MALICIOUS

Classifications: Spyware

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

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll**
ID	#969141
MD5	dc4fca98a02c5cc7ee5f565c56915c86
SHA1	4cecd255d9176fff8d0ca18cd3dabd690ce02fbf
SHA256	ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b
File Size	2068.00 KB
Report Created	2021-09-28 13:38 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (16 rules, 138 matches)

Score	Category	Operation	Count	Classification
4/5	Antivirus	Malicious content was detected by heuristic scan	12	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.76753". • Built-in AV detected the dropped file C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\DUI70.dll as "Trojan.GenericKDZ.76753". • Built-in AV detected the dropped file C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\MFC42u.dll as "Trojan.GenericKDZ.76753". • Built-in AV detected the dropped file C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\DUser.dll as "Trojan.GenericKDZ.76753". • Built-in AV detected the dropped file C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\WTSAPI32.dll as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #2) pgdqqc.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #6) explorer.exe as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #11) pgdqqc.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #14) pgdqqc.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #15) sysreseterr.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #17) pgdqqc.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #26) lockapphost.exe as "Gen:Variant.Mikey.113998".		
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #2) pgdqqc.exe alters context of (process #6) explorer.exe.			
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #6) explorer.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #6) explorer.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #6) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Hide Tracks	Deletes file after execution	4	-
	• (Process #6) explorer.exe deletes executed executable "c:\users\rdhj0cnfevzx\appdata\local\kb3\sysreseterr.exe". • (Process #6) explorer.exe deletes executed executable "c:\users\rdhj0cnfevzx\appdata\local\wmyxekae9\mspaint.exe". • (Process #6) explorer.exe deletes executed executable "c:\users\rdhj0cnfevzx\appdata\local\zdy8y\lockapphost.exe". • (Process #6) explorer.exe deletes executed executable "c:\users\rdhj0cnfevzx\appdata\local\t6geh01\slui.exe".			
1/5	Discovery	Reads system data	10	-

Score	Category	Operation	Count	Classification
		• (Process #2) pgdqqc.exe reads the Windows installation date from registry. • (Process #3) pgdqqc.exe reads the Windows installation date from registry. • (Process #4) pgdqqc.exe reads the Windows installation date from registry. • (Process #5) pgdqqc.exe reads the Windows installation date from registry. • (Process #7) pgdqqc.exe reads the Windows installation date from registry. • (Process #6) explorer.exe reads the Windows installation date from registry. • (Process #8) pgdqqc.exe reads the Windows installation date from registry. • (Process #9) pgdqqc.exe reads the Windows installation date from registry. • (Process #19) pgdqqc.exe reads the Windows installation date from registry. • (Process #21) pgdqqc.exe reads the Windows installation date from registry.		
1/5	Mutex	Creates mutex	87	-

- (Process #2) pgdqqc.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #2) pgdqqc.exe creates mutex with name "{20974a93-a551-df17-8967-748358091d34}".
- (Process #3) pgdqqc.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #4) pgdqqc.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #5) pgdqqc.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #7) pgdqqc.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #6) explorer.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #6) explorer.exe creates mutex with name "{298ddcca-efe5-2f07-cbb5-e91e37797537}".
- (Process #6) explorer.exe creates mutex with name "{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}".
- (Process #6) explorer.exe creates mutex with name "{389fe546-d029-33a7-6305-2ca1cede0678}".
- (Process #6) explorer.exe creates mutex with name "{e8b6fe55-d858-d6e4-ef99-a80106642ab4}".
- (Process #6) explorer.exe creates mutex with name "{03b2a674-5295-21d6-da36-fc13faee0e98}".
- (Process #6) explorer.exe creates mutex with name "{d439f686-d570-7182-3906-1e2d175d1088}".
- (Process #6) explorer.exe creates mutex with name "{7d6ed4f3-6751-62a2-fd4a-b51cf5291b13}".
- (Process #6) explorer.exe creates mutex with name "{a73fffb8-61a4-f5fe-f3bf-f23b8e0debc2}".
- (Process #6) explorer.exe creates mutex with name "{3e1c23ac-bb6d-7ca6-0ea0-2d76e5670962}".
- (Process #6) explorer.exe creates mutex with name "{9b151509-5138-7d7a-187c-44a5c211ec53}".
- (Process #6) explorer.exe creates mutex with name "{0f7daade-cabb-071c-b422-48138f19f093}".
- (Process #6) explorer.exe creates mutex with name "{376aea27-53fd-bd89-7168-ab488bf01459}".
- (Process #6) explorer.exe creates mutex with name "{8aadbf32-a058-ae7b-e2fa-32a552670e17}".
- (Process #6) explorer.exe creates mutex with name "{11af7784-fda9-4020-881a-e50efb1e84cd}".
- (Process #6) explorer.exe creates mutex with name "{96a8b4e8-9fb3-87d6-00d9-a27202e9fcb0}".
- (Process #6) explorer.exe creates mutex with name "{153471c9-9d0a-7104-5275-71ac64b2065e}".
- (Process #6) explorer.exe creates mutex with name "{347b949e-da97-ee8f-812b-2fca7cf89cb5}".
- (Process #6) explorer.exe creates mutex with name "{19a9def8-7e87-44e0-b180-e8de92fad2a5}".
- (Process #6) explorer.exe creates mutex with name "{25fdcad7-f614-d8db-5c91-5ebad4f4d05e}".
- (Process #6) explorer.exe creates mutex with name "{633b0084-f455-d65f-7a89-5c7a238812c2}".
- (Process #6) explorer.exe creates mutex with name "{95a1cd4d-d6fc-bfd3-3c8f-37dc107d2fca}".
- (Process #6) explorer.exe creates mutex with name "{d89ae3f6-8bc6-6d82-7660-2578a416e6c0}".
- (Process #6) explorer.exe creates mutex with name "{28d724ec-22da-95bd-9f65-2e17dc8aecd0}".
- (Process #6) explorer.exe creates mutex with name "{fc269880-1f3e-c6d2-e541-ca3ff24ab1bc}".
- (Process #6) explorer.exe creates mutex with name "{fe886e8c-a23d-7a39-eb2b-a2f6429f4e23}".
- (Process #6) explorer.exe creates mutex with name "{b59ea4fc-7bc4-2dca-f7bf-d3e31efaff7e}".
- (Process #6) explorer.exe creates mutex with name "{4236a99f-3514-853f-daf5-e82e3c1b0317}".
- (Process #6) explorer.exe creates mutex with name "{e300a459-3dc2-cd5e-7ba3-52ae228e2e90}".
- (Process #6) explorer.exe creates mutex with name "{acc1be65-c0b2-79a5-d2cb-9aa47275027b}".
- (Process #6) explorer.exe creates mutex with name "{08936f51-fe02-2054-cc27-6952c80ac716}".
- (Process #6) explorer.exe creates mutex with name "{13b3fa1d-d4bb-b7cc-c9f3-6fdf6b535b90}".
- (Process #6) explorer.exe creates mutex with name "{9b8e3f9b-6a14-ba61-86de-29155d8b4094}".
- (Process #6) explorer.exe creates mutex with name "{d87db754-0e49-5182-f0f9-ec9fe8dc9ec9}".
- (Process #6) explorer.exe creates mutex with name "{58f5e2e3-5e83-a5a1-f2f1-1115b521ea00}".
- (Process #6) explorer.exe creates mutex with name "{575fbde0-9713-efa5-165a-bc21541e4190}".
- (Process #6) explorer.exe creates mutex with name "{f9bbbbdf-59be-1b9c-d32d-15c9687d5250}".
- (Process #6) explorer.exe creates mutex with name "{c9a65329-61aa-8be1-61af-620ce6b5f66f}".
- (Process #6) explorer.exe creates mutex with name "{38a99613-bfcc-7bdc-541b-9cece7db7691}".
- (Process #6) explorer.exe creates mutex with name "{2899e51a-dd70-0150-e9f3-f3aba091c8e0}".
- (Process #6) explorer.exe creates mutex with name "{daf86618-6ec6-d890-7978-8720661e5a12}".
- (Process #6) explorer.exe creates mutex with name "{362882c5-03e2-fd0f-928d-c1120ad9c64f}".
- (Process #6) explorer.exe creates mutex with name "{a3dce688-6117-3ea3-fbbd-1defec717462}".
- (Process #6) explorer.exe creates mutex with name "{39fed215-396f-cbc9-07b5-5de635b0306d}".
- (Process #6) explorer.exe creates mutex with name "{35222349-38a9-6107-aeba-d926ff73ead9}".
- (Process #6) explorer.exe creates mutex with name "{168ee11b-299f-6d76-b48f-88a65a4a58ba}".
- (Process #6) explorer.exe creates mutex with name "{01f24baa-a48c-b675-d94f-c4d185fa1b74}".
- (Process #6) explorer.exe creates mutex with name "{60d53e50-c02a-fd11-36ca-0f91b9ec3738}".
- (Process #6) explorer.exe creates mutex with name "{6ec5b40a-313e-69df-1ad2-48a8055c5743}".
- (Process #6) explorer.exe creates mutex with name "{f7677ce1-197d-c706-bc9e-7239a2ec86e1}".
- (Process #6) explorer.exe creates mutex with name "{6c570128-9202-fd64-daa4-72143d141e8a}".
- (Process #6) explorer.exe creates mutex with name "{6a858a42-f46d-62bb-e142-0d99eeaf1f91}".
- (Process #6) explorer.exe creates mutex with name "{583163e6-97f6-ca24-26b7-ae90d9895822}".
- (Process #6) explorer.exe creates mutex with name "{[illegible]}".

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

• (Process #2) pgdqqc.exe reads from (process #6) explorer.exe.

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Writes an unusually large amount of data to the registry	1	-

• (Process #6) explorer.exe hides 3526 bytes in "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{61E3425B-6B05-A459-B4FE-174B2D84DE94}\ShellFolder\{DD4B594C-5D5B-1375-55F8-84E364592B6A}".

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Creates process with hidden window	4	-

• (Process #6) explorer.exe starts (process #13) sysreseterr.exe with a hidden window.
• (Process #6) explorer.exe starts (process #15) sysreseterr.exe with a hidden window.
• (Process #6) explorer.exe starts (process #20) mspaint.exe with a hidden window.
• (Process #6) explorer.exe starts (process #26) lockapphost.exe with a hidden window.

Score	Category	Operation	Count	Classification
1/5	Execution	Drops PE file	8	-

• (Process #6) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\DUI70.dll".
• (Process #6) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\MFC42u.dll".
• (Process #6) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\DUser.dll".
• (Process #6) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\WTSAPI32.dll".
• (Process #6) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\SysResetErr.exe".
• (Process #6) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\mspaint.exe".
• (Process #6) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\LockAppHost.exe".
• (Process #6) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\slui.exe".

Score	Category	Operation	Count	Classification
1/5	Execution	Executes dropped PE file	4	-

• Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\SysResetErr.exe".
• Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\mspaint.exe".
• Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\LockAppHost.exe".
• Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\slui.exe".

Score	Category	Operation	Count	Classification
1/5	Crash	A monitored process crashed	1	-

• (Process #17) pgdqqc.exe crashed.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	1	-

• (Process #6) explorer.exe resolves 26 API functions by name.

Score	Category	Operation	Count	Classification
-	Trusted	Known clean file	4	-

• File "C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\SysResetErr.exe" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\mspaint.exe" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\LockAppHost.exe" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\slui.exe" is a known clean file.

Mitre ATT&CK Matrix

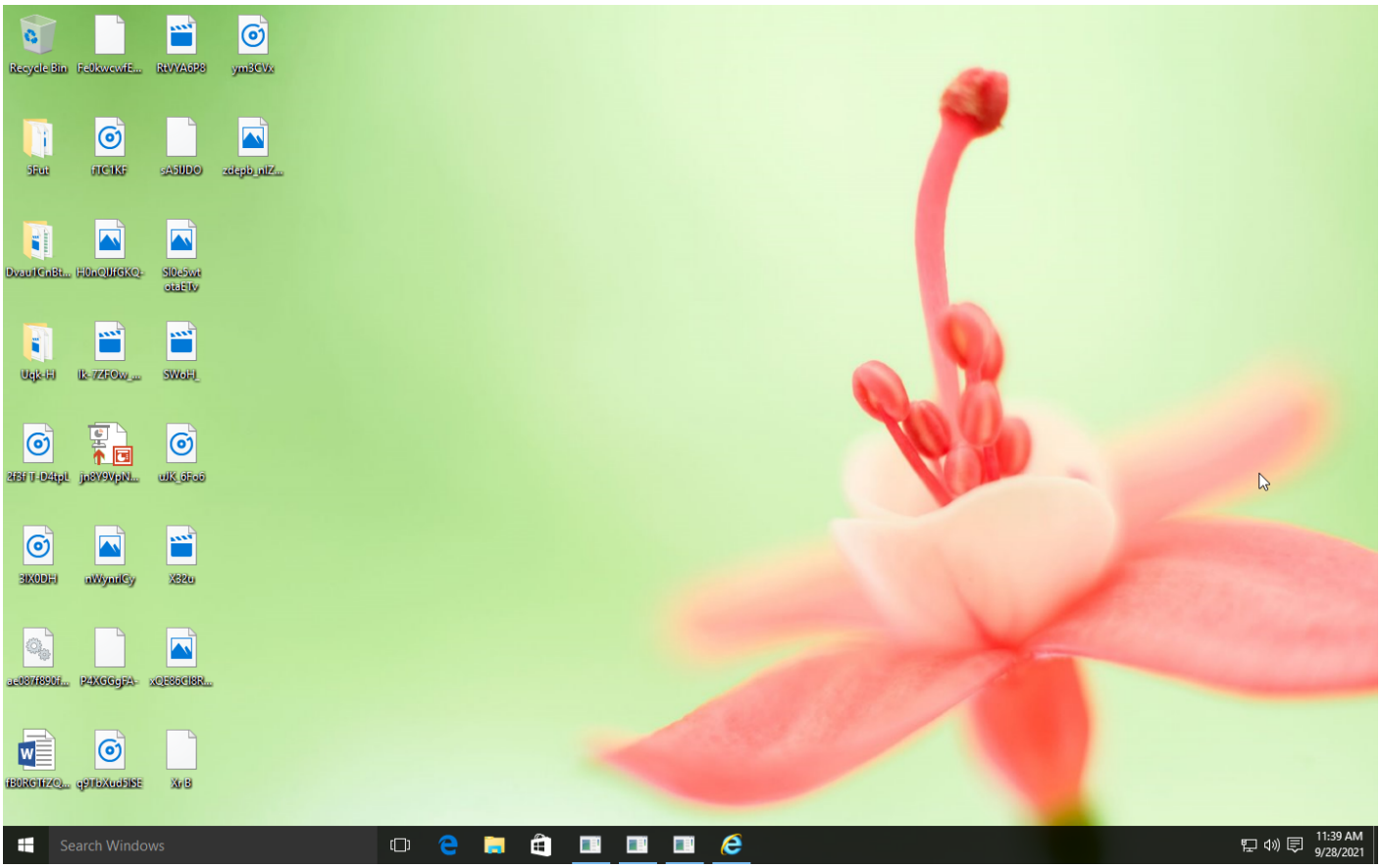
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1112 Modify Registry	#T1081 Credentials in Files	#T1082 System Information Discovery		#T1119 Automated Collection			
				#T1143 Hidden Window		#T1012 Query Registry		#T1005 Data from Local System			
				#T1045 Software Packing		#T1083 File and Directory Discovery					

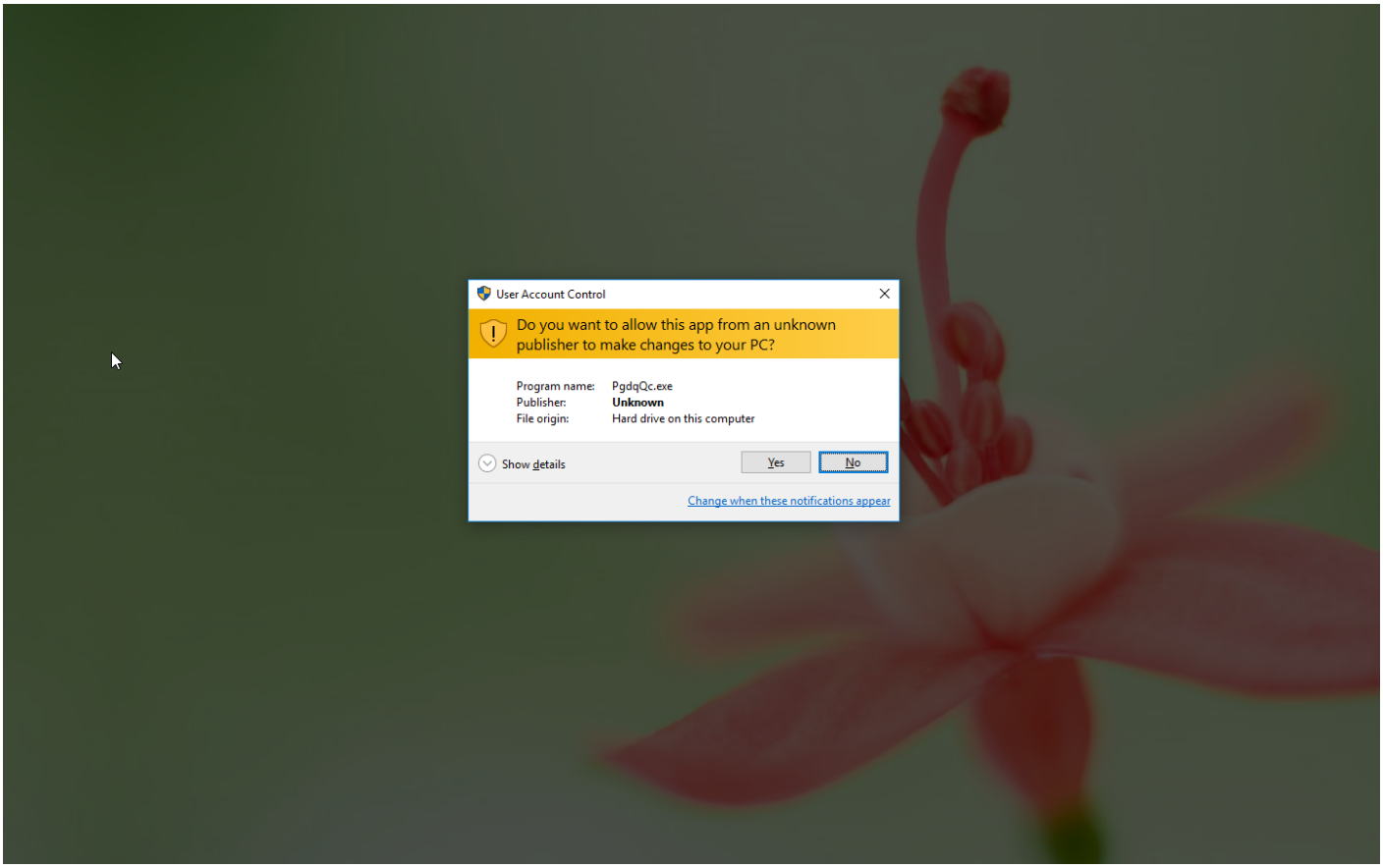
Sample Information

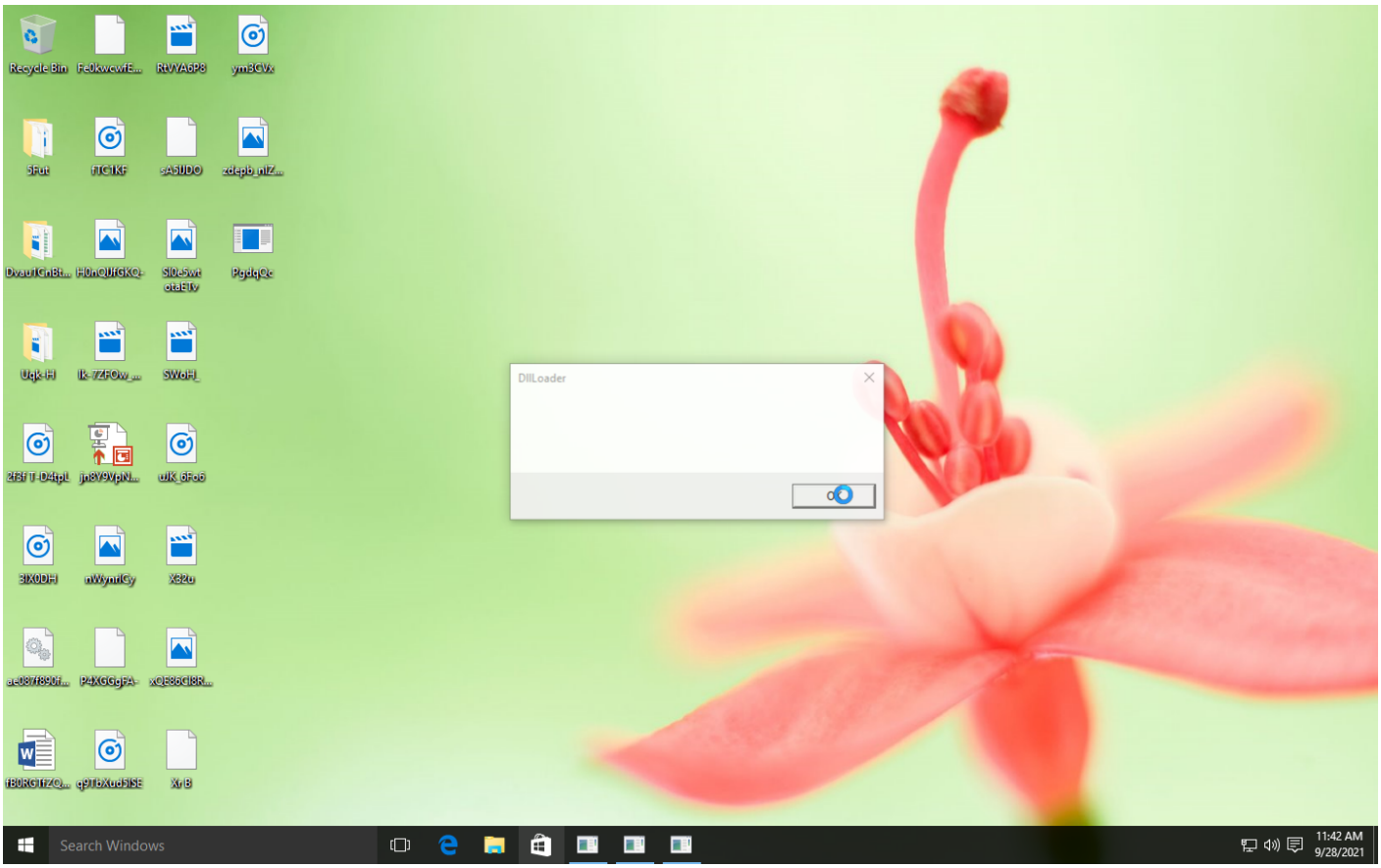
ID	#969141
MD5	dc4fca98a02c5cc7ee5f565c56915c86
SHA1	4cecd255d9176fff8d0ca18cd3dabd690ce02fbf
SHA256	ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b
SSDeep	12288:YVI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:NfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
ImpHash	6668be91e2c948b183827f040944057f
File Name	ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll
File Size	2068.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

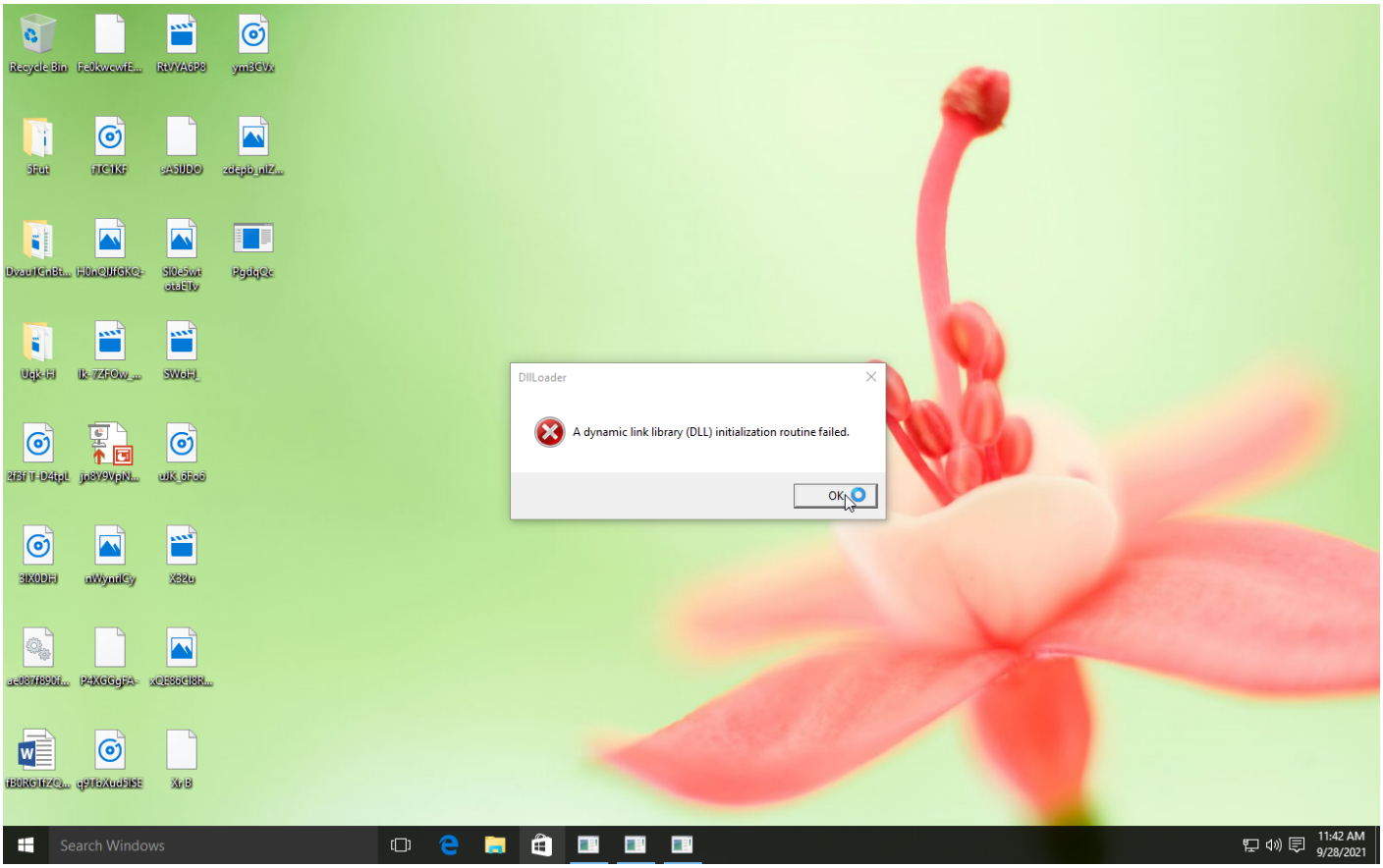
Analysis Information

Creation Time	2021-09-28 13:38 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	36
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	15
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Search Windows
11:39 AM
9/28/2021


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: PgdqQc.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

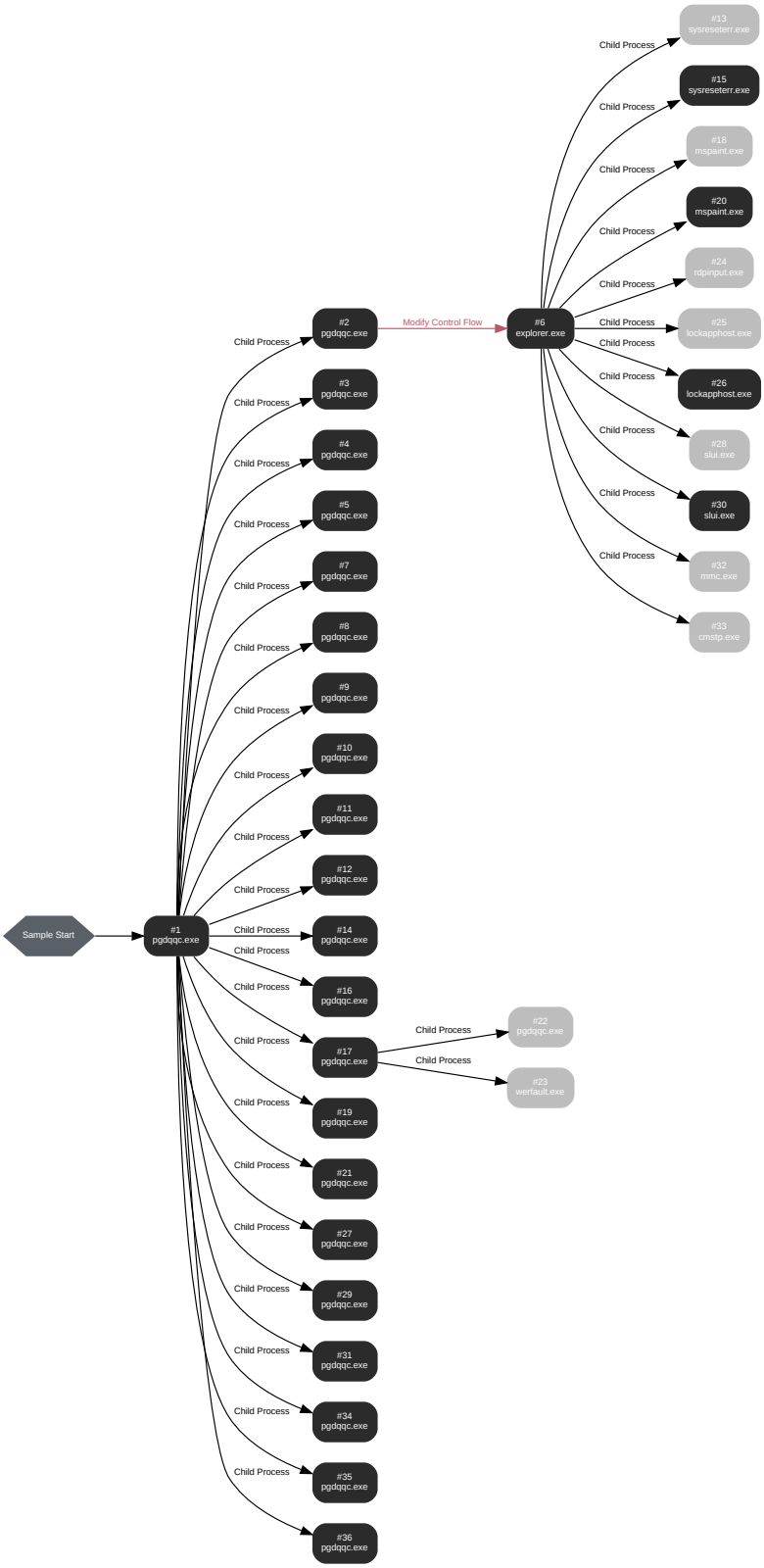
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: pgdqqc.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpzpfphz26" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 61251, Reason: Analysis Target
Unmonitor End Time	End Time: 301823, Reason: Terminated by Timeout
Monitor duration	240.57s
Return Code	Unknown
PID	4008
Parent PID	1636
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	6
Environment	1
Process	22

Process #2: pgdqqc.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=AddGadgetMessageHandler
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 84881, Reason: Child Process
Unmonitor End Time	End Time: 142167, Reason: Terminated
Monitor duration	57.29s
Return Code	0
PID	1512
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	35
Environment	2
Registry	768
Mutex	6
Process	2
-	50
-	32
-	124

Process #3: pgdqqc.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=AddLayeredRef
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 88223, Reason: Child Process
Unmonitor End Time	End Time: 101173, Reason: Terminated
Monitor duration	12.95s
Return Code	0
PID	864
Parent PID	4008
Bitness	64 Bit

Host Behavior

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

Process #4: pgdqqc.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=AdjustClipInsideRef
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 90750, Reason: Child Process
Unmonitor End Time	End Time: 102660, Reason: Terminated
Monitor duration	11.91s
Return Code	0
PID	656
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	769
Mutex	7

Process #5: pgdqqc.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=AttachWndProcA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 93455, Reason: Child Process
Unmonitor End Time	End Time: 104267, Reason: Terminated
Monitor duration	10.81s
Return Code	0
PID	1212
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	776
Mutex	7

Process #6: explorer.exe

ID	6
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 97287, Reason: Injection
Unmonitor End Time	End Time: 301823, Reason: Terminated by Timeout
Monitor duration	204.54s
Return Code	Unknown
PID	1636
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (75)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x668	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x694	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x6ac	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x6b0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x6b4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x6b8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x6bc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x6dc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x6e8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x71c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x734	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x73c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x74c	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x798	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x7a8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x7b0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x7d0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x7ec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x7f0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x460	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x83c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x954	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x9c0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0xbec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x4c4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x4ac	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x8b4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x984	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x97c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0xa20	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0xfd0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0xfec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x444	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x364	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0xa98	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0xdcc	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0xdb4	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0xa34	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x61c	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0xca4	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0xaf4	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0xcb8	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0xabc	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x1220	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x1228	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x1240	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x12e8	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5f8bb580(140721911477632)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5f8bb580(140721911477632)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe	0x368 / 0x690	0x7ffc5ecdce60(140721899032160)	-	✔	1

Dropped Files (12)

File Name	File Size	SHA256	YARA Match
-	53 bytes	e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	✘
C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\DUI70.dll	2336.00 KB	50f4a87ac83907aa2dcc8eb5453c5a40ed9f2dadfb4e41322df7d6c3737b4a9e	✘
C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\SysResetErr.exe	28.34 KB	9d4cb5b985028d5e16c1311cf1f9007523a7af7d879dc0b68cc31978d159b8fc	✘
C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\MFC42u.dll	2096.00 KB	6db3e593472a28b816404ca328fdf9b52b1b589ca3499e4fafca69dfee87c61d	✘
C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\mspaint.exe	6519.50 KB	7b9d7b5afa321faabed26764cd7859151beaa08e0833de477c27d6707fde3b45	✘

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\DUser.dll	2076.00 KB	ef7dffea98f914d9e7e1f21d4a13cac2111efa47e86b4f3a24178008c1211055	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\LockAppHost.exe	293.07 KB	261004ada21a7f0b3c16b9474783eccc4ec8595f547f498a06a480e7e69d123b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\WTSAPI32.dll	2072.00 KB	fa95fa9a2cd0fab863b61712fb9ede621905cba8e703c3dc28e6f60e616c4312	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\slui.exe	435.00 KB	71f372bf9d92c8f94ac688a0289b63a6133cba5e29cf5414eaa00ef5b7b13fd5	✗
-	1.42 KB	8cc33984023f1ea31937cf70487c39c4f394c4bb6a41f22da6f3f4c453757f0b	✗
-	1.42 KB	4459de34f31d879717f63fcf0b48c4b322ee763c7e60d4b0e2a2a61a7805cf43	✗
-	1.42 KB	e3b975fa3d855c2b3cc736075ea919bd07545feee2c021515f20671a1154fecc	✗

Host Behavior

Type	Count
Module	48
File	726
System	1129
Process	141
Registry	30426
Environment	2
-	29
Mutex	4499

Process #7: pgdqqc.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=AttachWndProcW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 100698, Reason: Child Process
Unmonitor End Time	End Time: 107197, Reason: Terminated
Monitor duration	6.50s
Return Code	0
PID	1648
Parent PID	4008
Bitness	64 Bit

Host Behavior

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

Process #8: pgdqqc.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=AutoTrace
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 102515, Reason: Child Process
Unmonitor End Time	End Time: 177203, Reason: Terminated
Monitor duration	74.69s
Return Code	0
PID	1192
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	227
Mutex	4

Process #9: pgdqqc.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=BeginHideInputPaneAnimation
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 103914, Reason: Child Process
Unmonitor End Time	End Time: 183157, Reason: Terminated
Monitor duration	79.24s
Return Code	0
PID	1880
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	227
Mutex	4

Process #10: pgdqqc.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=BeginShowInputPaneAnimation
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 126336, Reason: Child Process
Unmonitor End Time	End Time: 220859, Reason: Terminated
Monitor duration	94.52s
Return Code	0
PID	2524
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	95
Mutex	4

Process #11: pgdqqc.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=BuildAnimation
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 140946, Reason: Child Process
Unmonitor End Time	End Time: 219274, Reason: Terminated
Monitor duration	78.33s
Return Code	0
PID	4660
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	116
Mutex	4

Process #12: pgdqqc.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=BuildDropTarget
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 142737, Reason: Child Process
Unmonitor End Time	End Time: 218860, Reason: Terminated
Monitor duration	76.12s
Return Code	0
PID	1252
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	95
Mutex	4

Process #13: sysreseterr.exe

ID	13
File Name	c:\windows\system32\sysreseterr.exe
Command Line	C:\Windows\system32\SysResetErr.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 188133, Reason: Child Process
Unmonitor End Time	End Time: 196195, Reason: Terminated
Monitor duration	8.06s
Return Code	0
PID	1400
Parent PID	1636
Bitness	64 Bit

Process #14: pgdqqc.exe

ID	14
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=BuildInterpolation
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 195185, Reason: Child Process
Unmonitor End Time	End Time: 224432, Reason: Terminated
Monitor duration	29.25s
Return Code	0
PID	1728
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	95
Mutex	4

Process #15: sysreseterr.exe

ID	15
File Name	c:\users\rdhj0cnfevzx\appdata\local\kb3\sysreseterr.exe
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\SysResetErr.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 205680, Reason: Child Process
Unmonitor End Time	End Time: 218851, Reason: Terminated
Monitor duration	13.17s
Return Code	0
PID	2056
Parent PID	1636
Bitness	64 Bit

Host Behavior

Type	Count
File	109
Module	11

Process #16: pgdqqc.exe

ID	16
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=CacheDWriteRenderTarget
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 208635, Reason: Child Process
Unmonitor End Time	End Time: 246840, Reason: Terminated
Monitor duration	38.20s
Return Code	0
PID	4176
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	164
Mutex	4

Process #17: pgdqqc.exe

ID	17
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=ChangeCurrentAnimationScenario
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 212455, Reason: Child Process
Unmonitor End Time	End Time: 289225, Reason: Crashed
Monitor duration	76.77s
Return Code	1114
PID	4256
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	31
File	112
Environment	1
Window	1

Process #18: mspaint.exe

ID	18
File Name	c:\windows\system32\mspaint.exe
Command Line	C:\Windows\system32\mspaint.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 219316, Reason: Child Process
Unmonitor End Time	End Time: 222468, Reason: Terminated
Monitor duration	3.15s
Return Code	0
PID	4316
Parent PID	1636
Bitness	64 Bit

Process #19: pgdqqc.exe

ID	19
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=ClearPushedOpacitiesFromGadgetTree
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 223962, Reason: Child Process
Unmonitor End Time	End Time: 265818, Reason: Terminated
Monitor duration	41.86s
Return Code	0
PID	4324
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	226
Mutex	4

Process #20: mspaint.exe

ID	20
File Name	c:\users\rdhj0cnfevzx\appdata\local\wmyxekae9\mspaint.exe
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\mspaint.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 230914, Reason: Child Process
Unmonitor End Time	End Time: 246839, Reason: Terminated
Monitor duration	15.93s
Return Code	0
PID	4072
Parent PID	1636
Bitness	64 Bit

Host Behavior

Type	Count
File	109
Module	11

Process #21: pgdqqc.exe

ID	21
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=ClearTopmostVisual
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 234491, Reason: Child Process
Unmonitor End Time	End Time: 289177, Reason: Terminated
Monitor duration	54.69s
Return Code	0
PID	4360
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	226
Mutex	4

Process #22: pgdqqc.exe

ID	22
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=ChangeCurrentAnimationScenario
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 237032, Reason: Child Process
Unmonitor End Time	End Time: 277324, Reason: Terminated
Monitor duration	40.29s
Return Code	259
PID	4032
Parent PID	4256
Bitness	64 Bit

Process #23: werfault.exe

ID	23
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 4256 -s 360
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 239147, Reason: Child Process
Unmonitor End Time	End Time: 277302, Reason: Terminated
Monitor duration	38.16s
Return Code	0
PID	4884
Parent PID	4256
Bitness	64 Bit

Process #24: rdpinput.exe

ID	24
File Name	c:\windows\system32\rdpinput.exe
Command Line	C:\Windows\system32\rdpinput.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 243702, Reason: Child Process
Unmonitor End Time	End Time: 246137, Reason: Terminated
Monitor duration	2.44s
Return Code	3221226540
PID	5008
Parent PID	1636
Bitness	64 Bit

Process #25: lockapphost.exe

ID	25
File Name	c:\windows\system32\lockapphost.exe
Command Line	C:\Windows\system32\LockAppHost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 245266, Reason: Child Process
Unmonitor End Time	End Time: 249005, Reason: Terminated
Monitor duration	3.74s
Return Code	0
PID	2940
Parent PID	1636
Bitness	64 Bit

Process #26: lockapphost.exe

ID	26
File Name	c:\users\rdhj0cnfevzx\appdata\local\zdy8y\lockapphost.exe
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\LockAppHost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 251457, Reason: Child Process
Unmonitor End Time	End Time: 266222, Reason: Terminated
Monitor duration	14.77s
Return Code	0
PID	4876
Parent PID	1636
Bitness	64 Bit

Host Behavior

Type	Count
File	109
Module	11

Process #27: pgdqqc.exe

ID	27
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=CreateAction
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 252807, Reason: Child Process
Unmonitor End Time	End Time: 301823, Reason: Terminated by Timeout
Monitor duration	49.02s
Return Code	Unknown
PID	4368
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	95
Mutex	3

Process #28: slui.exe

ID	28
File Name	c:\windows\system32\slui.exe
Command Line	C:\Windows\system32\slui.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 261936, Reason: Child Process
Unmonitor End Time	End Time: 267677, Reason: Terminated
Monitor duration	5.74s
Return Code	0
PID	4644
Parent PID	1636
Bitness	64 Bit

Process #29: pgdqqc.exe

ID	29
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=CreateGadget
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 266159, Reason: Child Process
Unmonitor End Time	End Time: 301823, Reason: Terminated by Timeout
Monitor duration	35.66s
Return Code	Unknown
PID	616
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	113
Mutex	3

Process #30: slui.exe

ID	30
File Name	c:\users\rdhj0cnfevzx\appdata\local\t6geh01\slui.exe
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\slui.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 267103, Reason: Child Process
Unmonitor End Time	End Time: 279548, Reason: Terminated
Monitor duration	12.45s
Return Code	0
PID	2160
Parent PID	1636
Bitness	64 Bit

Host Behavior

Type	Count
File	109
Module	11

Process #31: pgdqqc.exe

ID	31
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=CustomGadgetHitTestQuery
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 276619, Reason: Child Process
Unmonitor End Time	End Time: 301823, Reason: Terminated by Timeout
Monitor duration	25.20s
Return Code	Unknown
PID	1264
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	95
Mutex	3

Process #32: mmc.exe

ID	32
File Name	c:\windows\system32\mmc.exe
Command Line	C:\Windows\system32\mmc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 278397, Reason: Child Process
Unmonitor End Time	End Time: 282450, Reason: Terminated
Monitor duration	4.05s
Return Code	3221226540
PID	3792
Parent PID	1636
Bitness	64 Bit

Process #33: cmstp.exe

ID	33
File Name	c:\windows\system32\cmstp.exe
Command Line	C:\Windows\system32\cmstp.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 279953, Reason: Child Process
Unmonitor End Time	End Time: 283689, Reason: Terminated
Monitor duration	3.74s
Return Code	0
PID	3316
Parent PID	1636
Bitness	64 Bit

Process #34: pgdqqc.exe

ID	34
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=DUserBuildGadget
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 288589, Reason: Child Process
Unmonitor End Time	End Time: 301823, Reason: Terminated by Timeout
Monitor duration	13.23s
Return Code	Unknown
PID	3392
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	95
Mutex	3

Process #35: pgdqqc.exe

ID	35
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=DUserCastClass
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 292501, Reason: Child Process
Unmonitor End Time	End Time: 301823, Reason: Terminated by Timeout
Monitor duration	9.32s
Return Code	Unknown
PID	2856
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #36: pgdqqc.exe

ID	36
File Name	c:\users\rdhj0cnfevzx\desktop\pgdqqc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=DUserCastDirect
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 295014, Reason: Child Process
Unmonitor End Time	End Time: 301823, Reason: Terminated by Timeout
Monitor duration	6.81s
Return Code	Unknown
PID	3728
Parent PID	4008
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b	C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll, C:\Users\RDhJ0CNFevzX\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll	Sample File	2068.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
50f4a87ac83907aa2dcc8eb5453c5a40ed9f2dadfb4e41322df7d6c3737b4a9e	C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\DUI70.dll	Dropped File	2336.00 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	MALICIOUS
6db3e593472a28b816404ca328fdf9b52b1b589ca3499e4fafca69dfee87c61d	C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\MFC42u.dll	Dropped File	2096.00 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	MALICIOUS
ef7dffea98f914d9e7e1f21d4a13cac2111efa47e86b4f3a24178008c1211055	C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\DUser.dll	Dropped File	2076.00 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	MALICIOUS
fa95fa9a2cd0fab863b61712fb9ede621905cba8e703c3dc28e6f60e616c4312	C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\WTSAPI32.dll	Dropped File	2072.00 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	MALICIOUS
9d4cb5b985028d5e16c1311cf1f9007523a7af7d879dc0b68cc31978d159b8fc	C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\SysResetErr.exe	Dropped File	28.34 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	SUSPICIOUS
7b9d7b5afa321faabed26764cd7859151beaa08e0833de477c27d6707fde3b45	C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\mspaint.exe	Dropped File	6519.50 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	SUSPICIOUS
261004ada21a7f0b3c16b9474783eccc4ec8595f547f498a06a480e7e69d123b	C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\LockAppHost.exe	Dropped File	293.07 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	SUSPICIOUS
71f372bf9d92c8f94ac688a0289b63a6133cba5e29cf5414eaa00ef5b7b13fd5	C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\slui.exe	Dropped File	435.00 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	SUSPICIOUS
e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	53 bytes	application/octet-stream	-	CLEAN
8cc33984023f1ea31937cf70487c39c4f394c4bb6a41f22da6f3f4c453757f0b	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	1.42 KB	application/octet-stream	-	CLEAN
4459de34f31d879717f63fcf0b48c4b322ee763c7e60d4b0e2a2a61a7805cf43	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	1.42 KB	application/octet-stream	-	CLEAN
e3b975fa3d855c2b3cc736075ea919bd07545feee2c021515f20671a1154fecc	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	1.42 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpzpfphz26	Accessed File	Read, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll	Accessed File	Read, Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\Explorer.EXE	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesCommonX86\system\msmapi\1033\msmapi32.dll	Accessed File	Read, Access	CLEAN
C:\Program Files (x86)\Internet Explorer\outlook.exe	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Adobe\MEhdx3	Accessed File	Create, Access	CLEAN
C:\Windows\system32\userinit.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\MdSched.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\PrintIsolationHost.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\verclsid.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\wpr.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\TSWbPrxy.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\chgport.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\Narrator.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\CredentialUIBroker.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\SysResetErr.exe	Accessed File	Read, Access	CLEAN
C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wow64.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wow64win.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wow64cpu.dll	Accessed File	Access	CLEAN
C:\Windows\system32\DUI70.dll	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\DUI70.dll	Dropped File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\SysResetErr.exe	Dropped File	Write, Create, Delete, Access	CLEAN
C:\Windows\system32\fixmapi.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\acu.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\mspaint.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\MFC42u.dll	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\MFC42u.dll	Dropped File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\mspaint.exe	Dropped File	Write, Create, Delete, Access	CLEAN
C:\Windows\system32\rdpinput.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\net.exe	Accessed File	Read, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\LockAppHost.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\DUser.dll	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\DUser.dll	Dropped File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\LockAppHost.exe	Dropped File	Write, Create, Delete, Access	CLEAN
C:\Windows\system32\slui.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WTSAPI32.dll	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\WTSAPI32.dll	Dropped File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\slui.exe	Dropped File	Write, Create, Delete, Access	CLEAN
C:\Windows\system32\extrac32.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\at.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\NetEvtFwdr.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\wininit.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\gpupdate.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\rwinsta.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\tzutil.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\dllhst3g.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\mmc.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\RunLegacyCPLElevated.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\DpiScaling.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\AutoWorkplace.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\cmstp.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\VERSION.dll	Accessed File	Read, Access	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{0aa26147-58aa-e888-6782-4bac88c336bd}	access	pgdqqc.exe	CLEAN
{20974a93-a551-df17-8967-748358091d34}	access	pgdqqc.exe	CLEAN
{298ddcca-efe5-2f07-cbb5-e91e37797537}	access	explorer.exe	CLEAN
{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}	access	explorer.exe	CLEAN
{389fe546-d029-33a7-6305-2ca1cede0678}	access	explorer.exe	CLEAN
{e8b6fe55-d858-d6e4-ef99-a80106642ab4}	access	explorer.exe	CLEAN
{03b2a674-5295-21d6-da36-fc13faee0e98}	access	explorer.exe	CLEAN
{d439f686-d570-7182-3906-1e2d175d1088}	access	explorer.exe	CLEAN
{7d6ed4f3-6751-62a2-fd4a-b51cf5291b13}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{a73fffb8-61a4-f5fe-f3bf-f23b8e0debc2}	access	explorer.exe	CLEAN
{3e1c23ac-bb6d-7ca6-0ea0-2d76e5670962}	access	explorer.exe	CLEAN
{9b151509-5138-7d7a-187c-44a5c211ec53}	access	explorer.exe	CLEAN
{0f7daade-cabb-071c-b422-48138f19f093}	access	explorer.exe	CLEAN
{376aea27-53fd-bd89-7168-ab488bf01459}	access	explorer.exe	CLEAN
{8aadbf32-a058-ae7b-e2fa-32a552670e17}	access	explorer.exe	CLEAN
{11af7784-fda9-4020-881a-e50efb1e84cd}	access	explorer.exe	CLEAN
{96a8b4e8-9fb3-87d6-00d9-a27202e9fcb0}	access	explorer.exe	CLEAN
{153471c9-9d0a-7104-5275-71ac64b2065e}	access	explorer.exe	CLEAN
{347b949e-da97-ee8f-812b-2fca7cf89cb5}	access	explorer.exe	CLEAN
{19a9def8-7e87-44e0-b180-e8de92fad2a5}	access	explorer.exe	CLEAN
{25fdcad7-f614-d8db-5c91-5ebad4f4d05e}	access	explorer.exe	CLEAN
{633b0084-f455-d65f-7a89-5c7a238812c2}	access	explorer.exe	CLEAN
{95a1cd4d-d6fc-bfd3-3c8f-37dc107d2fca}	access	explorer.exe	CLEAN
{d89ae3f6-8bc6-6d82-7660-2578a416e6c0}	access	explorer.exe	CLEAN
{28d724ec-22da-95bd-9f65-2e17dc8aecd0}	access	explorer.exe	CLEAN
{fc269880-1f3e-c6d2-e541-ca3ff24ab1bc}	access	explorer.exe	CLEAN
{fe886e8c-a23d-7a39-eb2b-a2f6429f4e23}	access	explorer.exe	CLEAN
{b59ea4fc-7bc4-2dca-f7bf-d3e31efaff7e}	access	explorer.exe	CLEAN
{4236a99f-3514-853f-daf5-e82e3c1b0317}	access	explorer.exe	CLEAN
{e300a459-3dc2-cd5e-7ba3-52ae228e2e90}	access	explorer.exe	CLEAN
{acc1be65-c0b2-79a5-d2cb-9aa47275027b}	access	explorer.exe	CLEAN
{08936f51-fe02-2054-cc27-6952c80ac716}	access	explorer.exe	CLEAN
{13b3fa1d-d4bb-b7cc-c9f3-6fdf6b535b90}	access	explorer.exe	CLEAN
{9b8e3f9b-6a14-ba61-86de-29155d8b4094}	access	explorer.exe	CLEAN
{d87db754-0e49-5182-f0f9-ec9fe8dc9ec9}	access	explorer.exe	CLEAN
{58f5e2e3-5e83-a5a1-f2f1-1115b521ea00}	access	explorer.exe	CLEAN
{575fbde0-9713-efa5-165a-bc21541e4190}	access	explorer.exe	CLEAN
{f9bbbbdf-59be-1b9c-d32d-15c9687d5250}	access	explorer.exe	CLEAN
{c9a65329-61aa-8be1-61af-620ce6b5f66f}	access	explorer.exe	CLEAN
{38a99613-bfcc-7bdc-541b-9cece7db7691}	access	explorer.exe	CLEAN
{2899e51a-dd70-0150-e9f3-f3aba091c8e0}	access	explorer.exe	CLEAN
{daf86618-6ec6-d890-7978-8720661e5a12}	access	explorer.exe	CLEAN
{362882c5-03e2-fd0f-928d-c1120ad9c64f}	access	explorer.exe	CLEAN
{a3dce688-6117-3ea3-fbbd-1defec717462}	access	explorer.exe	CLEAN
{39fed215-396f-cbc9-07b5-5de635b0306d}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{35222349-38a9-6107-aeba-d926ff73ead9}	access	explorer.exe	CLEAN
{168ee11b-299f-6d76-b48f-88a65a4a58ba}	access	explorer.exe	CLEAN
{01f24baa-a48c-b675-d94f-c4d185fa1b74}	access	explorer.exe	CLEAN
{60d53e50-c02a-fd11-36ca-0f91b9ec3738}	access	explorer.exe	CLEAN
{6ec5b40a-313e-69df-1ad2-48a8055c5743}	access	explorer.exe	CLEAN
{f7677ce1-197d-c706-bc9e-7239a2ec86e1}	access	explorer.exe	CLEAN
{6c570128-9202-fd64-daa4-72143d141e8a}	access	explorer.exe	CLEAN
{6a858a42-f46d-62bb-e142-0d99eeaf1f91}	access	explorer.exe	CLEAN
{583163e6-97f6-ca24-26b7-ae90d9895822}	access	explorer.exe	CLEAN
{64627196-149f-ef44-f53e-7c34ad6e86ef}	access	explorer.exe	CLEAN
{3fbd1d29-8e3d-a98d-695d-e7a831663d04}	access	explorer.exe	CLEAN
{fef37f2e-4f56-9012-852a-59484b5fed7e}	access	explorer.exe	CLEAN
{53be0c1d-6845-1fb9-9acf-69f1a3b7921b}	access	explorer.exe	CLEAN
{a4165b4a-bfe7-c4c5-3fb8-0a45db645781}	access	explorer.exe	CLEAN
{74cce2f8-af0d-c651-67a5-40d9130ec8dd}	access	explorer.exe	CLEAN
{985469d5-c515-9b89-778a-6ffac4b9b8b4}	access	explorer.exe	CLEAN
{e722aca1-f311-7487-c06a-2f0c9ed96cf8}	access	explorer.exe	CLEAN
{03493065-186f-661d-33ee-0c047dee9701}	access	explorer.exe	CLEAN
{497f1ddf-1131-8869-1c4d-19bc3c1533f0}	access	explorer.exe	CLEAN
{66f88062-bc56-b7bd-5e68-f476f8966290}	access	explorer.exe	CLEAN
{867eeaaa-9095-7d70-5174-9d6e7d728884}	access	explorer.exe	CLEAN
{1da4e1aa-6eb1-9190-a173-cc15c94ce697}	access	explorer.exe	CLEAN
{6a211e2f-1816-7b61-9139-24d5eb1a6e7a}	access	explorer.exe	CLEAN
{f9e73e00-f006-b49c-1dcf-ff85215b0c68}	access	explorer.exe	CLEAN
{6a4fe6c6-ce4d-1240-9924-4da205e310d4}	access	explorer.exe	CLEAN
{1bb6559c-a5ac-9df0-25de-8fc72fd80084}	access	explorer.exe	CLEAN
{14001fd5-42cb-a1e0-69b0-ab1633b2ae68}	access	explorer.exe	CLEAN
{45dc20d3-ad5e-b36d-80bb-cdcf7f417d73}	access	explorer.exe	CLEAN
{be160789-1fd9-ee8b-3528-3c09aeed0e96}	access	explorer.exe	CLEAN
{9bb57762-c68f-429c-9055-03f563f40f7c}	access	explorer.exe	CLEAN
{160d8ed2-0c45-c326-55b4-6c19e536f3e8}	access	explorer.exe	CLEAN
{17ea73bb-2d34-5bfd-182b-48b512b10749}	access	explorer.exe	CLEAN
{394a7c3c-ac56-58ce-d288-876ad1f16f45}	access	explorer.exe	CLEAN
{ff93c05d-33bd-c55e-00a2-880e7d7aae13}	access	explorer.exe	CLEAN
{66b318fe-548d-18e8-5507-9aae7f394fb4}	access	explorer.exe	CLEAN
{946d3aec-f0be-460d-b2db-c49c07ac46ae}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{05ed4310-2ecc-f984-b4f8-cedb1e8137f4}	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
-	create, access	pgdqqc.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE	access	pgdqqc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE	access	pgdqqc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft	access	pgdqqc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT	access	pgdqqc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	pgdqqc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate	read, access	pgdqqc.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows	access	pgdqqc.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion	access	pgdqqc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\EnableLUA	read, access	pgdqqc.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ConsentPromptBehaviorAdmin	read, access	pgdqqc.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\PromptOnSecureDesktop	read, access	pgdqqc.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	access	pgdqqc.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	access	pgdqqc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	read, access	pgdqqc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin	read, access	pgdqqc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop	read, access	pgdqqc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8C45A918-B075-FEF6-0DED-B5C899623EB0}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{61E3425B-6B05-A459-B4FE-174B2D84DE94}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{026F08C5-341A-9406-8117-0A9B26B9732B}\ShellFolder	create, access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InstallDate	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{98DFD738-1E78-D107-2616-FA30049BD427}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows\CurrentVersion	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows\CurrentVersion\Explorer	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{1384CAC3-17AC-E069-EB5C-4E613FCC6FE4}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\InstallDate	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows\CurrentVersion\InstallDate	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows\CurrentVersion\Explorer\InstallDate	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\InstallDate	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5CFB38CB-4922-AAF5-9C1E-F3F5A6338105}\ShellFolder	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5CFB38CB-4922-AAF5-9C1E-F3F5A6338105}\ShellFolder\{94F2B622-91AF-D4F6-BB5D-6051D2178CFF}	write, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder\{E1FF0420-B57E-0749-C88B-2A39F95180B3}	write, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\InstallDate	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail\Microsoft Outlook	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail\Microsoft Outlook\DllPathEx	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{61E3425B-6B05-A459-B4FE-174B2D84DE94}\ShellFolder\{DD4B594C-5D5B-1375-55F8-84E364592B6A}	write, access	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
sysreseterr.exe	C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\SysResetErr.exe	MALICIOUS
lockapphost.exe	C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\LockAppHost.exe	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpzpfphz26" /s	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=AddGadgetMessageHandler	CLEAN

Process Name	Commandline	Verdict
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=AddLayeredRef	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=AdjustClipInsideRef	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=AttachWndProcA	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=AttachWndProcW	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=AutoTrace	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=BeginHideInputPaneAnimation	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=BeginShowInputPaneAnimation	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=BuildAnimation	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=BuildDropTarget	CLEAN
sysreseterr.exe	C:\Windows\system32\SysResetErr.exe	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=BuildInterpolation	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=CacheDWriteRenderTarget	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=ChangeCurrentAnimationScenario	CLEAN
mspaint.exe	C:\Windows\system32\mspaint.exe	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=ClearPushedOpacitiesFromGadgetTree	CLEAN
mspaint.exe	C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\mspaint.exe	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=ClearTopmostVisual	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 4256 -s 360	CLEAN
rdpinput.exe	C:\Windows\system32\rdpinput.exe	CLEAN
lockapphost.exe	C:\Windows\system32\LockAppHost.exe	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=CreateAction	CLEAN
slui.exe	C:\Windows\system32\slui.exe	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=CreateGadget	CLEAN
slui.exe	C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\slui.exe	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=CustomGadgetHitTestQuery	CLEAN

Process Name	Commandline	Verdict
mmc.exe	C:\Windows\system32\mmc.exe	CLEAN
cmstp.exe	C:\Windows\system32\cmstp.exe	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=DUserBuildGadget	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=DUserCastClass	CLEAN
pgdqqc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PgdqQc.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll" /fn_id=DUserCastDirect	CLEAN

YARA / AV

Antivirus (15)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\Desktop\ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b.exe.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\AppData\Local\kb3\DUI70.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\AppData\Local\WMyxekaE9\MFC42u.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\AppData\Local\zDy8y\DUser.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\AppData\Local\T6GEH01\WTSAPI32.dll	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	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