MALICIOUS

Classifications: Injector | Backdoor

Threat Names: AsyncRAT.v057B | AsyncRAT | Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe**
ID	#5068470
MD5	30e619eed663b6696ba1269dec11e1a9
SHA1	04ad1454bb163c8e1c5820ba591ae613dd6f6d45
SHA256	faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d
File Size	3072.00 KB
Report Created	2022-08-05 18:25 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (25 rules, 68 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	AsyncRAT configuration was extracted	1	Backdoor
	• A configuration for AsyncRAT was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	3	Backdoor
	• Rule "AsyncRAT" from ruleset "RATs" has matched on a memory dump for (process #2) vbc.exe. • Rule "AsyncRAT" from ruleset "RATs" has matched on a memory dump for (process #24) vbc.exe. • Rule "AsyncRAT" from ruleset "RATs" has matched on a code dump for (process #11) iexplore.exe.			
4/5	Injection	Writes into the memory of another process	3	Injector
	• (Process #1) faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe modifies memory of (process #2) vbc.exe. • (Process #11) iexplore.exe modifies memory of (process #15) vbc.exe. • (Process #23) iexplore.exe modifies memory of (process #24) vbc.exe.			
4/5	Injection	Modifies control flow of another process	3	-
	• (Process #1) faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe alters context of (process #2) vbc.exe. • (Process #11) iexplore.exe alters context of (process #15) vbc.exe. • (Process #23) iexplore.exe alters context of (process #24) vbc.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #2) vbc.exe tries to detect antivirus software via WMI query: "Select * from AntivirusProduct".			
2/5	Anti Analysis	Tries to detect debugger	2	-
	• (Process #1) faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe tries to detect a debugger via API "CheckRemoteDebuggerPresent". • (Process #1) faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe tries to detect a debugger via API "IsDebuggerPresent".			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #2) vbc.exe queries OS version via WMI.			
2/5	Discovery	Executes WMI query	2	-
	• (Process #2) vbc.exe executes WMI query: select * from Win32_OperatingSystem. • (Process #2) vbc.exe executes WMI query: Select * from AntivirusProduct.			
2/5	_data_collection	Reads sensitive browser data	19	-

Score	Category	Operation	Count	Classification
		• (Process #2) vbc.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Opera" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Yandex Browser" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Comodo Dragon" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Maple Studio" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Chromium" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Torch" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "7Star" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Amigo" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "CentBrowser" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Chedot" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "CocCoc" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Elements Browser" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Epic Privacy Browser" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Kometa" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Orbitum" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Sputnik" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Uran" by file. • (Process #2) vbc.exe tries to read sensitive data of web browser "Vivaldi" by file.		
2/5	Anti Analysis	Tries to detect virtual machine	1	-
		• Multiple processes are possibly trying to detect a VM via rdtsc.		
2/5	YARA	Suspicious content matched by YARA rules	3	-
		• Rule "MultipleNetObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #23) iexplore.exe. • Rule "MultipleNetObfuscatorAttributes" from ruleset "Generic" has matched on the sample itself. • Rule "MultipleNetObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #1) faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe.		
2/5	Task Scheduling	Schedules task	1	-
		• Schedules task for command ""C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.		
2/5	Task Scheduling	Schedules task via schtasks	1	-
		• Schedules task "Nafifas" via the schtasks command line utility.		
1/5	Privilege Escalation	Enables process privilege	4	-
		• (Process #1) faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe enables process privilege "SeDebugPrivilege". • (Process #2) vbc.exe enables process privilege "SeDebugPrivilege". • (Process #11) iexplore.exe enables process privilege "SeDebugPrivilege". • (Process #23) iexplore.exe enables process privilege "SeDebugPrivilege".		
1/5	Hide Tracks	Creates process with hidden window	3	-
		• (Process #1) faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe starts (process #1) faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe with a hidden window. • (Process #11) iexplore.exe starts (process #11) iexplore.exe with a hidden window. • (Process #23) iexplore.exe starts (process #23) iexplore.exe with a hidden window.		
1/5	Obfuscation	Reads from memory of another process	3	-

Score	Category	Operation	Count	Classification
		• (Process #1) faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe reads from (process #1) faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe. • (Process #11) iexplore.exe reads from (process #11) iexplore.exe. • (Process #23) iexplore.exe reads from (process #23) iexplore.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	3	-
		• (Process #1) faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #11) iexplore.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #23) iexplore.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.		
1/5	Mutex	Creates mutex	2	-
		• (Process #2) vbc.exe creates mutex with name "AsyncMutex_6SI8OkPnk". • (Process #15) vbc.exe creates mutex with name "AsyncMutex_6SI8OkPnk".		
1/5	Hide Tracks	Writes an unusually large amount of data to the registry	1	-
		• (Process #2) vbc.exe hides 426755 bytes in "HKEY_CURRENT_USER\Software\FFCF46333CE8854C9474\405813D04B53574AB8C9721795E9FD705273487C852B7F4545FB875DA09C7350".		
1/5	Discovery	Possibly does reconnaissance	1	-
		• (Process #2) vbc.exe tries to gather information about application "Mozilla Firefox" by file.		
1/5	Network Connection	Connects to remote host	1	-
		• (Process #2) vbc.exe opens an outgoing TCP connection to host "191.101.130.243:7707".		
1/5	Network Connection	Tries to connect using an uncommon port	1	-
		• (Process #2) vbc.exe tries to connect to TCP port 7707 at 191.101.130.243.		
1/5	Obfuscation	Resolves API functions dynamically	1	-
		• (Process #2) vbc.exe resolves 58 API functions by name.		
1/5	YARA	Content matched by YARA rules	6	-
		• Rule "YanoObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #23) iexplore.exe. • Rule "BabelObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #23) iexplore.exe. • Rule "YanoObfuscatorAttributes" from ruleset "Generic" has matched on the sample itself. • Rule "BabelObfuscatorAttributes" from ruleset "Generic" has matched on the sample itself. • Rule "YanoObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #1) faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe. • Rule "BabelObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #1) faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe.		

Malware Configuration: AsyncRAT

Metadata	Key	Extracted Value
Version	Value	0.5.7B
Socket	Address Port Network Protocol C2 Listen	191.101.130.243 7707 tcp ✔ ✖
Mutex	Value	AsyncMutex_6SI8OkPnk
Interval	Tags Value	Delay 3.0
Mission ID	Value	Alibaba
Other: Install	Value	✖
Other: Key	Tags Value	PBKDF2 Input Password F37wL6kU6d1ln0ZzFzD1Z61sP0kXqYbm
Other: Salt	Value	v+seVvvNlzuyGQIkMKV4QwA9VkTSHmK51PGA5+bDOUE=
Other: Certificate	Value	MIIE8jCCAtqgAwIBAgIQALjgwS++igAkwAOyv5bgMTANBgkqhkiG9w0BAQ0FADAaMRgwFgYDVQQDDA9Bc3luY1JBVCBTZ…
Other: Serversignature	Value	LnD03k7cpYYvIPzVlgkFIKRQelVSCNDslUHUMdlARBBMyw1TZMPHK9AU16GUATrv8GN6kBdJLY0QW7A/k2nEAOJPZxlN…
Other: Anti Analysis Enabled	Value	✖
Other: BDOS Enabled	Value	✖

Mitre ATT&CK Matrix

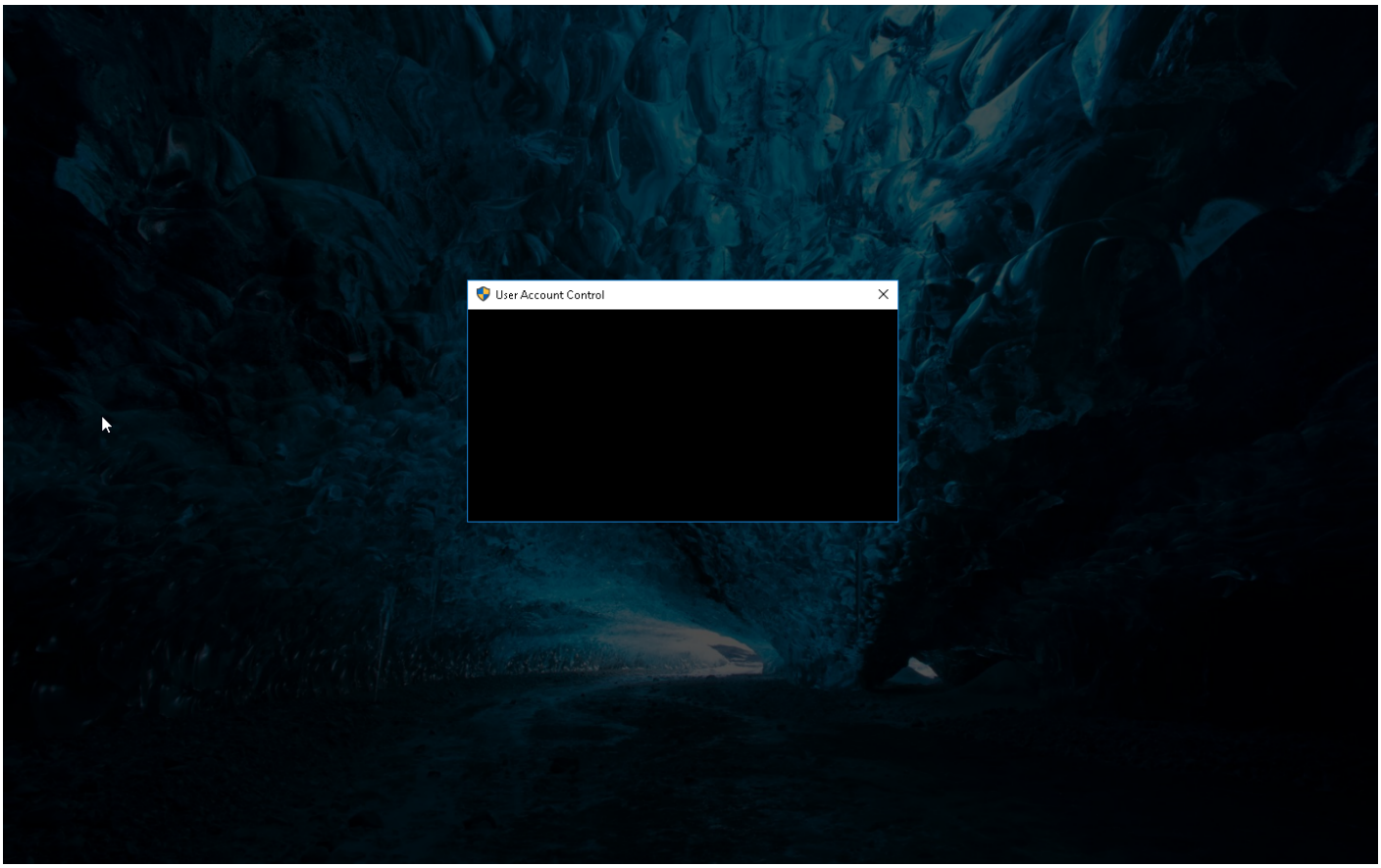
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window	#T1081 Credentials in Files	#T1082 System Information Discovery		#T1119 Automated Collection	#T1065 Uncommonly Used Port		
	#T1053 Scheduled Task			#T1045 Software Packing		#T1063 Security Software Discovery		#T1005 Data from Local System			
				#T1112 Modify Registry		#T1083 File and Directory Discovery					
				#T1497 Virtualization/ Sandbox Evasion		#T1497 Virtualization/ Sandbox Evasion					
						#T1124 System Time Discovery					

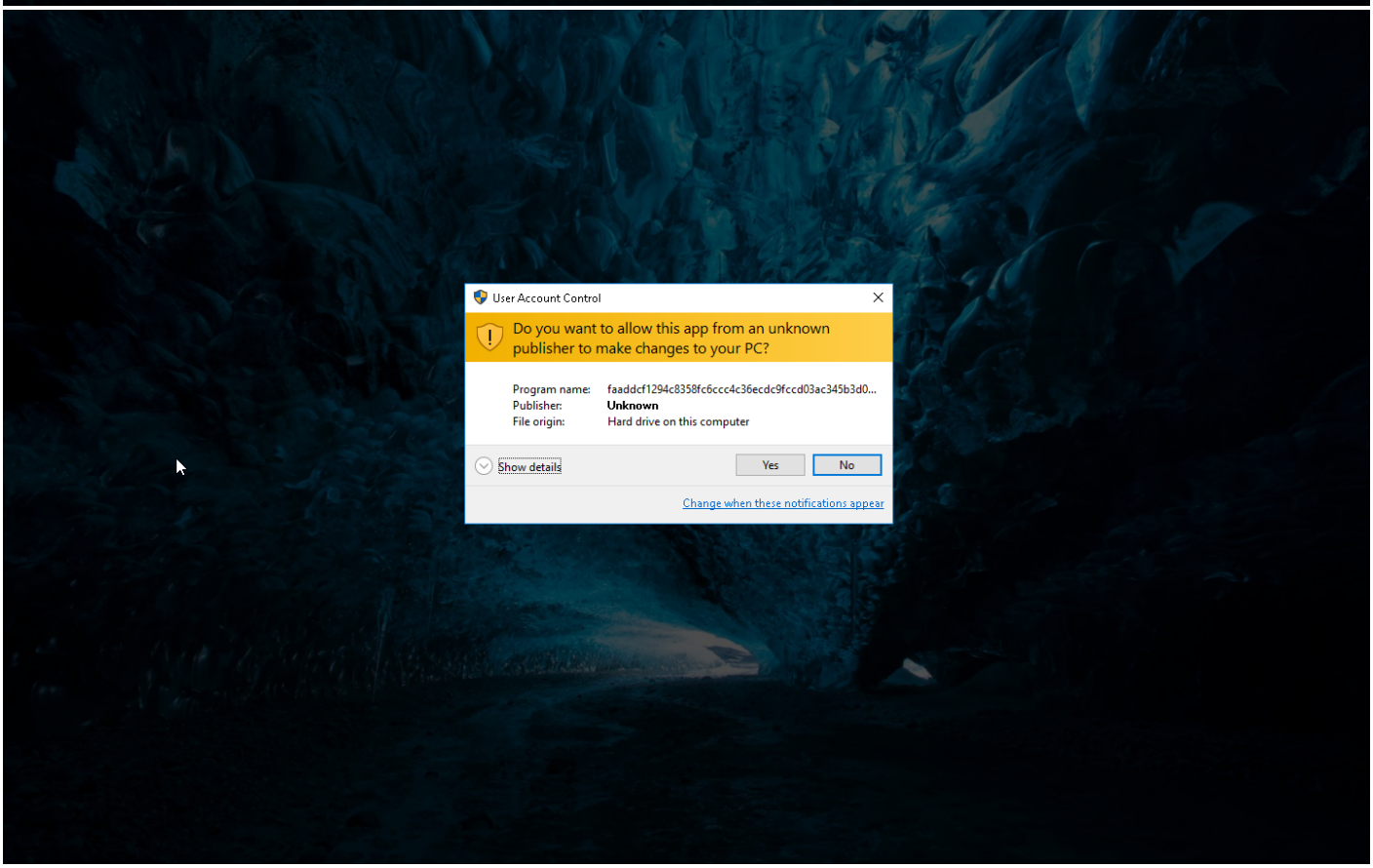
Sample Information

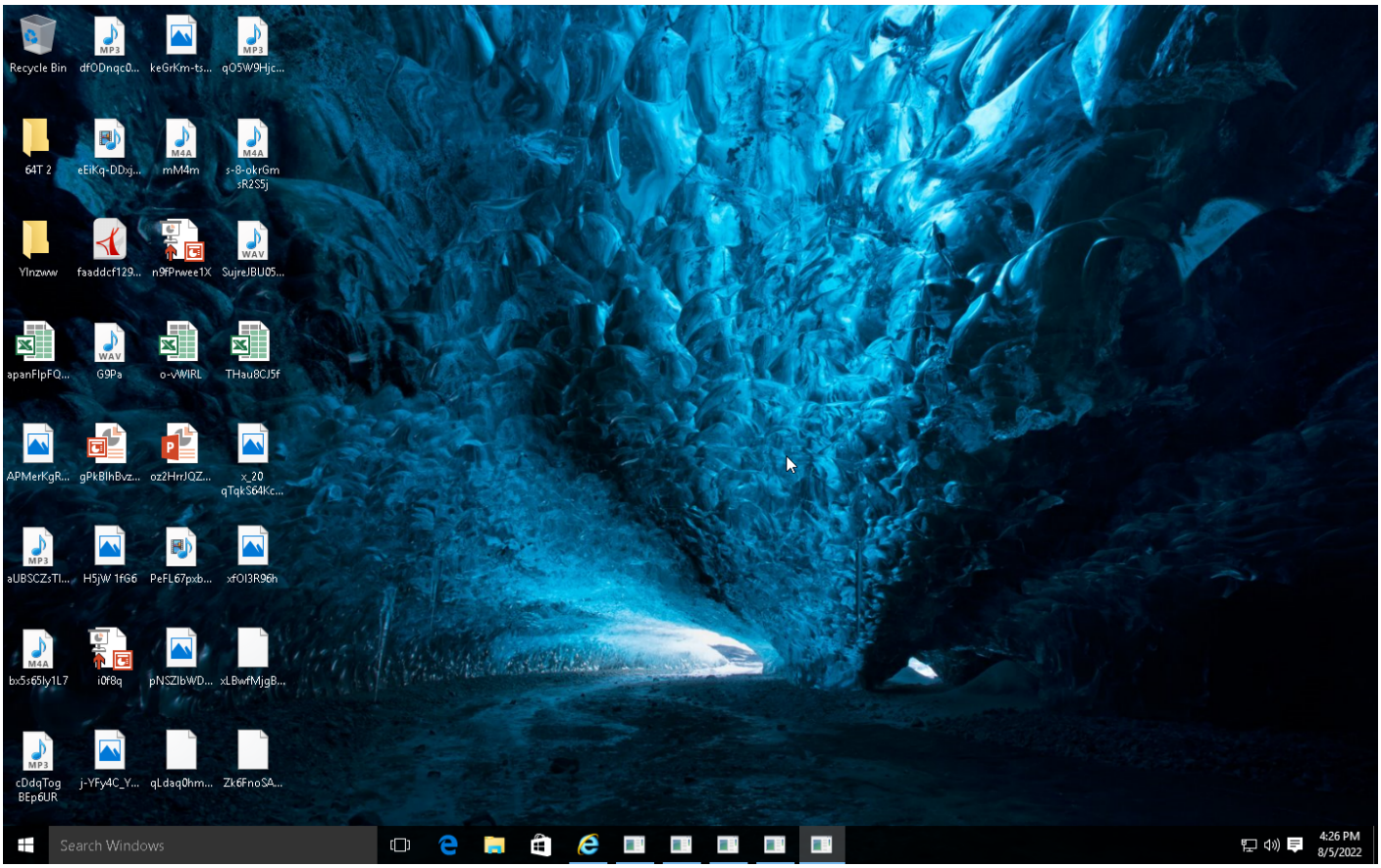
ID	#5068470
MD5	30e619eed663b6696ba1269dec11e1a9
SHA1	04ad1454bb163c8e1c5820ba591ae613dd6f6d45
SHA256	faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d
SSDeep	6144:PnsnxIpl/4MgsaffkOiBxqwuhiowOskDnlat1JLfwyTeiB0PJo3zzn:fs3pZ4MgzffDwsbikcJpnfn
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe
File Size	3072.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 18:25 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	19
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	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	12


User Account Control


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d0...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
dfODnqc0...
keGrKm-ts...
qO5W9Hjc...
64T 2
eEiKq-DDxj...
mM4m
s-8-okrGm
sR2S5j
Ylnzww
faaddcf129...
n9fPrwee1X
SujreJBU05...
apanFlpFQ...
G9Pa
o-vWIRL
THau8CJ5f
APMerKgR...
gPkBlkBvz...
oz2HrrJQZ...
x_20
qTqkS64Kc...
aUBSCZsTI...
H5jW 1fG6
PeFL67pxb...
xfOI3R96h
bx5s65ly1L7
i0f8q
pNSZIbWD...
xLBwfMjgB...
cDdqTog
BEp6UR
j-YFy4C_Y...
qLdaq0hm...
Zk6FnoSA...
Search Windows
4:26 PM
8/5/2022

NETWORK

General

12.26 KB total sent

440.46 KB total received

1 ports 7707

1 contacted IP addresses

1 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

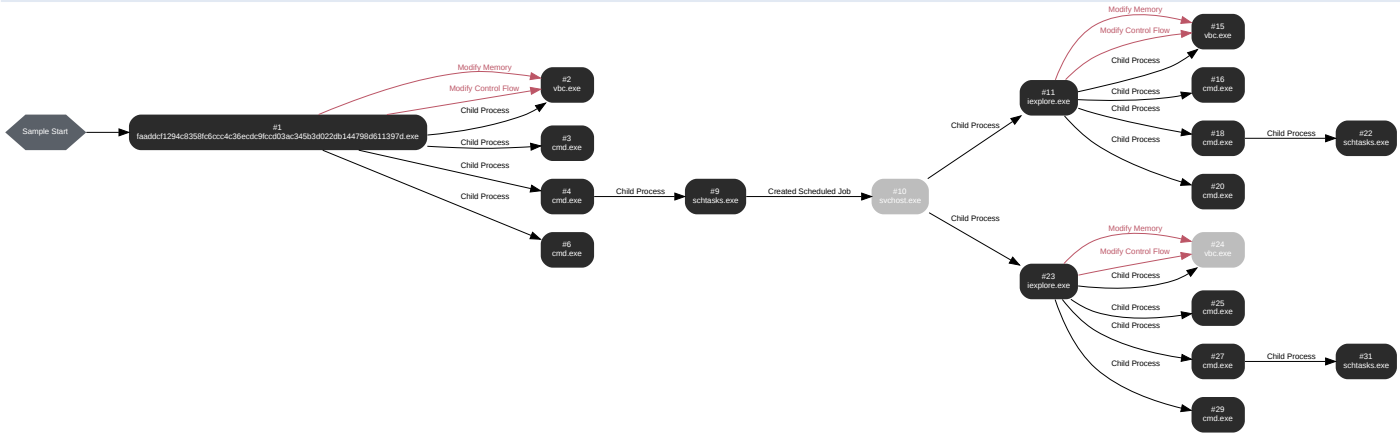
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 67213, Reason: Analysis Target
Unmonitor End Time	End Time: 127590, Reason: Terminated
Monitor duration	60.38s
Return Code	0
PID	5108
Parent PID	1972
Bitness	32 Bit

Host Behavior

Type	Count
Environment	3
User	1
Registry	1
-	96
File	15
Process	4
-	3
-	8
-	3
Module	1

Process #2: vbc.exe

ID	2
File Name	c:\windows\microsoft.net\framework\v4.0.30319\vbc.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 117123, Reason: Child Process
Unmonitor End Time	End Time: 308121, Reason: Terminated by timeout
Monitor duration	191.00s
Return Code	Unknown
PID	4296
Parent PID	5108
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe	0x13f8	0x1d0000(1900544)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe	0x13f8	0x1d2000(1908736)	0xa800	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe	0x13f8	0x1de000(1957888)	0xa00	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe	0x13f8	0x1e0000(1966080)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe	0x13f8	0x4720008(74579976)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe	0x13f8 / 0xb84	0x40c71e(4245278)	-	✔	1

Host Behavior

Type	Count
Registry	31
User	3
System	13428
File	113
Mutex	1
-	3
Module	73
COM	9

Type	Count
-	2
Environment	6

Network Behavior

Type	Count
TCP	2

Process #3: cmd.exe

ID	3
File Name	c:\windows\syswow64\cmd.exe
Command Line	"cmd" /c mkdir "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 121321, Reason: Child Process
Unmonitor End Time	End Time: 145287, Reason: Terminated
Monitor duration	23.97s
Return Code	1
PID	2044
Parent PID	5108
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	18
Environment	11
System	1

Process #4: cmd.exe

ID	4
File Name	c:\windows\syswow64\cmd.exe
Command Line	"cmd" /c schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe'" /f
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 122455, Reason: Child Process
Unmonitor End Time	End Time: 151130, Reason: Terminated
Monitor duration	28.68s
Return Code	0
PID	1984
Parent PID	5108
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	19
System	1
Process	1

Process #6: cmd.exe

ID	6
File Name	c:\windows\syswow64\cmd.exe
Command Line	"cmd" /c copy "C:\Users\RDhJ0CNFevzX\Desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe" "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 122692, Reason: Child Process
Unmonitor End Time	End Time: 145918, Reason: Terminated
Monitor duration	23.23s
Return Code	0
PID	3204
Parent PID	5108
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe	3072.00 KB	faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d	✔

Host Behavior

Type	Count
Module	8
Registry	17
File	28
Environment	11
System	1
Process	1

Process #9: schtasks.exe

ID	9
File Name	c:\windows\syswow64\schtasks.exe
Command Line	schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe'" /f
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 139941, Reason: Child Process
Unmonitor End Time	End Time: 149941, Reason: Terminated
Monitor duration	10.00s
Return Code	0
PID	4448
Parent PID	1984
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
System	3
COM	1
File	3

Process #10: svchost.exe

ID	10
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: 146716, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 308121, Reason: Terminated by timeout
Monitor duration	161.41s
Return Code	Unknown
PID	864
Parent PID	4448
Bitness	64 Bit

Process #11: iexplore.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 157891, Reason: Child Process
Unmonitor End Time	End Time: 236851, Reason: Terminated
Monitor duration	78.96s
Return Code	0
PID	4456
Parent PID	864
Bitness	32 Bit

Host Behavior

Type	Count
Environment	3
Registry	1
User	1
-	150
File	12
Process	4
-	3
-	8
-	3
Module	1

Process #15: vbc.exe

ID	15
File Name	c:\windows\microsoft.net\framework\v4.0.30319\vbc.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 230927, Reason: Child Process
Unmonitor End Time	End Time: 247561, Reason: Terminated
Monitor duration	16.63s
Return Code	0
PID	4176
Parent PID	4456
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe	0x2a4	0x1d0000(1900544)	0x200	✔	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe	0x2a4	0x1d2000(1908736)	0xa800	✔	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe	0x2a4	0x1de000(1957888)	0xa00	✔	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe	0x2a4	0x1e0000(1966080)	0x200	✔	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe	0x2a4	0x4614008(73482248)	0x4	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe	0x2a4 / 0x664	0x40c71e(4245278)	-	✔	1

Host Behavior

Type	Count
Registry	1
User	1
System	2
File	1
Mutex	1

Process #16: cmd.exe

ID	16
File Name	c:\windows\syswow64\cmd.exe
Command Line	"cmd" /c mkdir "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 233577, Reason: Child Process
Unmonitor End Time	End Time: 239489, Reason: Terminated
Monitor duration	5.91s
Return Code	1
PID	3572
Parent PID	4456
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	17
Environment	11
System	1

Process #18: cmd.exe

ID	18
File Name	c:\windows\syswow64\cmd.exe
Command Line	"cmd" /c schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 234027, Reason: Child Process
Unmonitor End Time	End Time: 239004, Reason: Terminated
Monitor duration	4.98s
Return Code	1
PID	2608
Parent PID	4456
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	14
Environment	19
System	1
Process	1

Process #20: cmd.exe

ID	20
File Name	c:\windows\syswow64\cmd.exe
Command Line	"cmd" /c copy "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe" "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 234540, Reason: Child Process
Unmonitor End Time	End Time: 239655, Reason: Terminated
Monitor duration	5.12s
Return Code	1
PID	2812
Parent PID	4456
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	26
Environment	11
System	1
Process	1

Process #22: schtasks.exe

ID	22
File Name	c:\windows\syswow64\schtasks.exe
Command Line	schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 237866, Reason: Child Process
Unmonitor End Time	End Time: 239593, Reason: Terminated
Monitor duration	1.73s
Return Code	1
PID	1932
Parent PID	2608
Bitness	32 Bit

Host Behavior

Type	Count
System	5
Module	3
COM	1
File	12

Process #23: iexplore.exe

ID	23
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 277844, Reason: Child Process
Unmonitor End Time	End Time: 302480, Reason: Terminated
Monitor duration	24.64s
Return Code	0
PID	3284
Parent PID	864
Bitness	32 Bit

Host Behavior

Type	Count
Environment	3
Registry	1
User	1
-	96
File	12
Process	4
-	3
-	8
-	3
Module	1

Process #24: vbc.exe

ID	24
File Name	c:\windows\microsoft.net\framework\v4.0.30319\vbc.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 297163, Reason: Child Process
Unmonitor End Time	End Time: 308121, Reason: Terminated by timeout
Monitor duration	10.96s
Return Code	Unknown
PID	3484
Parent PID	3284
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#23: c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe	0xcd8	0x1d0000(1900544)	0x200	✔	1
Modify Memory	#23: c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe	0xcd8	0x1d2000(1908736)	0xa800	✔	1
Modify Memory	#23: c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe	0xcd8	0x1de000(1957888)	0xa00	✔	1
Modify Memory	#23: c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe	0xcd8	0x1e0000(1966080)	0x200	✔	1
Modify Memory	#23: c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe	0xcd8	0x4735008(74665992)	0x4	✔	1
Modify Control Flow	#23: c:\users\rdhj0cnfevzx\appdata\local\temp\iexplore\iexplore.exe	0xcd8 / 0xda0	0x40c71e(4245278)	-	✔	1

Process #25: cmd.exe

ID	25
File Name	c:\windows\syswow64\cmd.exe
Command Line	"cmd" /c mkdir "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 299740, Reason: Child Process
Unmonitor End Time	End Time: 305715, Reason: Terminated
Monitor duration	5.97s
Return Code	1
PID	4172
Parent PID	3284
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	17
Environment	11
System	1

Process #27: cmd.exe

ID	27
File Name	c:\windows\syswow64\cmd.exe
Command Line	"cmd" /c schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 300248, Reason: Child Process
Unmonitor End Time	End Time: 306323, Reason: Terminated
Monitor duration	6.08s
Return Code	1
PID	2828
Parent PID	3284
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	14
Environment	19
System	1
Process	1

Process #29: cmd.exe

ID	29
File Name	c:\windows\syswow64\cmd.exe
Command Line	"cmd" /c copy "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe" "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 300639, Reason: Child Process
Unmonitor End Time	End Time: 305715, Reason: Terminated
Monitor duration	5.08s
Return Code	1
PID	4648
Parent PID	3284
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	26
Environment	11
System	1
Process	1

Process #31: schtasks.exe

ID	31
File Name	c:\windows\syswow64\schtasks.exe
Command Line	schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 304067, Reason: Child Process
Unmonitor End Time	End Time: 305486, Reason: Terminated
Monitor duration	1.42s
Return Code	1
PID	1472
Parent PID	2828
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
System	3
COM	1
File	12

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d	C:\Users\RDhJ0CNFevzX\Desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe, C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe	Sample File	3072.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	MALICIOUS
607c7b32ca17ef830932ceb8f5568e91d51c54555d84ab9f5dddda9ef61fd354	-	Extracted File	14.82 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe	Sample File, Accessed File, VM File	Access, Read	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe	Dropped File, Accessed File, VM File	Access, Create, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data\Login Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data\Login Data	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\Profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.Config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrcompression.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data\Login Data	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://191.101.130.243:7707	-	191.101.130.243	-	-	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
191.101.130.243	-	United States	TCP, TLS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
AsyncMutex_6SI8OkPnk	access	vbc.exe	MALICIOUS

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\FFCF46333CE8854C9474\405813D04B53574AB8C9721795E9FD705273487C852B7F4545FB875DA09C7350	read, access, write	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\FFCF46333CE8854C9474	create, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	iexplore.exe, faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe, vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	vbc.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN

Process

Process Name	Commandline	Verdict
faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe	"C:\Users\RDhJ0CNFevzX\Desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe"	MALICIOUS
iexplore.exe	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe	MALICIOUS
iexplore.exe	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe	MALICIOUS
vbc.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe"	SUSPICIOUS
cmd.exe	"cmd" /c copy "C:\Users\RDhJ0CNFevzX\Desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe" "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe"	SUSPICIOUS
schtasks.exe	schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe'" /f	SUSPICIOUS
vbc.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe"	SUSPICIOUS
cmd.exe	"cmd" /c copy "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe" "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe"	SUSPICIOUS
vbc.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe"	SUSPICIOUS
cmd.exe	"cmd" /c copy "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe" "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe"	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
cmd.exe	"cmd" /c mkdir "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore"	CLEAN
cmd.exe	"cmd" /c schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe'" /f	CLEAN
cmd.exe	"cmd" /c mkdir "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore"	CLEAN
cmd.exe	"cmd" /c schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe'" /f	CLEAN
schtasks.exe	schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe'" /f	CLEAN
cmd.exe	"cmd" /c mkdir "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore"	CLEAN
cmd.exe	"cmd" /c schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe'" /f	CLEAN
schtasks.exe	schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\iexplore\iexplore.exe'" /f	CLEAN

YARA / AV

YARA (12)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
RATs	AsyncRAT	AsyncRAT	Memory Dump	-	Backdoor	5/5
RATs	AsyncRAT	AsyncRAT	Memory Dump	-	Backdoor	5/5
RATs	AsyncRAT	AsyncRAT	-	-	Backdoor	5/5
Generic	MultipleNetObfuscatorAttributes	.NET file contains multiple obfuscator attributes	Memory Dump	-	-	2/5
Generic	MultipleNetObfuscatorAttributes	.NET file contains multiple obfuscator attributes	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe	-	2/5
Generic	MultipleNetObfuscatorAttributes	.NET file contains multiple obfuscator attributes	Memory Dump	-	-	2/5
Generic	YanoObfuscatorAttributes	Yano Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	BabelObfuscatorAttributes	Babel Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	YanoObfuscatorAttributes	Yano Obfuscator Attributes	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe	-	1/5
Generic	BabelObfuscatorAttributes	Babel Obfuscator Attributes	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d.exe	-	1/5
Generic	YanoObfuscatorAttributes	Yano Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	BabelObfuscatorAttributes	Babel Obfuscator Attributes	Memory Dump	-	-	1/5

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	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.14 / 2022-08-03 12:19:21
YARA Built-in Ruleset Version	4.6.1.10

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
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