason: Terminated by Timeout
Monitor duration	1.24s
Return Code	Unknown
PID	1992
Parent PID	5052
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d	C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll, C:\Users\RDhJ0CNFevzX\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll	Sample File	2116.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpfppy89vx	Accessed File	Access, Read	CLEAN
C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.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	gcgcuoqb.exe	CLEAN
{54137ce8-d76d-e7fc-dec3-c85f290e5b98}	access	gcgcuoqb.exe	CLEAN

Registry

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

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

Process

Process Name	Commandline	Verdict
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpfppy89vx" /s	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=LogonIdFromWinStationNameA	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=LogonIdFromWinStationNameW	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=RemoteAssistancePrepareSystemRestore	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerGetInternetConnectorStatus	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingClose	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingDeactivateCurrentPolicy	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingFreePolicyInformation	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingGetAvailablePolicyIds	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingGetPolicy	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingGetPolicyInformationA	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingGetPolicyInformationW	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingLoadPolicy	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingOpenA	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingOpenW	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingSetPolicy	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerLicensingUnloadPolicy	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerQueryInetConnectorInformationA	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerQueryInetConnectorInformationW	CLEAN

Process Name	Commandline	Verdict
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=ServerSetInternetConnectorStatus	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WTSRegisterSessionNotificationEx	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WTSUnRegisterSessionNotificationEx	CLEAN
active-charge.exe	"C:\Program Files (x86)\MSBuild\active-charge.exe"	CLEAN
yahoomessenger.exe	"C:\Program Files\Windows Journal\yahoomessenger.exe"	CLEAN
omnipos.exe	"C:\Program Files (x86)\Common Files\omnipos.exe"	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationActivateLicense	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationAutoReconnect	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 1600 -s 3604	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationBroadcastSystemMessage	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationCheckAccess	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationCheckLoopBack	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationCloseServer	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationConnectA	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationConnectAndLockDesktop	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationConnectCallback	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationConnectEx	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationConnectW	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationCreateChildSessionTransport	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 5108 -s 664	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationDisconnect	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnableChildSessions	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerateA	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerateExW	CLEAN

Process Name	Commandline	Verdict
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerateLicenses	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerateProcesses	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerateW	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 3920 -s 664	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerate_IndexedA	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationEnumerate_IndexedW	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationFreeConsoleNotification	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationFreeEXECENVDATAEX	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationFreeGAPMemory	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationFreeMemory	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 4460 -s 664	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationFreePropertyValue	CLEAN
gcgcuoqb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\gCGCUoQB.exe" /dll="C:\Users\RDHJ0C~1\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.exe.dll" /fn_id=WinStationFreeUserCertificates	CLEAN

YARA / AV

Antivirus (6)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\Desktop\eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d.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	Trojan.GenericKDZ.76753	-	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