MALICIOUS

Classifications: Spyware

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

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll**
ID	#2782718
MD5	f8295446e335b679641637334c99242d
SHA1	18b9a40791f1a52c70507b29d0b631510f2e33c6
SHA256	96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9
File Size	2180.00 KB
Report Created	2021-09-28 13:14 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (11 rules, 99 matches)

Score	Category	Operation	Count	Classification
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #2) rgqzicu.exe alters context of (process #5) explorer.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	4	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #2) rgqzicu.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #5) explorer.exe as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #9) rgqzicu.exe as "Gen:Variant.Mikey.113998".			
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #5) explorer.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #5) explorer.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #5) explorer.exe has a thread which sleeps more than 5 minutes.			
1/5	Discovery	Reads system data	6	-
	• (Process #2) rgqzicu.exe reads the Windows installation date from registry. • (Process #3) rgqzicu.exe reads the Windows installation date from registry. • (Process #4) rgqzicu.exe reads the Windows installation date from registry. • (Process #6) rgqzicu.exe reads the Windows installation date from registry. • (Process #7) rgqzicu.exe reads the Windows installation date from registry. • (Process #5) explorer.exe reads the Windows installation date from registry.			
1/5	Mutex	Creates mutex	81	-

- (Process #2) rgqzicu.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #2) rgqzicu.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #3) rgqzicu.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #4) rgqzicu.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #6) rgqzicu.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #7) rgqzicu.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #5) explorer.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #5) explorer.exe creates mutex with name "{298ddcca-efe5-2f07-cbb5-e91e37797537}".
- (Process #5) explorer.exe creates mutex with name "{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}".
- (Process #5) explorer.exe creates mutex with name "{2fb46568-32c9-06dc-d0b5-f1ab83aee93b}".
- (Process #5) explorer.exe creates mutex with name "{e8353f60-b296-77d3-712c-682bf3e23f29}".
- (Process #5) explorer.exe creates mutex with name "{25390bbd-f8e2-0cdc-c922-ea2f65111ff1}".
- (Process #5) explorer.exe creates mutex with name "{3efe96e0-aada-6cdc-4854-db5a860aa498}".
- (Process #5) explorer.exe creates mutex with name "{07854ab8-d7ab-8463-c8a4-b76bc68ea3f8}".
- (Process #5) explorer.exe creates mutex with name "{47862a83-7903-9f79-1a0f-4a84f706a67b}".
- (Process #5) explorer.exe creates mutex with name "{834a16cd-8577-dafc-374f-5cc03abf6fd0}".
- (Process #5) explorer.exe creates mutex with name "{70f81a58-e1d1-bdc6-b9d8-56d2655f0a24}".
- (Process #5) explorer.exe creates mutex with name "{8d1bc1d3-ef74-6f36-473a-76cde4cb3d47}".
- (Process #5) explorer.exe creates mutex with name "{0b20e235-b4b6-7fec-73bc-29f7c8afd7c3}".
- (Process #5) explorer.exe creates mutex with name "{c56bfebc-07d0-407d-cbe5-cb676ed93a41}".
- (Process #5) explorer.exe creates mutex with name "{e78cb100-e225-784c-5efb-3387830a6236}".
- (Process #5) explorer.exe creates mutex with name "{cdac0f5b-6ff9-2ff1-eae0-d785678bb550}".
- (Process #5) explorer.exe creates mutex with name "{96a8b4e8-9fb3-87d6-00d9-a27202e9fcb0}".
- (Process #5) explorer.exe creates mutex with name "{7cc7f05f-d1e7-4c02-9550-b3b0d22630c1}".
- (Process #5) explorer.exe creates mutex with name "{a137fbc8-158c-502e-14a9-c5fb1fc89200}".
- (Process #5) explorer.exe creates mutex with name "{13b3fa1d-d4bb-b7cc-c9f3-6fdf6b535b90}".
- (Process #5) explorer.exe creates mutex with name "{2e3acbd9-86c3-6d1d-162b-fd78140d46b4}".
- (Process #5) explorer.exe creates mutex with name "{2e6aa22d-bdb0-484a-3826-fb080adf07f8}".
- (Process #5) explorer.exe creates mutex with name "{c2932214-8c85-76a4-7832-abffc3d4e344}".
- (Process #5) explorer.exe creates mutex with name "{3f962b47-4d0a-da84-a641-0744d03cca5e}".
- (Process #5) explorer.exe creates mutex with name "{bf2dfecf-9cce-a068-c413-79c5d4e13d28}".
- (Process #5) explorer.exe creates mutex with name "{0543b54c-df93-6503-0f5f-03111d930d96}".
- (Process #5) explorer.exe creates mutex with name "{71dba081-a28d-be08-fa55-bf22ddb35cb9}".
- (Process #5) explorer.exe creates mutex with name "{723617d4-b898-1019-fc4e-58f72e97f0e8}".
- (Process #5) explorer.exe creates mutex with name "{6712a992-54f7-9e39-c636-e9e98ff9182c}".
- (Process #5) explorer.exe creates mutex with name "{742c4235-61f7-6f13-cec8-924c395053dd}".
- (Process #5) explorer.exe creates mutex with name "{f2947db2-76ce-20cf-3821-b4e020fbf40d}".
- (Process #5) explorer.exe creates mutex with name "{83d2f837-aafd-e34e-af7e-1aa680eb08c8}".
- (Process #5) explorer.exe creates mutex with name "{0b7ba948-3cca-a9ee-ef68-bca12f0e84a2}".
- (Process #5) explorer.exe creates mutex with name "{45d7bc7c-5d8d-3d92-b257-6c94926a1756}".
- (Process #5) explorer.exe creates mutex with name "{1fd4ce32-1652-23b5-f64f-63e609c14ad1}".
- (Process #5) explorer.exe creates mutex with name "{633b0084-f455-d65f-7a89-5c7a238812c2}".
- (Process #5) explorer.exe creates mutex with name "{ac6ced00-3f82-50bc-3836-09b4162a8a23}".
- (Process #5) explorer.exe creates mutex with name "{dbd86cc3-ce57-ee06-8a30-e3ab4352d687}".
- (Process #5) explorer.exe creates mutex with name "{d05d4038-ac1b-920e-67e9-93d0f90020fa}".
- (Process #5) explorer.exe creates mutex with name "{aadb65f8-5aae-bb01-afa3-e769be98792f}".
- (Process #5) explorer.exe creates mutex with name "{176a93eb-d636-4841-39a9-d3a6d4c92b27}".
- (Process #5) explorer.exe creates mutex with name "{ed9037cf-84b5-6f0c-01db-1f89943b4ec1}".
- (Process #5) explorer.exe creates mutex with name "{085452ff-38fe-d18a-56ea-bc278c02b894}".
- (Process #5) explorer.exe creates mutex with name "{5966af2b-3b83-75fd-a06a-71ed28dac8fc}".
- (Process #5) explorer.exe creates mutex with name "{40abb0bc-1059-4ed5-7e80-3532ddff1c1b}".
- (Process #5) explorer.exe creates mutex with name "{a2e3a1c4-1044-26ac-2fa3-30ee391a0657}".
- (Process #5) explorer.exe creates mutex with name "{01f24baa-a48c-b675-d94f-c4d185fa1b74}".
- (Process #5) explorer.exe creates mutex with name "{7e5d2be3-0634-bb96-47ee-3083eb9bef97}".
- (Process #5) explorer.exe creates mutex with name "{ad578bd5-3c50-f523-98ef-c00bb2e8cdcd}".
- (Process #5) explorer.exe creates mutex with name "{3c33918e-27da-9f35-2586-b9f012933134}".
- (Process #5) explorer.exe creates mutex with name "{6c570128-9202-fd64-daa4-72143d141e8a}".
- (Process #5) explorer.exe creates mutex with name "{6a858a42-f46d-62bb-e142-0d99eeaf1f91}".
- (Process #5) explorer.exe creates mutex with name "{476e628c-b7ac-454c-9d23-569675a51104}".
- (Process #5) explorer.exe creates mutex with name "{a05f0639-d54b-7c4f-c3f7-6ad4daa512b6}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #2) rgqzicu.exe reads from (process #5) explorer.exe.			
1/5	Hide Tracks	Writes an unusually large amount of data to the registry	1	-
	• (Process #5) explorer.exe hides 3526 bytes in "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{61E3425B-6B05-A459-B4FE-174B2D84DE94}\ShellFolder\{E0B5E69C-4155-78B2-8F46-4AE033942ED8}".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #5) explorer.exe resolves 26 API functions by name.			

Mitre ATT&CK Matrix

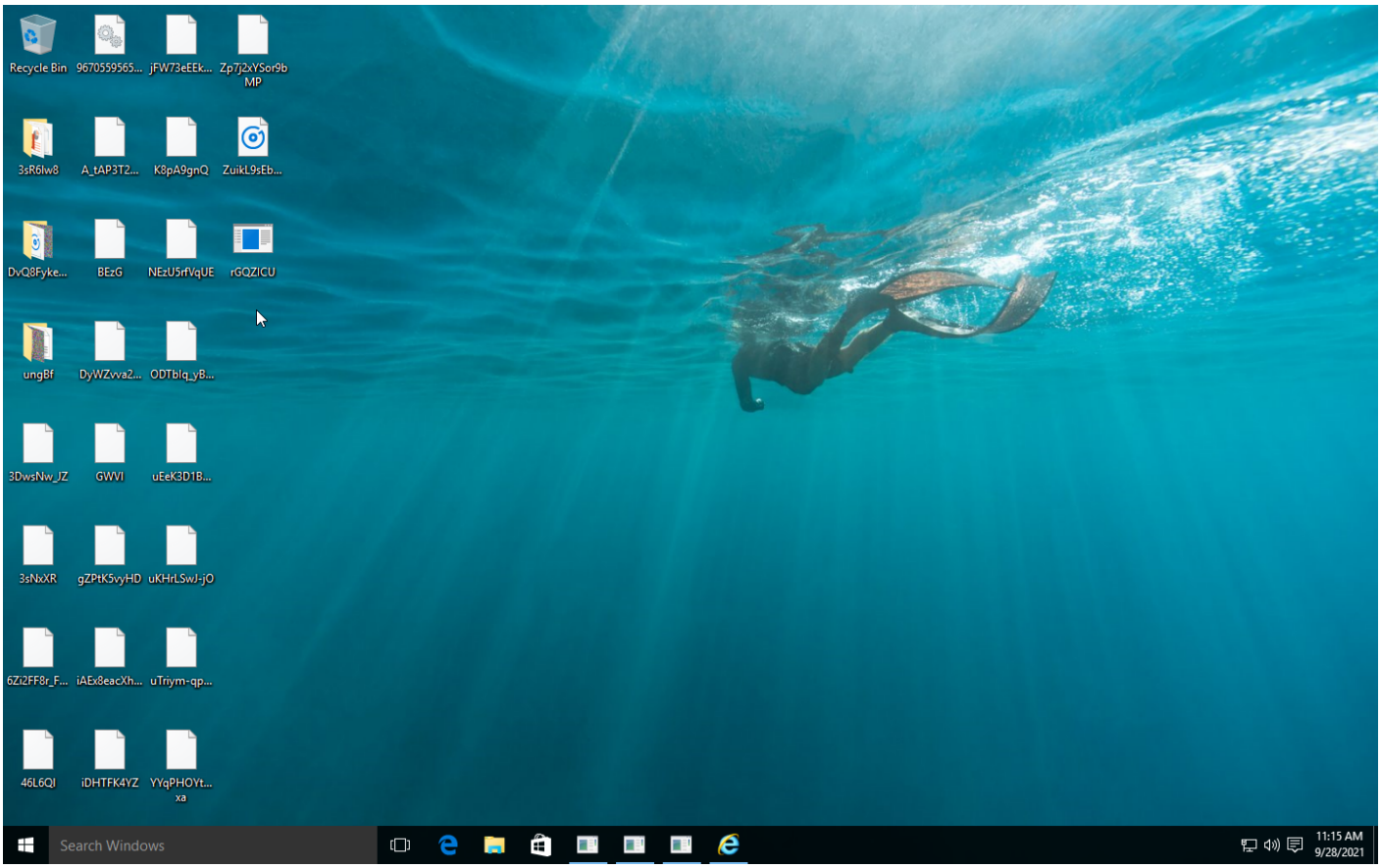
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1112 Modify Registry	#T1081 Credentials in Files	#T1082 System Information Discovery		#T1119 Automated Collection			
				#T1045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

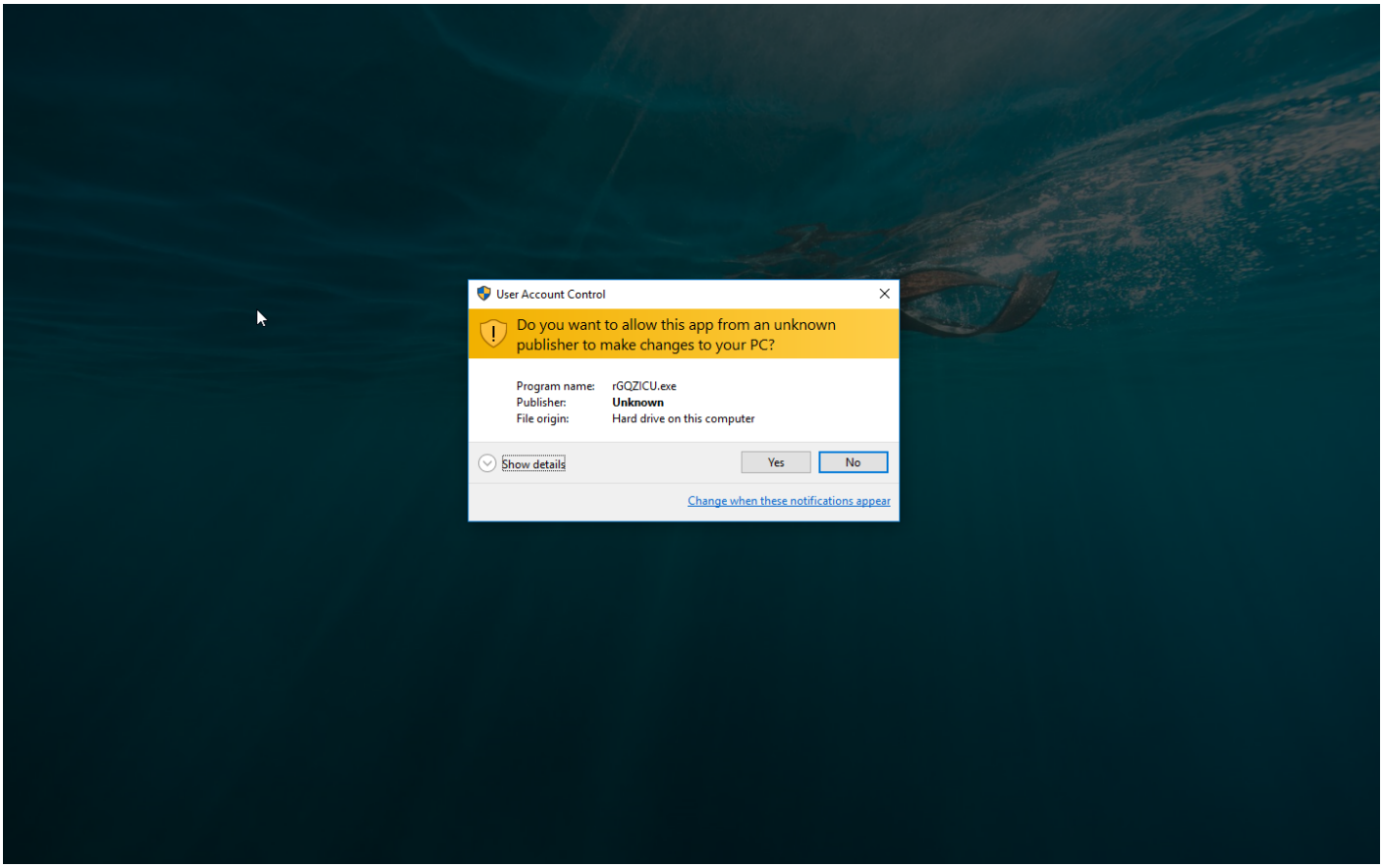
Sample Information

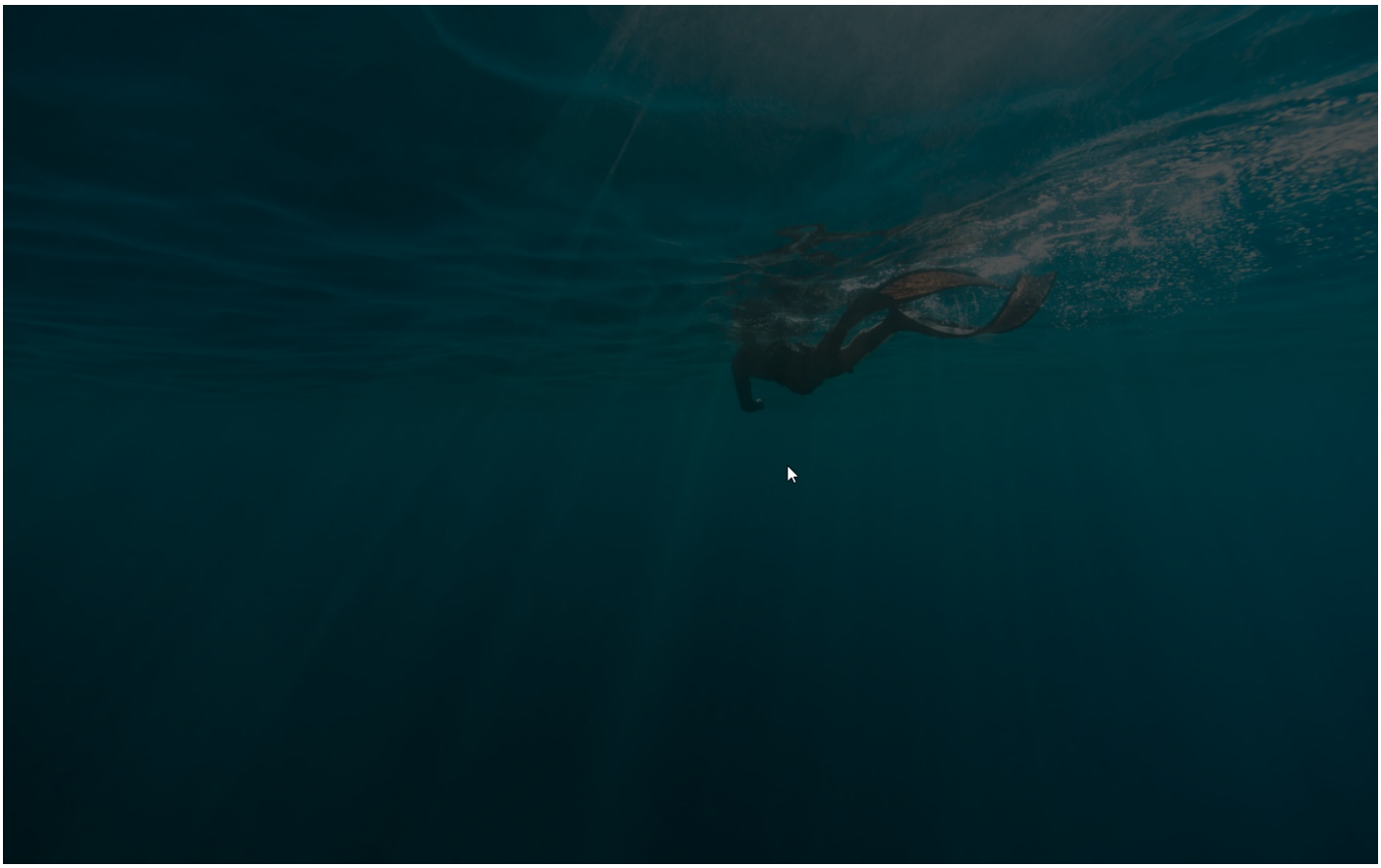
ID	#2782718
MD5	f8295446e335b679641637334c99242d
SHA1	18b9a40791f1a52c70507b29d0b631510f2e33c6
SHA256	96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9
SSDeep	12288:/VI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:2fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
ImpHash	6668be91e2c948b183827f040944057f
File Name	96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll
File Size	2180.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 13:14 (UTC+2)
Analysis Duration	00:03:58
Termination Reason	Maximum binlog size reached
Number of Monitored Processes	13
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✓
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	4
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
9670559565...
jFW73eEEk...
Zp7j2xYSor9bMP
3sR6lw8
A_tAP3T2...
K8pA9gnQ
ZuikL9sEb...
DvQ8Fyke...
BEzG
NEzU5rfVqUE
rGQZICU
ungBf
DyWZvva2...
ODTblq_yB...
3DwsNw_JZ
GWVI
uEeK3D1B...
3sNxXR
gZPtK5vyHD
uKHrLSwJ-jO
6Zi2FF8r_F...
iAEx8eacXh...
uTriym-qp...
46L6QI
iDHTFK4YZ
YYqPHOYt...xa
Search Windows
11:15 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: rGQZICU.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



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

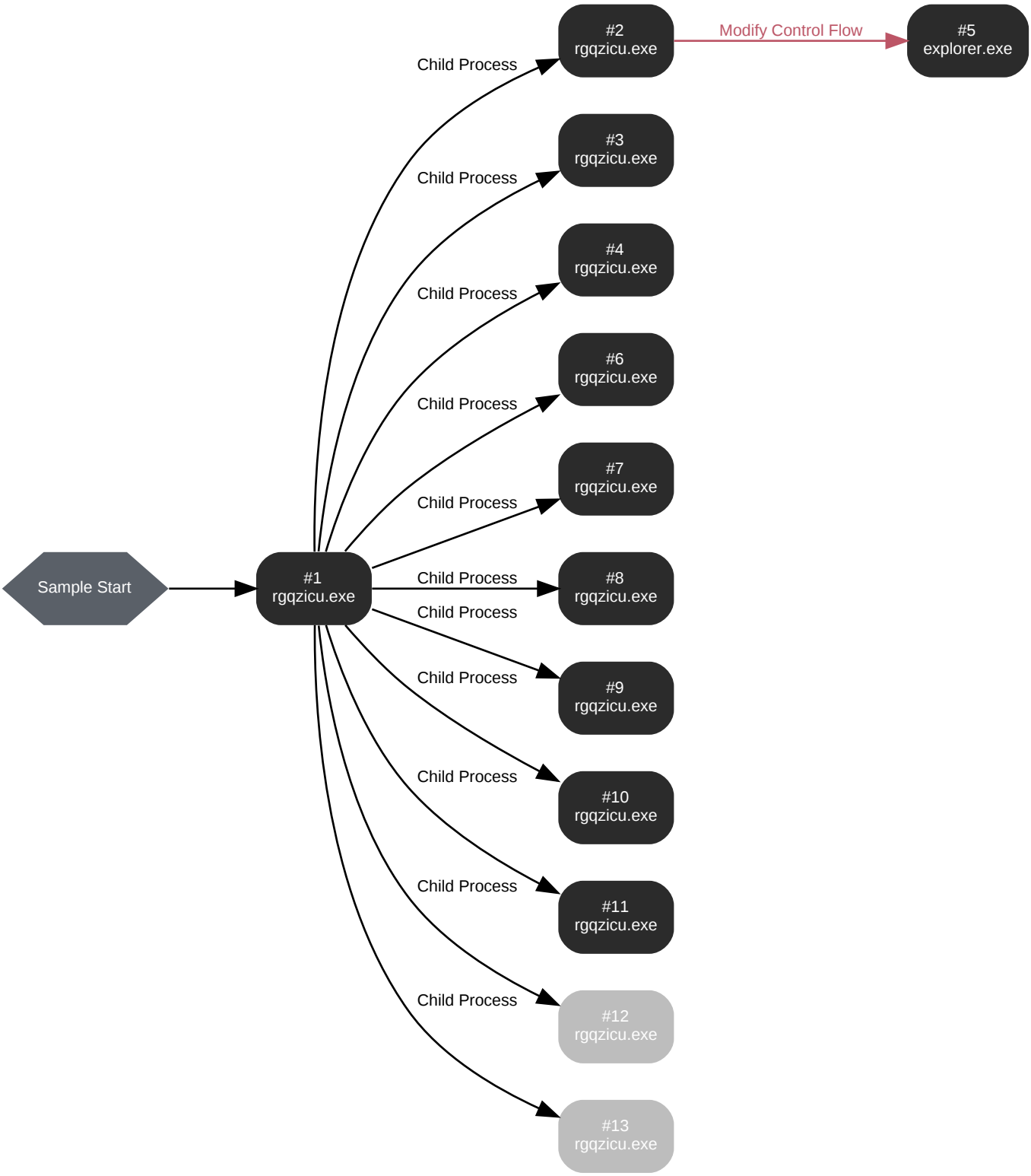
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: rgqzicu.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpt36r42xw" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 68448, Reason: Analysis Target
Unmonitor End Time	End Time: 307188, Reason: Terminated by Timeout
Monitor duration	238.74s
Return Code	Unknown
PID	1688
Parent PID	1600
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	6
Environment	1
Process	12

Process #2: rgqzicu.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxFreeMemory
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 92326, Reason: Child Process
Unmonitor End Time	End Time: 178429, Reason: Terminated
Monitor duration	86.10s
Return Code	0
PID	3088
Parent PID	1688
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	44
Environment	2
Registry	768
Mutex	6
Process	2
-	112
-	40
-	201

Process #3: rgqzicu.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxNewJob
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 94650, Reason: Child Process
Unmonitor End Time	End Time: 102674, Reason: Terminated
Monitor duration	8.02s
Return Code	0
PID	1708
Parent PID	1688
Bitness	64 Bit

Host Behavior

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

Process #4: rgqzicu.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C: \Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxNewJobEx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 96971, Reason: Child Process
Unmonitor End Time	End Time: 106244, Reason: Terminated
Monitor duration	9.27s
Return Code	0
PID	2524
Parent PID	1688
Bitness	64 Bit

Host Behavior

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

Process #5: explorer.exe

ID	5
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 101189, Reason: Injection
Unmonitor End Time	End Time: 307188, Reason: Terminated by Timeout
Monitor duration	206.00s
Return Code	Unknown
PID	1600
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (145)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x644	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x684	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x688	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x6b8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x6c8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x6d0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x6d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x6f0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x710	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x728	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x73c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x75c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x764	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x768	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x774	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x7a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x7b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xa9c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xb94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xbf8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xbfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x8b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x5d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x8bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x928	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xe30	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xe64	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xfb4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xfe4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xc38	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xc20	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xb14	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x228	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x690	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x750	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x778	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x118c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x1190	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x1194	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x11a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x1224	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x122c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x1230	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x1268	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x1288	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x128c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x12a0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x12c0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x13b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xcfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x688	0x7ffb28bab580(140716696843648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x688	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x688	0x7ffb2623ce60(140716653399648)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x688	0x7ffb2623ce60(140716653 399648)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x688	0x7ffb2623ce60(140716653 399648)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x688	0x7ffb2623ce60(140716653 399648)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x688	0x7ffb2623ce60(140716653 399648)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x688	0x7ffb2623ce60(140716653 399648)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x688	0x7ffb2623ce60(140716653 399648)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x644	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x684	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x68c	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x69c	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x6a4	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x6a8	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x6b4	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x6b8	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x6c8	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x6d0	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x6d4	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x6f0	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x710	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x728	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x73c	0x7ffb28ba4f00(1407166968 17408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x75c	0x7ffb28ba4f00(1407166968 17408)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x764	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x768	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x774	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x7a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x7b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xa9c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xb94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xbf8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xbfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x8b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x5d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x8bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x928	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xe30	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xe64	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xfb4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xfe4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xc38	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xc20	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0xb14	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x228	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x690	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x750	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x778	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x118c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x1190	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x1194	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x11a8	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x1224	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x122c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x1230	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x1268	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x1288	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x128c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x12a0	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x12c0	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x13b0	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0xcfc	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x688	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c: \users\rdhj0cnfevzx\desktop \rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb28bab580(140716696843648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe	0x11f4 / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
-	53 bytes	e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	✗
-	1.42 KB	7c5c06b5ed49695fcd156c005970535abc60cfa5ae50f4bbee035717016437e7	✗
-	1.42 KB	4459de34f31d879717f63fcf0b48c4b322ee763c7e60d4b0e2a2a61a7805cf43	✗
-	1.42 KB	33a74144f3a4f82bdf6f7c94a6639df405ed84200d2a88d6168b4aebc613ef6d	✗

Host Behavior

Type	Count
Module	48
File	171
System	483
Process	101
Registry	25174
Environment	2
-	21
Mutex	1797

Process #6: rgqzicu.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxRestoreJob
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 103216, Reason: Child Process
Unmonitor End Time	End Time: 110107, Reason: Terminated
Monitor duration	6.89s
Return Code	0
PID	1660
Parent PID	1688
Bitness	64 Bit

Host Behavior

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

Process #7: rgqzicu.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxRestoreJobEx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 106246, Reason: Child Process
Unmonitor End Time	End Time: 157056, Reason: Terminated
Monitor duration	50.81s
Return Code	0
PID	4740
Parent PID	1688
Bitness	64 Bit

Host Behavior

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

Process #8: rgqzicu.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxFreeMemory /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 109483, Reason: Child Process
Unmonitor End Time	End Time: 307188, Reason: Terminated by Timeout
Monitor duration	197.71s
Return Code	Unknown
PID	828
Parent PID	1688
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #9: rgqzicu.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxNewJob /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 206454, Reason: Child Process
Unmonitor End Time	End Time: 307188, Reason: Terminated by Timeout
Monitor duration	100.73s
Return Code	Unknown
PID	4584
Parent PID	1688
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #10: rgqzicu.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxNewJobEx /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 255501, Reason: Child Process
Unmonitor End Time	End Time: 307188, Reason: Terminated by Timeout
Monitor duration	51.69s
Return Code	Unknown
PID	176
Parent PID	1688
Bitness	64 Bit

Host Behavior

Type	Count
Module	15
File	3
Environment	1

Process #11: rgqzicu.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxRestoreJob /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 285086, Reason: Child Process
Unmonitor End Time	End Time: 307188, Reason: Terminated by Timeout
Monitor duration	22.10s
Return Code	Unknown
PID	2696
Parent PID	1688
Bitness	64 Bit

Host Behavior

Type	Count
Module	11

Process #12: rgqzicu.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxRestoreJobEx /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 291324, Reason: Child Process
Unmonitor End Time	End Time: 307188, Reason: Terminated by Timeout
Monitor duration	15.86s
Return Code	Unknown
PID	3760
Parent PID	1688
Bitness	64 Bit

Process #13: rgqzicu.exe

ID	13
File Name	c:\users\rdhj0cnfevzx\desktop\rgqzicu.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxFreeMemory /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 297915, Reason: Child Process
Unmonitor End Time	End Time: 307188, Reason: Terminated by Timeout
Monitor duration	9.27s
Return Code	Unknown
PID	3984
Parent PID	1688
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9	C:\Users\RDhJ0CNFevzX\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll, C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll	Sample File	2180.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
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
7c5c06b5ed49695fcd156c005970535abc60cfa5ae50f4bbee035717016437e7	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
33a74144f3a4f82bdf6f7c94a6639df405ed84200d2a88d6168b4aebc613ef6d	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\rGQZICU.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpt36r42xw	Accessed File	Access, Read	CLEAN
C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll	Accessed File	Access, Read	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\Explorer.EXE	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesCommonX86\system\msmapi\1033\msmapi32.dll	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\Reference Assemblies\outlook.exe	Accessed File	Access, Read	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

Mutex

Name	Operations	Parent Process Name	Verdict
{0aa26147-58aa-e888-6782-4bac88c336bd}	access	rgqzicu.exe	CLEAN
{54137ce8-d76d-e7fc-dec3-c85f290e5b98}	access	rgqzicu.exe	CLEAN
{298ddcca-efe5-2f07-cbb5-e91e37797537}	access	explorer.exe	CLEAN
{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}	access	explorer.exe	CLEAN
{2fb46568-32c9-06dc-d0b5-f1ab83aee93b}	access	explorer.exe	CLEAN
{e8353f60-b296-77d3-712c-682bf3e23f29}	access	explorer.exe	CLEAN
{25390bbd-f8e2-0cdc-c922-ea2f65111ff1}	access	explorer.exe	CLEAN
{3efe96e0-aada-6cdc-4854-db5a860aa498}	access	explorer.exe	CLEAN
{07854ab8-d7ab-8463-c8a4-b76bc68ea3f8}	access	explorer.exe	CLEAN
{47862a83-7903-9f79-1a0f-4a84f706a67b}	access	explorer.exe	CLEAN
{834a16cd-8577-dafc-374f-5cc03abf6fd0}	access	explorer.exe	CLEAN
{70f81a58-e1d1-bdc6-b9d8-56d2655f0a24}	access	explorer.exe	CLEAN
{8d1bc1d3-ef74-6f36-473a-76cde4cb3d47}	access	explorer.exe	CLEAN
{0b20e235-b4b6-7fec-73bc-29f7c8afd7c3}	access	explorer.exe	CLEAN
{c56bfebc-07d0-407d-cbe5-cb676ed93a41}	access	explorer.exe	CLEAN
{e78cb100-e225-784c-5efb-3387830a6236}	access	explorer.exe	CLEAN
{cdac0f5b-6ff9-2ff1-eae0-d785678bb550}	access	explorer.exe	CLEAN
{96a8b4e8-9fb3-87d6-00d9-a27202e9fcb0}	access	explorer.exe	CLEAN
{7cc7f05f-d1e7-4c02-9550-b3b0d22630c1}	access	explorer.exe	CLEAN
{a137fbc8-158c-502e-14a9-c5fb1fc89200}	access	explorer.exe	CLEAN
{13b3fa1d-d4bb-b7cc-c9f3-6fdf6b535b90}	access	explorer.exe	CLEAN
{2e3acbd9-86c3-6d1d-162b-fd78140d46b4}	access	explorer.exe	CLEAN
{2e6aa22d-bdb0-484a-3826-fb080adf07f8}	access	explorer.exe	CLEAN
{c2932214-8c85-76a4-7832-abffc3d4e344}	access	explorer.exe	CLEAN
{3f962b47-4d0a-da84-a641-0744d03cca5e}	access	explorer.exe	CLEAN
{bf2dfecf-9cce-a068-c413-79c5d4e13d28}	access	explorer.exe	CLEAN
{0543b54c-df93-6503-0f5f-03111d930d96}	access	explorer.exe	CLEAN
{71dba081-a28d-be08-fa55-bf22ddb35cb9}	access	explorer.exe	CLEAN
{723617d4-b898-1019-fc4e-58f72e97f0e8}	access	explorer.exe	CLEAN
{6712a992-54f7-9e39-c636-e9e98ff9182c}	access	explorer.exe	CLEAN
{742c4235-61f7-6f13-cec8-924c395053dd}	access	explorer.exe	CLEAN
{f2947db2-76ce-20cf-3821-b4e020fbf40d}	access	explorer.exe	CLEAN
{83d2f837-aafd-e34e-af7e-1aa680eb08c8}	access	explorer.exe	CLEAN
{0b7ba948-3cca-a9ee-ef68-bca12f0e84a2}	access	explorer.exe	CLEAN
{45d7bc7c-5d8d-3d92-b257-6c94926a1756}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{1fd4ce32-1652-23b5-f64f-63e609c14ad1}	access	explorer.exe	CLEAN
{633b0084-f455-d65f-7a89-5c7a238812c2}	access	explorer.exe	CLEAN
{ac6ced00-3f82-50bc-3836-09b4162a8a23}	access	explorer.exe	CLEAN
{dbd86cc3-ce57-ee06-8a30-e3ab4352d687}	access	explorer.exe	CLEAN
{d05d4038-ac1b-920e-67e9-93d0f90020fa}	access	explorer.exe	CLEAN
{aadb65f8-5aae-bb01-afa3-e769be98792f}	access	explorer.exe	CLEAN
{176a93eb-d636-4841-39a9-d3a6d4c92b27}	access	explorer.exe	CLEAN
{ed9037cf-84b5-6f0c-01db-1f89943b4ec1}	access	explorer.exe	CLEAN
{085452ff-38fe-d18a-56ea-bc278c02b894}	access	explorer.exe	CLEAN
{5966af2b-3b83-75fd-a06a-71ed28dac8fc}	access	explorer.exe	CLEAN
{40abb0bc-1059-4ed5-7e80-3532ddff1c1b}	access	explorer.exe	CLEAN
{a2e3a1c4-1044-26ac-2fa3-30ee391a0657}	access	explorer.exe	CLEAN
{01f24baa-a48c-b675-d94f-c4d185fa1b74}	access	explorer.exe	CLEAN
{7e5d2be3-0634-bb96-47ee-3083eb9bef97}	access	explorer.exe	CLEAN
{ad578bd5-3c50-f523-98ef-c00bb2e8cdcd}	access	explorer.exe	CLEAN
{3c33918e-27da-9f35-2586-b9f012933134}	access	explorer.exe	CLEAN
{6c570128-9202-fd64-daa4-72143d141e8a}	access	explorer.exe	CLEAN
{6a858a42-f46d-62bb-e142-0d99eeaf1f91}	access	explorer.exe	CLEAN
{476e628c-b7ac-454c-9d23-569675a51104}	access	explorer.exe	CLEAN
{a05f0669-d546-7c4b-c5ff-6ad44aa5f2b6}	access	explorer.exe	CLEAN
{fd7ca6f8-1404-d767-4318-5ce05ac233ab}	access	explorer.exe	CLEAN
{64627196-149f-ef44-f53e-7c34ad6e86ef}	access	explorer.exe	CLEAN
{ede07ea5-2e12-7d74-5185-75bb288d7c70}	access	explorer.exe	CLEAN
{b707c8db-10a1-da7e-58a9-0531358e4e63}	access	explorer.exe	CLEAN
{a4165b4a-bfe7-c4c5-3fb8-0a45db645781}	access	explorer.exe	CLEAN
{4055b8dd-d64d-bfbf-12c7-e1fd01a226ba}	access	explorer.exe	CLEAN
{1439a690-60db-c7ba-74ad-63f3b3396ce4}	access	explorer.exe	CLEAN
{e722aca1-f311-7487-c06a-2f0c9ed96cf8}	access	explorer.exe	CLEAN
{469a5cd7-873f-8a0b-58df-c06ad65a1566}	access	explorer.exe	CLEAN
{946d3aec-f0be-460d-b2db-c49c07ac46ae}	access	explorer.exe	CLEAN
{b894408f-30d6-e44c-93a0-15251ca9bab4}	access	explorer.exe	CLEAN
{497f1ddf-1131-8869-1c4d-19bc3c1533f0}	access	explorer.exe	CLEAN
{66f88062-bc56-b7bd-5e68-f476f8966290}	access	explorer.exe	CLEAN
{1da4e1aa-6eb1-9190-a173-cc15c94ce697}	access	explorer.exe	CLEAN
{6a211e2f-1816-7b61-9139-24d5eb1a6e7a}	access	explorer.exe	CLEAN
{69d53eb4-a66f-0ded-c220-8d4dd3c77fd2}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{fdb83606-4ef7-5a58-ba85-687f05c6dbcf}	access	explorer.exe	CLEAN
{205d5366-f15a-2f49-d587-0637683a4897}	access	explorer.exe	CLEAN
{b40a23fb-61b0-e9b8-fa7e-358ab19faa31}	access	explorer.exe	CLEAN
{456ac938-8006-3bbb-dd85-06e6e8271668}	access	explorer.exe	CLEAN
{bbe712f6-5e32-f9e6-bb54-9a2f43b77a6d}	access	explorer.exe	CLEAN

Registry

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

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8C45A918-B075-FEF6-0DED-B5C899623EB0}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{61E3425B-6B05-A459-B4FE-174B2D84DE94}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{026F08C5-341A-9406-8117-0A9B26B9732B}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{98DFD738-1E78-D107-2616-FA30049BD427}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InstallDate	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{1384CAC3-17AC-E069-EB5C-4E613FCC6FE4}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5E441BBB-4FA0-7A47-C898-77D45B377F36}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{28ABA520-2C1D-6C61-C0C7-A14CF6B906F1}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{62E4E317-0062-79DE-48F0-1E0765BB0FBB}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{3588360E-206F-AD4B-5FE2-CA87B137A0AE}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5CFB38CB-4922-AAF5-9C1E-F3F5A6338105}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BD715941-4DC5-0356-AE8C-CD7DA56A3E36}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{2576763A-EFDC-256B-2964-9C5E743B0B1B}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{92405BE0-7F95-9DE5-BB58-67AC75F6DB46}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5CFB38CB-4922-AAF5-9C1E-F3F5A6338105}\ShellFolder\{6163A5A0-8F6D-BC6F-0F85-4E9A4DFDDFCD}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder\{6781384C-D1DE-7FD4-2373-2921CB5EC9EF}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{A13D7EA4-5D34-8684-2E14-FDAFDFB3E2D8}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4D2056E1-92AF-EC5C-2615-AA80579018DA}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{368B1D7B-EAC9-2EB9-9178-5819EFDD132A}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9D74D8D1-A2C2-8A4E-2A5F-EBAAE5390403}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}\DisplayName	access, read	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008F-0000-1000-0000000FF1CE}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008F-0000-1000-0000000FF1CE}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008F-0000-1000-0000000FF1CE}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{929FBD26-9020-399B-9A7A-751D61F0B942}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{929FBD26-9020-399B-9A7A-751D61F0B942}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{929FBD26-9020-399B-9A7A-751D61F0B942}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EEA66967-97E2-4561-A999-5C22E3CDE428}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EEA66967-97E2-4561-A999-5C22E3CDE428}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EEA66967-97E2-4561-A999-5C22E3CDE428}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	access, read	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	access, read	explorer.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
rgqzicu.exe	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpt36r42xw" /s	CLEAN
rgqzicu.exe	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxFreeMemory	CLEAN
rgqzicu.exe	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxNewJob	CLEAN
rgqzicu.exe	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxNewJobEx	CLEAN
rgqzicu.exe	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxRestoreJob	CLEAN
rgqzicu.exe	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxRestoreJobEx	CLEAN
rgqzicu.exe	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxFreeMemory /fn_args="0"	CLEAN
rgqzicu.exe	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxNewJob /fn_args="0"	CLEAN
rgqzicu.exe	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxNewJobEx /fn_args="0"	CLEAN
rgqzicu.exe	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxRestoreJob /fn_args="0"	CLEAN
rgqzicu.exe	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxRestoreJobEx /fn_args="0"	CLEAN
rgqzicu.exe	"C:\Users\RDhJ0CNFevzX\Desktop\rGQZICU.exe" /dll="C:\Users\RDHJ0C~1\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll" /fn_id=DpxFreeMemory /fn_args="1"	CLEAN

YARA / AV

Antivirus (4)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\Desktop\96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9.exe.dll	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-28 08:04:18+00:00
Built-in AV Database Records	10477558

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

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

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