MALICIOUS

Classifications: -

Threat Names: AgentTesla | AgentTesla.v3

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe**
ID	#4259493
MD5	5d5f37a7cf3a9ff4277b3a9dc2c4b9d2
SHA1	1a115c8a1761ef2a2cf61d854d1d2c201c902d53
SHA256	31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969
File Size	673.50 KB
Report Created	2022-05-04 17:14 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (26 rules, 59 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Agent Tesla configuration was extracted	1	Spyware
	• A configuration for Agent Tesla was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	2	Spyware
	• Rule "AgentTesla_HTML_Message" from ruleset "Malware" has matched on request data of URL "https://api.telegram.org/bot1698102386:AAHWYbuf-rLmgfOsAgCnA_t8ncjPXSF5S8c/sendDocument". • Rule "AgentTesla_StringDecryption_v3" from ruleset "Malware" has matched on a memory dump for (process #2) msbuild.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Pocomail, Comodo IceDragon, BlackHawk, Opera Mail, Internet Explorer, Flock, Cyberfox, OpenVPN, I... ...lorer / Edge, The Bat!, SeaMonkey, Mozilla Thunderbird, k-Meleon, IncrediMail, Mozilla Firefox, Opera, Postbox, Microsoft Outlook.			
4/5	System Modification	Modifies network configuration	1	-
	• (Process #2) msbuild.exe modifies the host.conf file, probably to redirect network traffic.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #2) msbuild.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\ykVBUY\ykVBUY.exe".			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe modifies memory of (process #2) msbuild.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #1) 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe alters context of (process #2) msbuild.exe.			
3/5	Input Capture	Monitors keyboard input	1	Keylogger
	• (Process #2) msbuild.exe installs system wide "WH_KEYBOARD_LL" hook(s) to monitor keystrokes.			
2/5	Defense Evasion	Sends control codes to connected devices	3	-
	• (Process #5) wmiprvse.exe controls device "\\.\{9E8A7ED5-49C8-421B-A782-D46C28931105}" through API DeviceIOControl. • (Process #5) wmiprvse.exe controls device "\\.\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}" through API DeviceIOControl. • (Process #5) wmiprvse.exe controls device "\\.\{E96D977E-F067-4CE9-924D-F6E0A04729E4}" through API DeviceIOControl.			
2/5	Data Collection	Reads sensitive browser data	9	-
	• (Process #2) msbuild.exe tries to read sensitive data of web browser "Opera" by file. • (Process #2) msbuild.exe tries to read sensitive data of web browser "Comodo IceDragon" by file. • (Process #2) msbuild.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #2) msbuild.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #2) msbuild.exe tries to read sensitive data of web browser "Flock" by file. • (Process #2) msbuild.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault. • (Process #2) msbuild.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #2) msbuild.exe tries to read sensitive data of web browser "BlackHawk" by file. • (Process #2) msbuild.exe tries to read sensitive data of web browser "k-Meleon" by file.			

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive mail data	7	-
	• (Process #2) msbuild.exe tries to read sensitive data of mail application "Postbox" by file. • (Process #2) msbuild.exe tries to read sensitive data of mail application "The Bat!" by file. • (Process #2) msbuild.exe tries to read sensitive data of mail application "IncrediMail" by registry. • (Process #2) msbuild.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file. • (Process #2) msbuild.exe tries to read sensitive data of mail application "Pocomail" by file. • (Process #2) msbuild.exe tries to read sensitive data of mail application "Opera Mail" by file. • (Process #2) msbuild.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.		
2/5	Data Collection	Reads sensitive application data	2	-
	• (Process #2) msbuild.exe tries to read sensitive data of application "OpenVPN" by registry. • (Process #2) msbuild.exe tries to read sensitive data of application "SeaMonkey" by file.		
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #2) msbuild.exe queries OS version via WMI.		
2/5	Discovery	Executes WMI query	2	-
	• (Process #2) msbuild.exe executes WMI query: select * from Win32_OperatingSystem. • (Process #2) msbuild.exe executes WMI query: SELECT * FROM Win32_Processor.		
2/5	Discovery	Collects hardware properties	1	-
	• (Process #2) msbuild.exe queries hardware properties via WMI.		
1/5	Mutex	Creates mutex	1	-
	• (Process #1) 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe creates mutex with name "mwyLJQTCzoERzESbkqhGjwVkw".		
1/5	Privilege Escalation	Enables process privilege	2	-
	• (Process #1) 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe enables process privilege "SeDebugPrivilege". • (Process #2) msbuild.exe enables process privilege "SeDebugPrivilege".		
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe starts (process #1) 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe with a hidden window.		
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe reads from (process #1) 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.		
1/5	System Modification	Modifies operating system directory	1	-
	• (Process #2) msbuild.exe creates file "C:\Windows\system32\drivers\etc\hosts" in the OS directory.		
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #2) msbuild.exe adds "C:\Users\RDhJ0CNFevzX\AppData\Roaming\ykVBUY\ykVBUY.exe" to Windows startup via registry.		
1/5	Discovery	Possibly does reconnaissance	14	-

Score	Category	Operation	Count	Classification
	• (Process #2) msbuild.exe tries to gather information about application "Postbox" by file. • (Process #2) msbuild.exe tries to gather information about application "Comodo IceDragon" by file. • (Process #2) msbuild.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #2) msbuild.exe tries to gather information about application "The Bat!" by file. • (Process #2) msbuild.exe tries to gather information about application "Foxmail" by registry. • (Process #2) msbuild.exe tries to gather information about application "Pocomail" by file. • (Process #2) msbuild.exe tries to gather information about application "Opera Mail" by file. • (Process #2) msbuild.exe tries to gather information about application "Qualcomm Eudora" by registry. • (Process #2) msbuild.exe tries to gather information about application "Flock" by file. • (Process #2) msbuild.exe tries to gather information about application "Cyberfox" by file. • (Process #2) msbuild.exe tries to gather information about application "blackHawk" by file. • (Process #2) msbuild.exe tries to gather information about application "k-Meleon" by file. • (Process #2) msbuild.exe tries to gather information about application "icecat" by file. • (Process #2) msbuild.exe tries to gather information about application "SeaMonkey" by file.		
1/5	Network Connection	Performs DNS request	1	-
	• (Process #2) msbuild.exe resolves host name "api.telegram.org" to IP "-".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #2) msbuild.exe opens an outgoing TCP connection to host "149.154.167.220:443".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #2) msbuild.exe resolves 51 API functions by name.			
-	Trusted	Known clean file	1	-
	• File "C:\Users\RDhJ0CNFevzX\AppData\Roaming\ykVBUY\ykVBUY.exe" is a known clean file.			

Malware Configuration: AgentTesla

Metadata	Key	Extracted Value
Encryption Key	Key Algorithm	qg== XOR
URL	Url Tags	https://api.telegram.org/bot1698102386:AAHWYbuf-rLmgfOsAgCnA_t8ncjPXSF5S8c/sendDocument Telegram
Other: Telegram Chat ID	Tags Value	Telegram 1131810225

Mitre ATT&CK Matrix

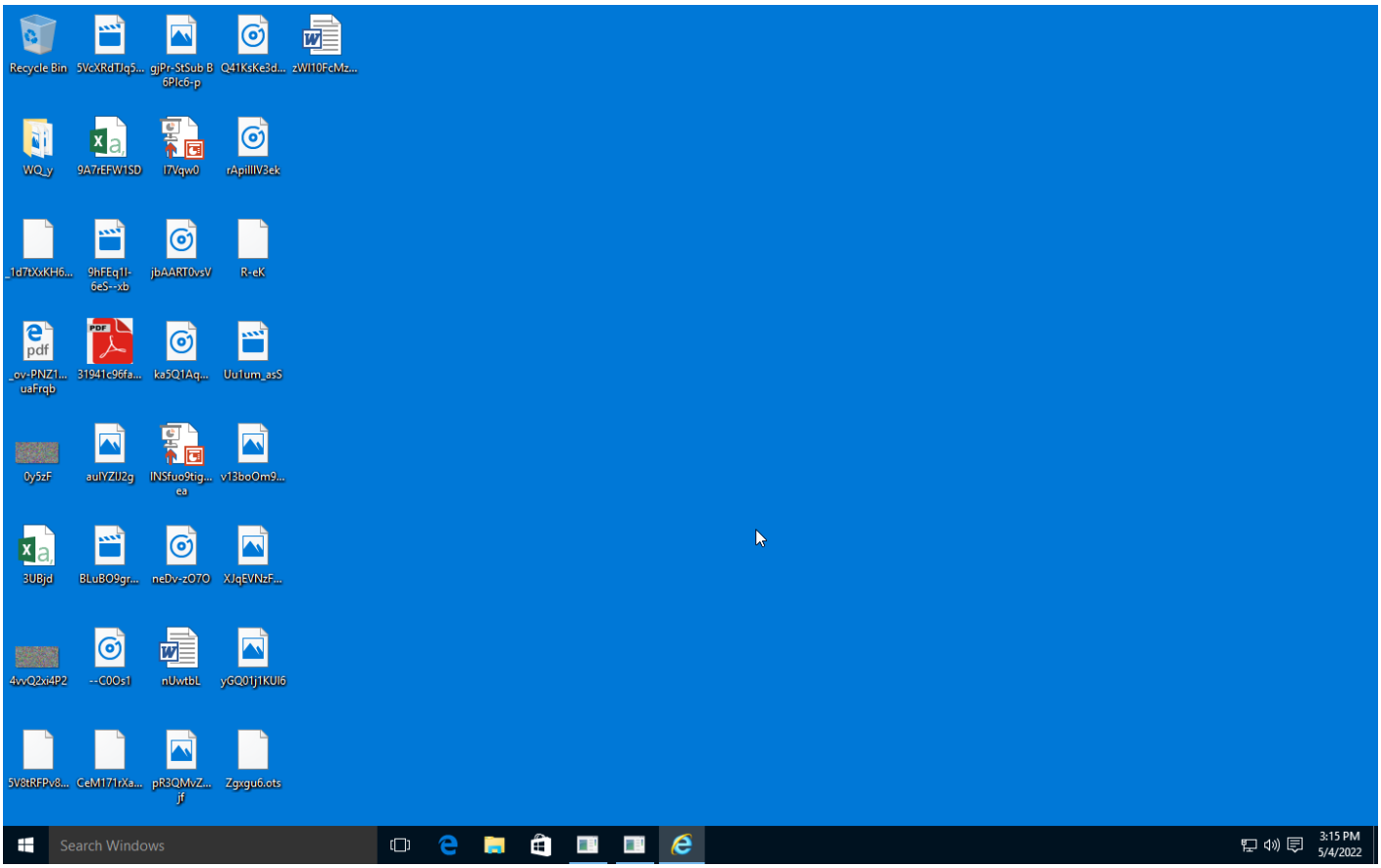
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1060 Registry Run Keys / Startup Folder	#T1179 Hooking	#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection	#T1090 Connection Proxy		
		#T1179 Hooking		#T1045 Software Packing	#T1214 Credentials in Registry	#T1012 Query Registry		#T1005 Data from Local System			
				#T1112 Modify Registry	#T1003 Credential Dumping	#T1082 System Information Discovery		#T1056 Input Capture			
				#T1096 NTFS File Attributes	#T1056 Input Capture						
					#T1179 Hooking						

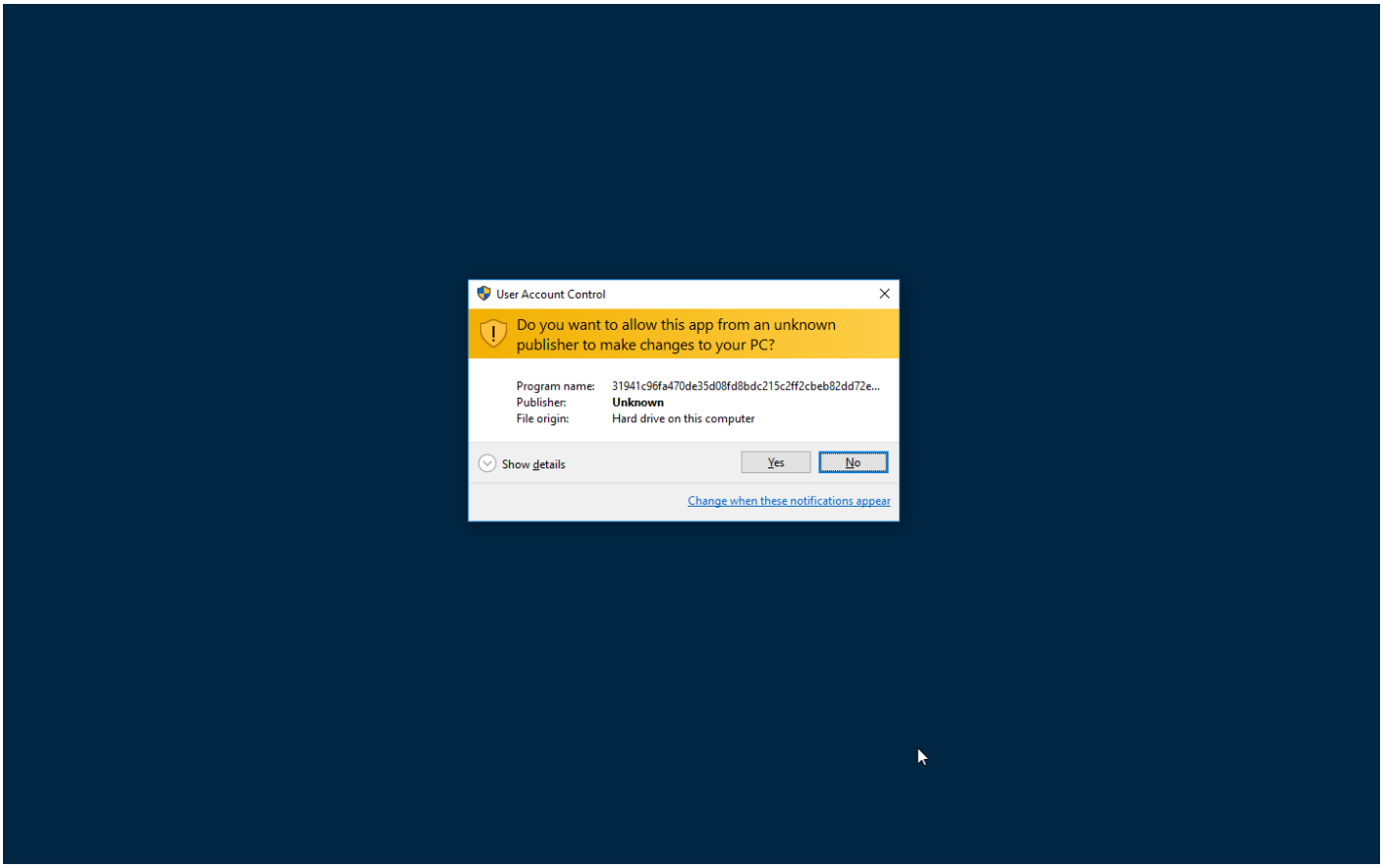
Sample Information

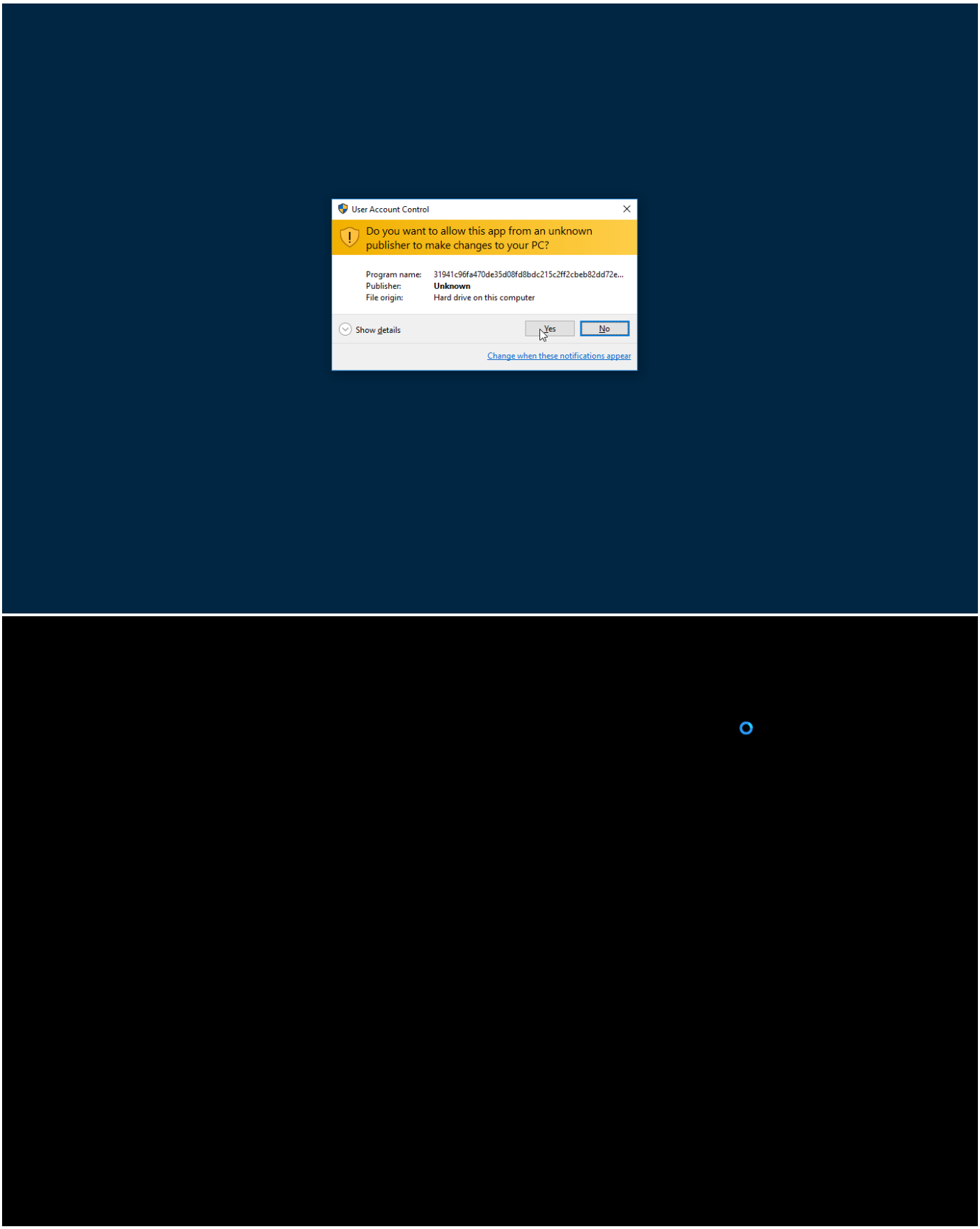
ID	#4259493
MD5	5d5f37a7cf3a9ff4277b3a9dc2c4b9d2
SHA1	1a115c8a1761ef2a2cf61d854d1d2c201c902d53
SHA256	31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969
SSDeep	12288:22L2lOI6QPAc9lIZx2tDPG2xMN1HHG05LZ524R8douFvjkntY9DTVYCsK5iZ1:22j6gz92AtDPGaMnnRBZ7+1F70481Z
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe
File Size	673.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-05-04 17:14 (UTC+2)
Analysis Duration	00:03:40
Termination Reason	Timeout
Number of Monitored Processes	4
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	2


Recycle Bin
Search Windows
3:15 PM
5/4/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

1.94 KB total sent

7.32 KB total received

2 ports 443, 53

2 contacted IP addresses

2 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

0 URLs contacted, 0 servers

1 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	http://api.telegram.org/bot1698102386:AAHWYbuf-rLmgfOsAgCnA_t8ncjPXSF5S8c/sendDocument	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	api.telegram.org	NO_ERROR			NA

BEHAVIOR

Process Graph

Process #1: 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 103225, Reason: Analysis Target
Unmonitor End Time	End Time: 197725, Reason: Terminated
Monitor duration	94.50s
Return Code	0
PID	1900
Parent PID	1932
Bitness	32 Bit

Host Behavior

Type	Count
Module	83
Window	6
System	4
Process	1
-	3
File	1
Mutex	2
-	7
Registry	3
User	1

Process #2: msbuild.exe

ID	2
File Name	c:\windows\microsoft.net\framework\v4.0.30319\msbuild.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 195456, Reason: Child Process
Unmonitor End Time	End Time: 262496, Reason: Terminated
Monitor duration	67.04s
Return Code	1073807364
PID	4784
Parent PID	1900
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\31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe	0x12cc	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe	0x12cc	0x402000(4202496)	0x34000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe	0x12cc	0x436000(4415488)	0x2cc00	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe	0x12cc	0x464000(4603904)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe	0x12cc	0x3ec008(4112392)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe	0x12cc / 0x2fc	0x435f7e(4415358)	-	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\ykVBUY\ykVBUY.exe	254.30 KB	2c75ad03937eee1046942d48b0fdc366e908dc00a5defc8f3b9513c7821a78b8	✖

Host Behavior

Type	Count
Module	67
COM	39
File	139
-	29

Type	Count
Registry	83
System	26
User	4
Environment	16
Window	6
-	3
-	1

Network Behavior

Type	Count
HTTP	1
DNS	1
TCP	2

Process #3: svchost.exe

ID	3
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: 206864, Reason: RPC Server
Unmonitor End Time	End Time: 321592, Reason: Terminated by timeout
Monitor duration	114.73s
Return Code	Unknown
PID	868
Parent PID	4784
Bitness	64 Bit

Process #5: wmiprvse.exe

ID	5
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 206864, Reason: RPC Server
Unmonitor End Time	End Time: 321592, Reason: Terminated by timeout
Monitor duration	114.73s
Return Code	Unknown
PID	3608
Parent PID	868
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
System	10
File	6
-	6
Registry	6

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969	C:\Users\RDhJ0CNFevzX\Desktop\31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe	Sample File	673.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
2c75ad03937eee1046942d48b0fdc366e908dc00a5defc8f3b9513c7821a78b8	C:\Users\RDhJ0CNFevzX\AppData\Roaming\ykVBUY\ykVBUY.exe	Dropped File	254.30 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	CLEAN
9b13a3ea948a1071a81787aac1930b89e30df22ce13f8ff751f31b5d83e79ffb	C:\Windows\system32\drivers\etc\hosts	Accessed File	835 bytes	text/plain	Access, Create, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe	Sample File, VM File	-	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Claws-mail	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe.config	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\Chromium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Protect\S-1-5-21-1560258661-3990802383-1811730007-1000\26d4f968-a540-431b-ab1b-a50e9bbda5d1	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data\Default\EncryptedStorage	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Mail\Opera Mail\wand.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\plutil.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\falkon\profiles\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\ykVBUY\	Accessed File	Access, Create	CLEAN
\\.\{E25A642B-6CEB-4194-8F83-8BC82AF94F5A}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Claws-mail\clawsrc	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\profiles.ini	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Comodo\IceDragon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\icecat\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Trillian\users\global\accounts.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data	Accessed File	Access	CLEAN
C:\Windows\system32\drivers\etc\hosts	Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Waterfox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Mailbird\Store\Store.db	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
\\.\{9E8A7ED5-49C8-421B-A782-D46C28931105}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files (x86)\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data	Accessed File	Access	CLEAN
\\.\{017EF944-8C88-42C3-8F92-C8F7B6022F8D}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\NordVPN	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\The Bat!	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\ykVBUY\ykVBUY.exe	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Storage\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\MySQL\Workbench\workbench_user_data.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Postbox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Psi+\profiles	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data	Accessed File	Access	CLEAN
C:\mail\	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe.Config	Accessed File	Access, Read	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHawk\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Pocomail\accounts.ini	Accessed File	Access	CLEAN
\\.\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
\\.\{E4D2000A-6025-4C58-8789-AF7349886E11}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Psi\profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\eM Client	Accessed File	Access	CLEAN
\\.\{E96D977E-F067-4CE9-924D-F6E0A04729E4}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Flock\Browser\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Folder.lst	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\ykVBUY\ykVBUY.exe:Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://api.telegram.org/bot1698102386:AAHWYbuf-rLmgfOsAgCnA_t8ncjPXSF5S8c/sendDocument	-	149.154.167.220	-	-	MALICIOUS
http://api.telegram.org/bot1698102386:AAHWYbuf-rLmgfOsAgCnA_t8ncjPXSF5S8c/sendDocument	-	149.154.167.220	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
api.telegram.org	149.154.167.220	-	DNS, HTTPS, TCP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
mwyLJQTCzoERzESbkqhGjwVkw	access	31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\RimArts\B2\Settings	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Qualcomm\Eudora\CommandLine	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	msbuild.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	msbuild.exe, 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\OpenVPN-GUI\configs	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\FoxmailPreview	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	msbuild.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\ykVBUY	read, write, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	msbuild.exe, 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	msbuild.exe, 31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	msbuild.exe	CLEAN

Process

Process Name	Commandline	Verdict
31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe	"C:\Users\RDhJ0CNFevzX\Desktop\31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969.exe"	MALICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
msbuild.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe"	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Web Request	-	Spyware	5/5
Malware	AgentTesla_StringDecryption_v3	Agent Tesla v3 string decryption	Memory Dump	-	Spyware	5/5

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	4.5.0
Dynamic Engine Version	4.5.0 / 04/22/2022 19:04
Static Engine Version	4.5.0.0 / 2022-04-22 17:45:13
AV Exceptions Version	4.5.0.2 / 2022-04-03 15:57:54
Link Detonation Heuristics Version	4.5.0.19 / 2022-04-20 05:46:11
Smart Memory Dumping Rules Version	4.5.0.2 / 2022-04-03 15:57:54
Config Extractors Version	4.5.0.14 / 2022-04-07 17:00:08
Signature Trust Store Version	4.5.0.2 / 2022-04-03 15:57:54
VMRay Threat Identifiers Version	4.5.0.24 / 2022-04-26 09:10:00
YARA Built-in Ruleset Version	4.5.0.2

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