MALICIOUS

Classifications: Injector

Threat Names: Mal/HTMLGen-A, Generic.Andromeda.FF046139, Generic.Andromeda.79093CCD, Gen:Variant.Razy.655877

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe**
ID	#2780744
MD5	fb45ecbfb0e13b103b6b1c583479a21d
SHA1	9cb9eead55f3b3f4847fd8f1bdd8d20ca46d9dc2
SHA256	d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6
File Size	128.00 KB
Report Created	2021-09-27 21:30 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (24 rules, 37 matches)

Score	Category	Operation	Count	Classification
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #3) explorer.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih".			
4/5	Reputation	Contacts known malicious URL	8	-
	• Reputation analysis labels the URL "geenaldencia9.top/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "kimballiett2.top/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "xadriettany3.top/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "jebeccallis4.top/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "nityanneron5.top/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "umayaniela6.top/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "lynettaram7.top/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "sadineyalas8.top/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A".			
4/5	Antivirus	Malicious content was detected by heuristic scan	3	-
	• Built-in AV detected a memory dump of (process #1) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe as "Generic.Andromeda.FF046139". • Built-in AV detected a memory dump of (process #1) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe as "Generic.Andromeda.79093CCD". • Built-in AV detected a memory dump of (process #2) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe as "Gen:Variant.Razy.655877".			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #2) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe modifies memory of (process #3) explorer.exe.			
4/5	Injection	Modifies control flow of another process	1	Injector
	• (Process #2) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe creates thread in (process #3) explorer.exe.			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #2) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Hide Tracks	Deletes file after execution	2	-
	• (Process #3) explorer.exe deletes executed executable "c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih". • (Process #3) explorer.exe deletes executed executable "c:\users\rdhj0cnfevzx\desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe".			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #3) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #5) 9dc0.exe reads the network adapters' addresses by API.			
2/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih", to be triggered by Logon. • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih", to be triggered by Time. Task has been rescheduled by the analyzer.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-

Score	Category	Operation	Count	Classification
	• (Process #1) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe modifies memory of (process #2) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe alters context of (process #2) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe reads from (process #2) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #3) explorer.exe enumerates running processes.			
1/5	Mutex	Creates mutex	1	-
	• (Process #3) explorer.exe creates mutex with name "FE7F15060B875FB9FB2A49F08D5D03120C287F38".			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #3) explorer.exe starts (process #5) 9dc0.exe with a hidden window. • (Process #5) 9dc0.exe starts (process #8) powershell.exe with a hidden window.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #5) 9dc0.exe enables process privilege "SeDebugPrivilege".			
1/5	Execution	Drops PE file	1	-
	• (Process #3) explorer.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\9DC0.exe".			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\9DC0.exe".			
1/5	Execution	Executes itself	2	-
	• (Process #1) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe. • (Process #4) svchost.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe resolves 42 API functions by name.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #5) 9dc0.exe resolves host name "store2.gofile.io" to IP "31.14.69.10".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #5) 9dc0.exe opens an outgoing TCP connection to host "31.14.69.10:443".			
-	Trusted	Known clean file	2	-

Score	Category	Operation	Count	Classification
		• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fe77092-4798-42ae-bda5-e7f822b580e9" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_da21122d-ae44-4f93-ba1d-c9a978ca5b20" is a known clean file.		

Mitre ATT&CK Matrix

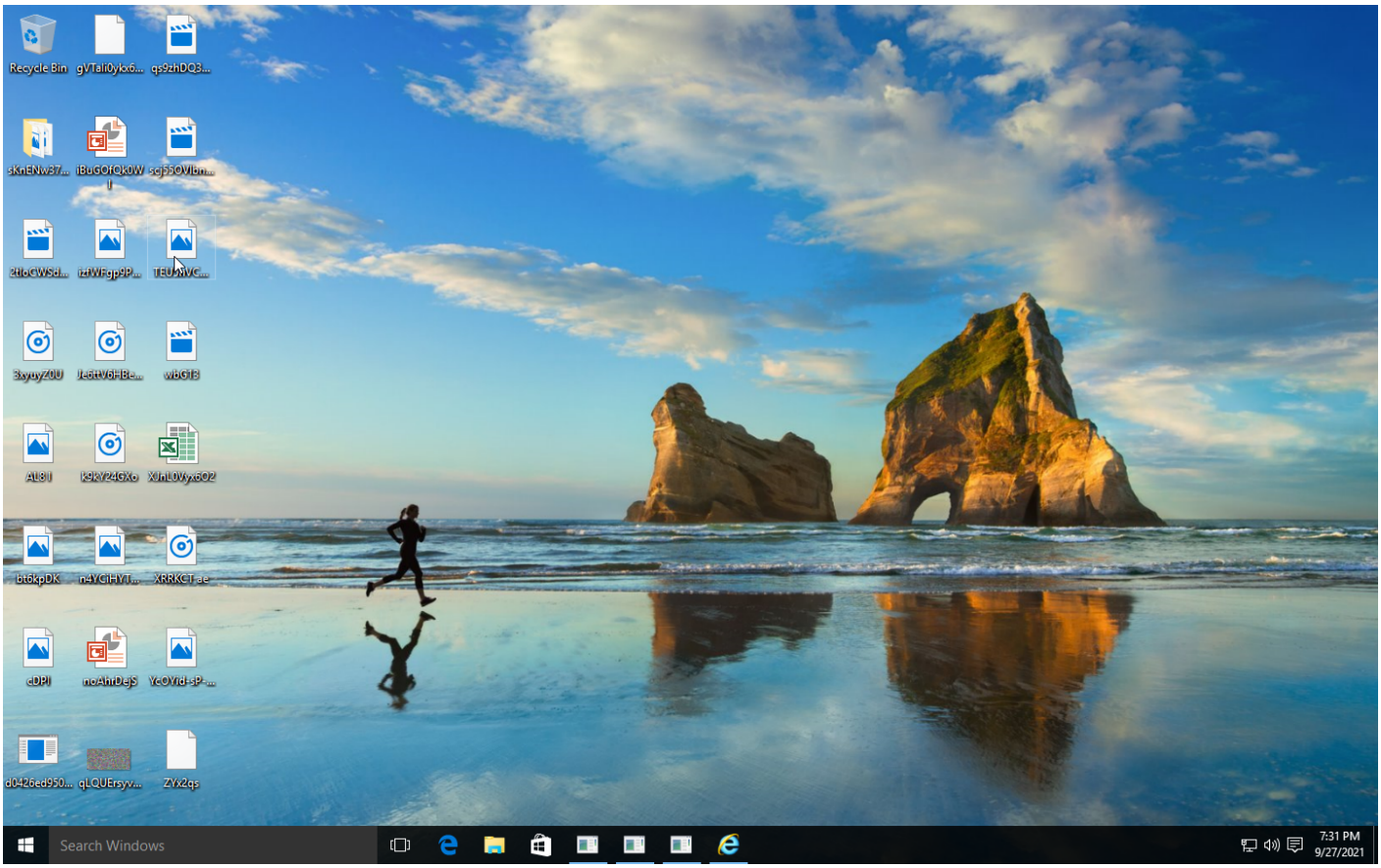
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1045 Software Packing		#T1057 Process Discovery					
				#T1096 NTFS File Attributes		#T1016 System Network Configuration Discovery					
				#T1143 Hidden Window							

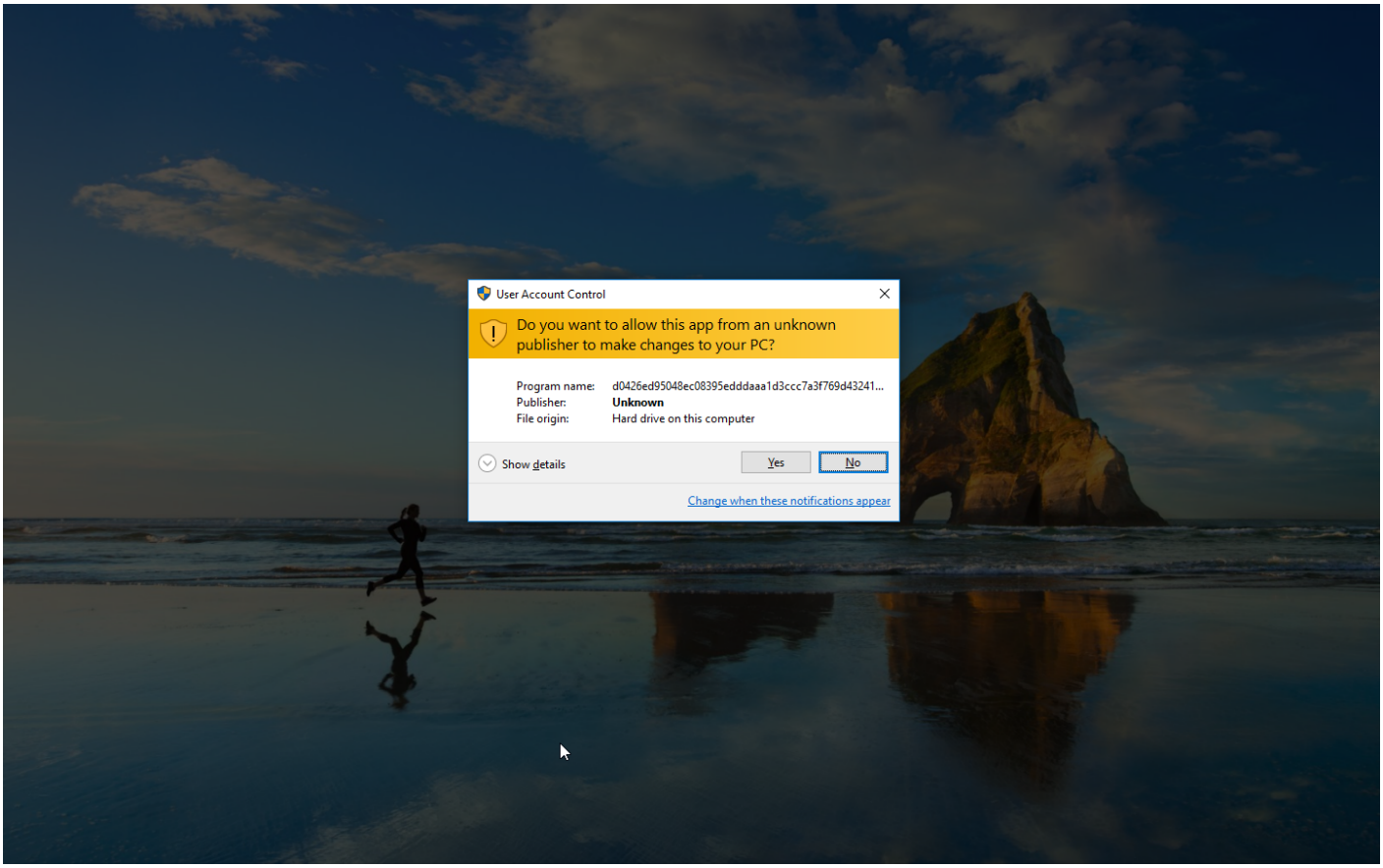
Sample Information

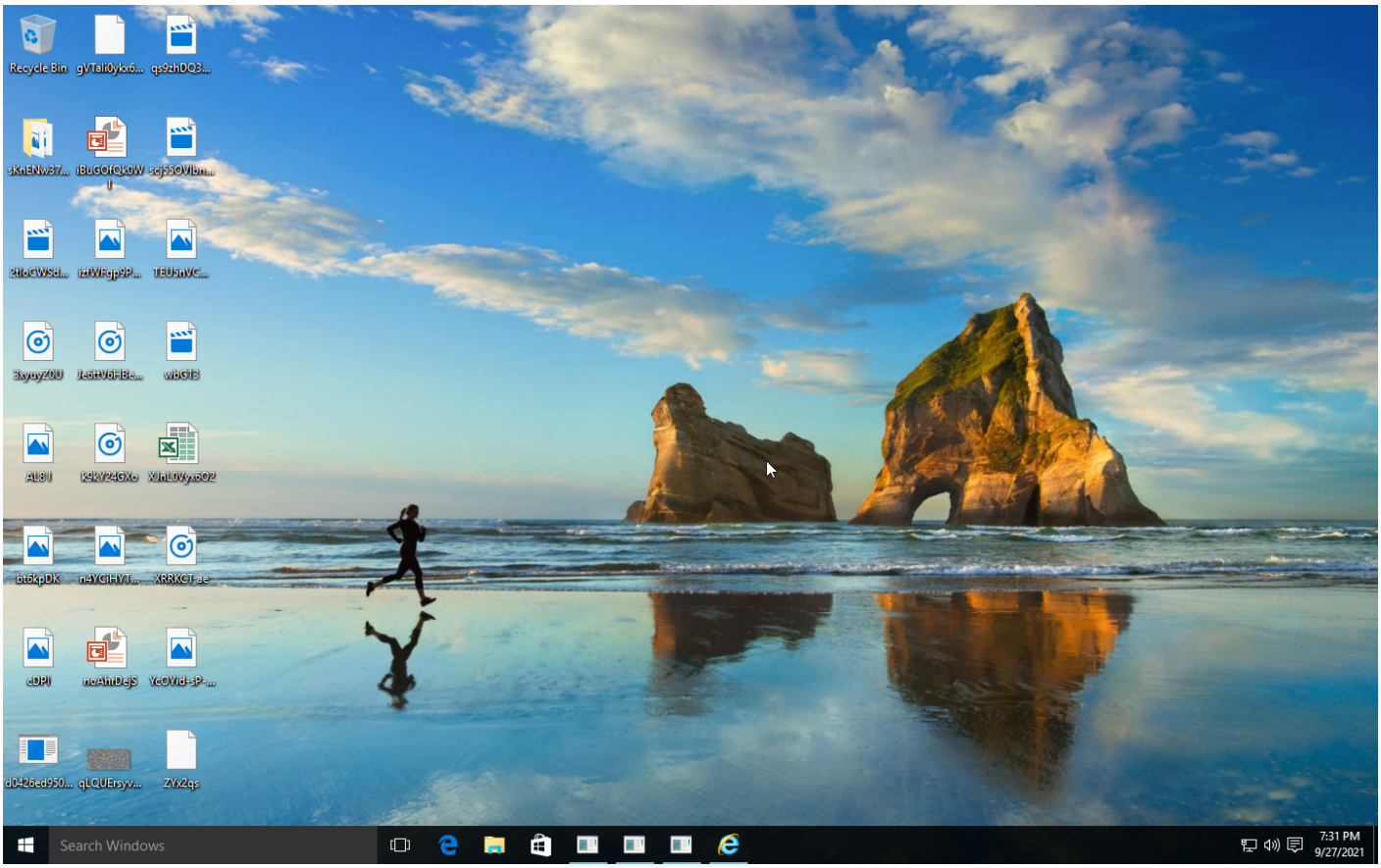
ID	#2780744
MD5	fb45ecbfb0e13b103b6b1c583479a21d
SHA1	9cb9eead55f3b3f4847fd8f1bdd8d20ca46d9dc2
SHA256	d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6
SSDeep	1536:jLOCZw1YLUlP7fXadkUQ0+78Au2SRjj/WgmO/Z/eh3uJp+Q7Jgz70elacRbUozsz:jnwcUNPfjQv5/Z0qfPeZcRwKsz
ImpHash	f98cc9327e2d65cc6189a693f26e1c1d
File Name	d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe
File Size	128.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

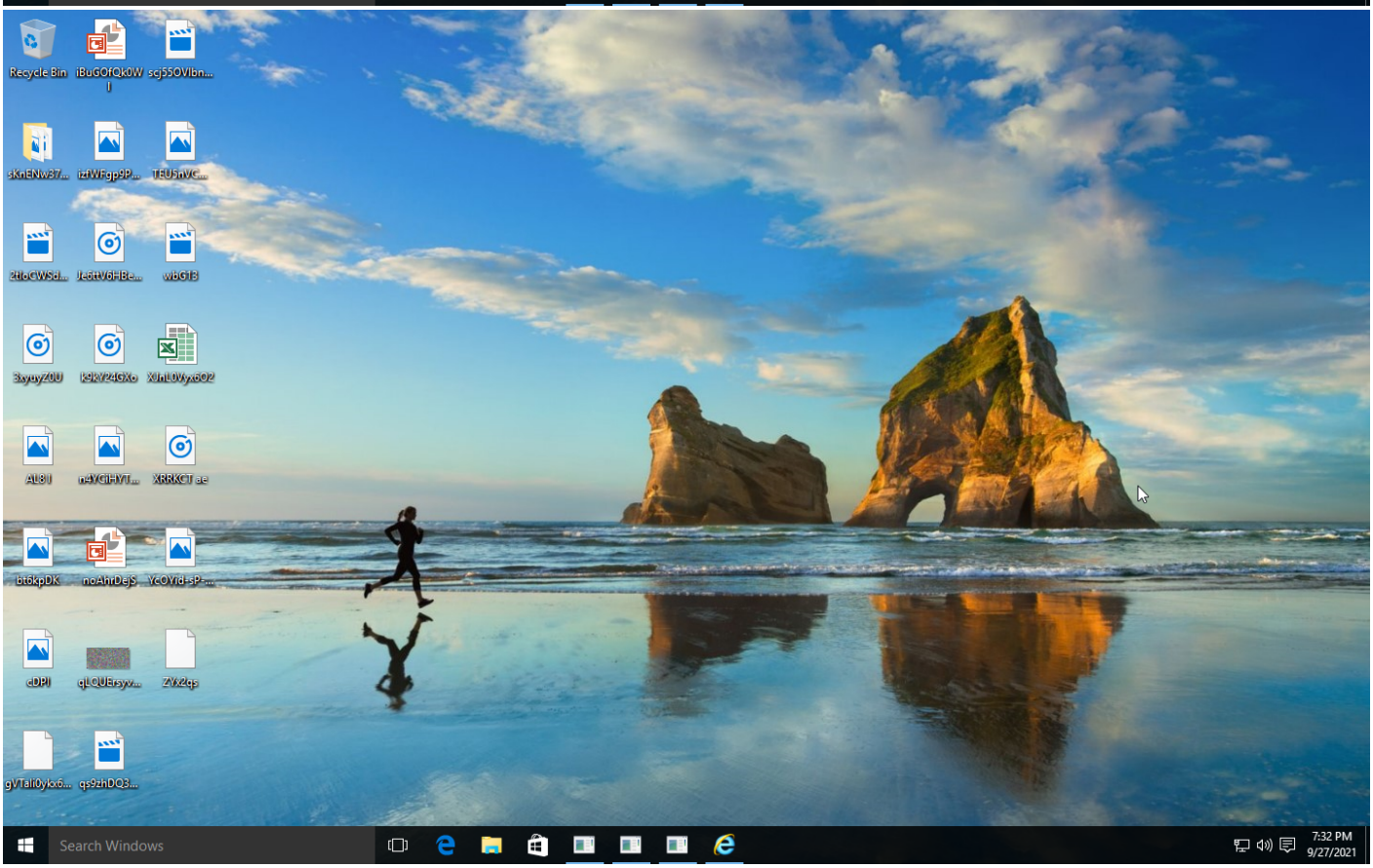
Analysis Information

Creation Time	2021-09-27 21:30 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	9
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✓
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	6
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
Search Windows
7:31 PM
9/27/2021


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: d0426ed95048ec08395edddaaa1d3ccc7a3f769d43241...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

7.87 KB total sent

1855.79 KB total received

2 ports 80, 443

4 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

10 URLs contacted, 10 servers

14 sessions, 7.87 KB sent, 1855.79 KB received

HTTP Requests

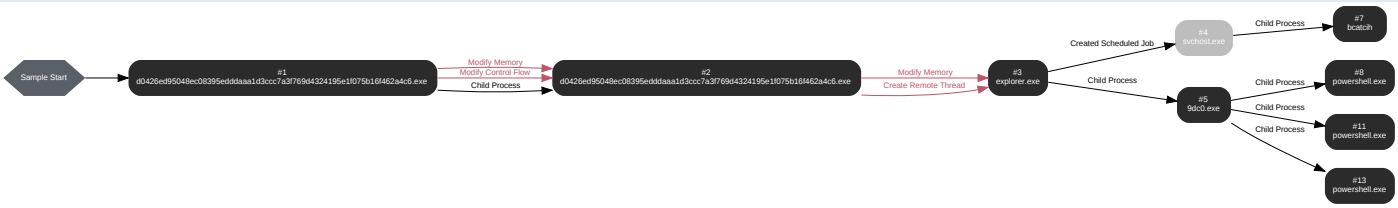
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	geenaldencia9.top/	-	-		0 bytes	NA
POST	naghenrietti1.top/	-	-		0 bytes	NA
POST	kimballiett2.top/	-	-		0 bytes	NA
POST	xadriettany3.top/	-	-		0 bytes	NA
POST	jebeccallis4.top/	-	-		0 bytes	NA
POST	nityanneron5.top/	-	-		0 bytes	NA
POST	umayaniela6.top/	-	-		0 bytes	NA
POST	lynettaram7.top/	-	-		0 bytes	NA
POST	sadineyalas8.top/	-	-		0 bytes	NA
GET	https://store2.gofile.io/download/7bc2a4cf-1f0e-4a03-a2cd-1ea9f4b5afa0/Sxlotftizemiin.dll	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	store2.gofile.io	NoError	31.14.69.10		NA

BEHAVIOR

Process Graph



Process #1: d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 59843, Reason: Analysis Target
Unmonitor End Time	End Time: 84804, Reason: Terminated
Monitor duration	24.96s
Return Code	0
PID	2928
Parent PID	1600
Bitness	32 Bit

Host Behavior

Type	Count
Module	72
File	6
Environment	1
Window	1
Process	1
-	3
-	5

Process #2: d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 78839, Reason: Child Process
Unmonitor End Time	End Time: 97051, Reason: Terminated
Monitor duration	18.21s
Return Code	0
PID	3212
Parent PID	2928
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe	0x2fc	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe	0x2fc	0x401000(4198400)	0x7400	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe	0x2fc	0x28c008(2670600)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe	0x2fc / 0x808	0x77968fe0(2006355936)	-	✓	1

Host Behavior

Type	Count
Module	17
Keyboard	2
Process	1
File	1
System	6
-	1
Registry	12
-	1

Process #3: explorer.exe

ID	3
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 92651, Reason: Injection
Unmonitor End Time	End Time: 300342, Reason: Terminated by Timeout
Monitor duration	207.69s
Return Code	Unknown
PID	1600
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe	0x808	0x2830000(42139648)	0x5000	✓	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe	0x808	0x520000(5373952)	0x16000	✓	1
Create Remote Thread	#2: c:\users\rdhj0cnfevzx\desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe	0x808	0x521a20(5380640)	-	✓	1

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	128.00 KB	d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\9DC0.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\9DC0.exe	56.50 KB	93b774f3ae8414dfad632811c6aee959fa09eec02c03a20706176cfe2b6eed4a	✗

Host Behavior

Type	Count
Module	25
System	11273
Process	8079
Mutex	1
Registry	2
File	27
User	1
COM	1

Network Behavior

Type	Count
HTTP	13
TCP	13

Process #4: svchost.exe

ID	4
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 125938, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 300342, Reason: Terminated by Timeout
Monitor duration	174.40s
Return Code	Unknown
PID	96
Parent PID	536
Bitness	64 Bit

Process #5: 9dc0.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\9dc0.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\9DC0.exe
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 134315, Reason: Child Process
Unmonitor End Time	End Time: 300342, Reason: Terminated by Timeout
Monitor duration	166.03s
Return Code	Unknown
PID	1752
Parent PID	1600
Bitness	64 Bit

Host Behavior

Type	Count
User	1
Process	3
System	4
-	10
Registry	24
File	18
Environment	8
Module	5

Network Behavior

Type	Count
HTTPS	1
DNS	1
TCP	1

Process #7: bcatcih

ID	7
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 136126, Reason: Child Process
Unmonitor End Time	End Time: 300342, Reason: Terminated by Timeout
Monitor duration	164.22s
Return Code	Unknown
PID	1552
Parent PID	96
Bitness	32 Bit

Host Behavior

Type	Count
Module	30
File	3
Environment	1

Process #8: powershell.exe

ID	8
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Start-Sleep -s 5
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 146229, Reason: Child Process
Unmonitor End Time	End Time: 199861, Reason: Terminated
Monitor duration	53.63s
Return Code	0
PID	3544
Parent PID	1752
Bitness	64 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.16 KB	779d2f224e62c6e4470e00582475be919e67c554cb3d8760ab3a9f3bdda4a464	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.16 KB	92b1624b445f72288a2b5a009e108e325933b5b24f70b22deaffbb31322004d0	✗

Host Behavior

Type	Count
Module	5
File	783
Environment	30
Registry	52
Mutex	12
-	24
System	12

Process #11: powershell.exe

ID	11
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Start-Sleep -s 5
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 198901, Reason: Child Process
Unmonitor End Time	End Time: 242924, Reason: Terminated
Monitor duration	44.02s
Return Code	0
PID	1304
Parent PID	1752
Bitness	64 Bit

Host Behavior

Type	Count
Module	5
File	446
Environment	21
Registry	45
Mutex	2
-	19
System	8

Process #13: powershell.exe

ID	13
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Start-Sleep -s 5
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 241907, Reason: Child Process
Unmonitor End Time	End Time: 280607, Reason: Terminated
Monitor duration	38.70s
Return Code	0
PID	4272
Parent PID	1752
Bitness	64 Bit

Host Behavior

Type	Count
Module	5
File	499
Environment	21
Registry	45
Mutex	2
-	19
System	8

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d0426ed95048ec08395eddd aaa1d3ccc7a3f769d4324195 e1f075b16f462a4c6	C: \Users\RDhJ0CNFevzX\Desktop\d04 26ed95048ec08395edddaaa1d3ccc7a3 f769d4324195e1f075b16f462a4c6.exe, C: \Users\RDhJ0CNFevzX\AppData\Ro aming\bcatcih	Sample File	128.00 KB	application/ vnd.microsoft.portable- executable	Write, Access, Delete, Create	MALICIOUS
93b774f3ae8414dfad632811 c6aee959fa09eec02c03a207 06176cfe2b6eed4a	C: \Users\RDHJ0C~1\AppData\Local\Te mp\9DC0.exe	Dropped File	56.50 KB	application/ vnd.microsoft.portable- executable	Write, Access, Create	SUSPICIOUS
db123d2d2807b259aa3a7cd bba857fb570602df5bf5a9039 fe79329b39e36bf5	C: \Users\RDhJ0CNFevzX\AppData\Loc al\Microsoft\Windows\PowerShell\Co mmandAnalysis\PowerShell_Analysis CacheIndex	Modified File	2.16 KB	application/octet-stream	Write, Access, Read, Create	CLEAN
bfd60204585f1603ee9faac7c 44adb9fcd6fa56b7748f03ecb 1a9beaa7c56ea1	C: \Users\RDhJ0CNFevzX\AppData\Loc al\Microsoft\Windows\PowerShell\Co mmandAnalysis\PowerShell_Analysis CacheEntry_6fe77092-4798-42ae- bda5-e7f822b580e9	Modified File	1.16 KB	application/octet-stream	Write, Access, Create	CLEAN
72831bc6962c8017ea71abc 038a8f60e79976ebaf05d363 c80f32c975a55d0d9	C: \Users\RDhJ0CNFevzX\AppData\Loc al\Microsoft\Windows\PowerShell\Co mmandAnalysis\PowerShell_Analysis CacheEntry_da21122d-ae44-4f93- ba1d-c9a978ca5b20	Modified File	10.76 KB	application/octet-stream	Write, Access, Read, Create	CLEAN
779d2f224e62c6e4470e0058 2475be919e67c554cb3d876 0ab3a9f3bdda4a464	C: \Users\RDhJ0CNFevzX\AppData\Loc al\Microsoft\Windows\PowerShell\Co mmandAnalysis\PowerShell_Analysis CacheIndex	Dropped File	2.16 KB	application/octet-stream	Write, Access, Read, Create	CLEAN
92b1624b445f72288a2b5a00 9e108e325933b5b24f70b22d eaffbb31322004d0	C: \Users\RDhJ0CNFevzX\AppData\Loc al\Microsoft\Windows\PowerShell\Co mmandAnalysis\PowerShell_Analysis CacheIndex	Dropped File	2.16 KB	application/octet-stream	Write, Access, Read, Create	CLEAN

Filename

File Name	Category	Operations	Verdict
C: \Users\RDhJ0CNFevzX\Desktop\d0426ed95048ec08395edddaaa1d3 ccc7a3f769d4324195e1f075b16f462a4c6.exe	Sample File	Access, Delete	CLEAN
apfHQ	Accessed File	Access	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	Sample File	Write, Access, Delete, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih:Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Windows\system32\advapi32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\wvhwbfa	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\9DC0.tmp	Accessed File	Access, Delete, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\9DC0.exe	Dropped File	Write, Access, Create	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Windows	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\System32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppBackgroundTask	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppLocker	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppLocker\AppLocker.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Appx	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Appx\Appx.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AssignedAccess	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\BitLocker	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\BitLocker\BitLocker.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\BitsTransfer	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\BranchCache	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\BranchCache\BranchCache.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\CimCmdlets	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Defender	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Defender\Defender.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Dism	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Dism\Dism.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\DnsClient	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
c:\windows\system32\windowspowershell\v1.0\Modules\DnsClient\DnsClient.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\EventTracingManagement	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\International	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\International\International.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\iSCSI	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\iSCSI\iSCSI.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\ISE	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\ISE\ISE.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Kds	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Kds\Kds.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\en-US.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\en-US.psm1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\en-US.cdxml	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\en-US.xaml	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\en-US.dll	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\en-US.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\en-US.psm1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\en-US.cdxml	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\en-US.xaml	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\en-US.dll	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\MMAgent	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\MMAgent\MMAgent.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\MsDtc	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\MsDtc\MsDtc.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetAdapter\NetAdapter.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetConnection	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetConnection\NetConnection.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture\NetEventPacketCapture.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
c:\windows\system32\windowspowershell\v1.0\Modules\NetLbfo	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetLbfo\NetLbfo.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetSecurity	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetSecurity\NetSecurity.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetSwitchTeam	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetSwitchTeam\NetSwitchTeam.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetTCPIP	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetTCPIP\NetTCPIP.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus\NetworkConnectivityStatus.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\SecureBoot	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\SecureBoot\SecureBoot.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\SmbShare	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\SmbShare\SmbShare.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\SmbWitness	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\SmbWitness\SmbWitness.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\StartLayout	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\StartLayout\StartLayout.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\Pester.psd1	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask	Accessed File	Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://geenaldencia9.top	-	194.147.85.186	-	POST	MALICIOUS
http://kimballiett2.top	-	-	-	POST	MALICIOUS
http://xadriettany3.top	-	-	-	POST	MALICIOUS
http://jebeccallis4.top	-	-	-	POST	MALICIOUS
http://nityanneron5.top	-	-	-	POST	MALICIOUS
http://umayaniela6.top	-	-	-	POST	MALICIOUS
http://lynettaram7.top	-	-	-	POST	MALICIOUS
http://sadineyalas8.top	-	-	-	POST	MALICIOUS
https://store2.gofile.io/download/7bc2a4cf-1f0e-4a03-a2cd-1ea9f4b5afa0/Sxlotftizemiin.dll	-	31.14.69.10	-	GET	CLEAN
http://naghenrietti1.top	-	-	-	POST	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
naghenrietti1.top	-	-	HTTP	CLEAN
kimballiett2.top	-	-	HTTP	CLEAN
xadriettany3.top	-	-	HTTP	CLEAN
jebeccallis4.top	-	-	HTTP	CLEAN
nityanneron5.top	-	-	HTTP	CLEAN
umayaniela6.top	-	-	HTTP	CLEAN
lynettaram7.top	-	-	HTTP	CLEAN
sadineyalas8.top	-	-	HTTP	CLEAN
geenaldencia9.top	194.147.85.186	-	HTTP	CLEAN

Domain	IP Address	Country	Protocols	Verdict
store2.gofile.io	31.14.69.10	-	HTTPS, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
194.147.85.186	geenaldencia9.top	Russia	TCP, HTTP, DNS	CLEAN
31.14.69.10	store2.gofile.io	France	TCP, HTTPS, DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
FE7F15060B875FB9FB2A49F08D5D03120C287F38	access	explorer.exe	CLEAN
Global\PowerShell_CommandAnalysis_Lock_S-1-5-21-1560258661-3990802383-1811730007-1000	access	powershell.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\IDE	access	d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe	CLEAN
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\SCSI	access	d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\svcVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine\ApplicationBase	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment__PSLockdownPolicy	access, read	powershell.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	powershell.exe	CLEAN
HKEY_PERFORMANCE_DATA	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	access, read	9dc0.exe	CLEAN
HKEY_CURRENT_USER	access	9dc0.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	9dc0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	9dc0.exe	CLEAN

Process

Process Name	Commandline	Verdict
d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe	"C:\Users\RDhJ0CNFevzX\Desktop\d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6.exe"	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
9dc0.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\9DC0.exe	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
bcatcih	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	CLEAN
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Start-Sleep -s 5	CLEAN

YARA / AV

Antivirus (6)

File Type	Threat Name	File Name	Verdict
Memory Dump	Generic.Andromeda.FF046139	-	MALICIOUS
Memory Dump	Generic.Andromeda.79093CCD	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	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	2021-09-27 16:34:30+00:00
Built-in AV Database Records	10473840

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