MALICIOUS

Classifications: Injector | Exploit | Keylogger | Spyware | Downloader

Threat Names: AgentTesla | AgentTesla.v3 | Mal/HTMLGen-A | Mal/Generic-S

Verdict Reason: -

Sample Type	**Excel Document**
File Name	**831518fee7137eb607ad0fd8b629784dd692f981f6060465079945a13dba6c4c.xlsx**
ID	#5067668
MD5	d0cd467a481799f5dc06a498e24ff4ad
SHA1	da919b490b8192eab7c577b4a85337d09eb56a9e
SHA256	831518fee7137eb607ad0fd8b629784dd692f981f6060465079945a13dba6c4c
File Size	2753.01 KB
Report Created	2022-08-05 14:56 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (35 rules, 93 matches)

Score	Category	Operation	Count	Classification
5/5	Input Capture	Monitors keyboard input	1	Keylogger
	• (Process #4) powershell_ise.exe installs system wide "WH_KEYBOARD_LL" hook(s) to monitor keystrokes.			
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/bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument". • Rule "AgentTesla_StringDecryption_v3" from ruleset "Malware" has matched on a memory dump for (process #4) powershell_ise.exe.			
5/5	_data_collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Flock, FTP Navigator, Internet Download Manager, Mozilla Thunderbird, Opera Mail, FileZilla, Ipsw... ...rnet Explorer, Comodo IceDragon, Postbox, Opera, OpenVPN, CoreFTP, k-Meleon, Mozilla Firefox, WinSCP, Cyberfox, Microsoft Outlook.			
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
	• Based on a combination of other detections, the sample gathers information about the running system to identify it.			
4/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe reads from (process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe.			
4/5	Defense Evasion	Sends control codes to connected devices	3	-
	• (Process #6) wmiprvse.exe controls device "\\.\{9E8A7ED5-49C8-421B-A782-D46C28931105}" through API DeviceIOControl. • (Process #6) wmiprvse.exe controls device "\\.\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}" through API DeviceIOControl. • (Process #6) wmiprvse.exe controls device "\\.\{E96D977E-F067-4CE9-924D-F6E0A04729E4}" through API DeviceIOControl.			
4/5	Discovery	Queries OS version via WMI	1	-
	• (Process #4) powershell_ise.exe queries OS version via WMI.			
4/5	Discovery	Executes WMI query	2	-
	• (Process #4) powershell_ise.exe executes WMI query: select * from Win32_OperatingSystem. • (Process #4) powershell_ise.exe executes WMI query: SELECT * FROM Win32_Processor.			
4/5	Discovery	Collects hardware properties	1	-
	• (Process #4) powershell_ise.exe queries hardware properties via WMI.			
4/5	Exploit	Exploits a vulnerability in MS Office	1	Exploit
	• Exploits equation editor vulnerability CVE-2017-11882 or CVE-2018-0802 in MS Office.			
4/5	Network Connection	Performs DNS request	2	-
	• (Process #4) powershell_ise.exe resolves host name "api.telegram.org" to IP "149.154.167.220". • (Process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe resolves host name "cdn.discordapp.com" to IP "162.159.135.233".			

Score	Category	Operation	Count	Classification
4/5	Network Connection	Connects to remote host	3	-
	• (Process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe opens an outgoing TCP connection to host "109.206.241.81:80". • (Process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe opens an outgoing TCP connection to host "162.159.135.233:443". • (Process #4) powershell_ise.exe opens an outgoing TCP connection to host "149.154.167.220:443".		
4/5	Network Connection	Downloads executable	3	Downloader
	• (Process #2) eqnedt32.exe downloads Windows executable via http from https://pkusukoharjo.com/giving/qGTGx.exe. • (Process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe downloads Windows executable via http from https://cdn.discordapp.com/attachments/1001850193580392480/1002961152617222144/seven.dll. • (Process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe downloads Windows executable via http from http://109.206.241.81/htdocs/zTALg.exe.		
4/5	Network Connection	Downloads file	1	Downloader
	• (Process #4) powershell_ise.exe downloads file via http from https://api.telegram.org/bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument.		
4/5	Network Connection	Attempts to connect through HTTP	1	-
	• (Process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe connects to http://109.206.241.81/htdocs/zTALg.exe.		
4/5	Network Connection	Attempts to connect through HTTPS	3	-
	• (Process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe connects to https://cdn.discordapp.com/attachments/1001850193580392480/1002961152617222144/seven.dll. • (Process #2) eqnedt32.exe connects to https://pkusukoharjo.com/giving/qGTGx.exe. • (Process #4) powershell_ise.exe connects to https://api.telegram.org/bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument.		
4/5	Network Connection	Sends data via a Telegram bot	1	-
	• (Process #4) powershell_ise.exe sends data via Telegram method sendDocument.		
4/5	Exploit	Possible exploitation attempt	1	Exploit
	• Office document may try to exploit a common vulnerability or exposure (CVE): CVE-2017-11882.		
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe modifies memory of (process #4) powershell_ise.exe.		
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe alters context of (process #4) powershell_ise.exe.		
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels embedded file "" as Mal/Generic-S. • Reputation analysis labels the sample itself as Mal/Generic-S.		
4/5	Reputation	Contacts known malicious URL	3	-
	• Reputation analysis labels the URL "https://cdn.discordapp.com/attachments/1001850193580392480/1002961152617222144/seven.dll" which was contacted by (process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe as Mal/HTMLGen-A. • (Process #2) eqnedt32.exe contacted known malicious URL https://pkusukoharjo.com/giving/qGTGx.exe. • Reputation analysis labels the URL "http://109.206.241.81/htdocs/zTALg.exe" which was contacted by (process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe as Mal/HTMLGen-A.		
4/5	Reputation	Resolves known malicious domain	1	-
	• Resolved domain "pkusukoharjo.com" is a known malicious domain.		
4/5	Reputation	Contacts known malicious IP address	1	-

Score	Category	Operation	Count	Classification
	• Reputation analysis labels the contacted IP address 109.206.241.81 as Mal/HTMLGen-A.			
4/5	Execution	Document tries to create process	1	-
	• Document creates (process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe.			
3/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe enables process privilege "SeDebugPrivilege".			
3/5	Discovery	Enumerates running processes	1	-
	• (Process #4) powershell_ise.exe enumerates running processes.			
2/5	Discovery	Reads network adapter information	2	-
	• (Process #3) jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe reads the network adapters' addresses by API. • (Process #6) wmiprvse.exe reads the network adapters' addresses by API.			
2/5	_data_collection	Reads sensitive browser data	9	-
	• (Process #4) powershell_ise.exe tries to read sensitive data of web browser "Opera" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of web browser "Flock" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of web browser "k-Meleon" by file. • (Process #4) powershell_ise.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault. • (Process #4) powershell_ise.exe tries to read sensitive data of web browser "Comodo IceDragon" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of web browser "BlackHawk" by file.			
2/5	_data_collection	Reads sensitive application data	6	-
	• (Process #4) powershell_ise.exe tries to read sensitive data of application "WinSCP" by registry. • (Process #4) powershell_ise.exe tries to read sensitive data of application "Internet Download Manager" by registry. • (Process #4) powershell_ise.exe tries to read sensitive data of application "SeaMonkey" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of application "OpenVPN" by registry. • (Process #4) powershell_ise.exe tries to read sensitive data of application "TightVNC" by registry. • (Process #4) powershell_ise.exe tries to read sensitive data of application "TigerVNC" by registry.			
2/5	Discovery	Possibly does reconnaissance	22	-

Score	Category	Operation	Count	Classification
		• (Process #4) powershell_ise.exe tries to gather information about application "WinSCP" by registry. • (Process #4) powershell_ise.exe tries to gather information about application "Flock" by file. • (Process #4) powershell_ise.exe tries to gather information about application "Cyberfox" by file. • (Process #4) powershell_ise.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #4) powershell_ise.exe tries to gather information about application "k-Meleon" by file. • (Process #4) powershell_ise.exe tries to gather information about application "The Bat!" by file. • (Process #4) powershell_ise.exe tries to gather information about application "Pocomail" by file. • (Process #4) powershell_ise.exe tries to gather information about application "icecat" by file. • (Process #4) powershell_ise.exe tries to gather information about application "Qualcomm Eudora" by registry. • (Process #4) powershell_ise.exe tries to gather information about application "SeaMonkey" by file. • (Process #4) powershell_ise.exe tries to gather information about application "Opera Mail" by file. • (Process #4) powershell_ise.exe tries to gather information about application "FlashFXP" by file. • (Process #4) powershell_ise.exe tries to gather information about application "Comodo IceDragon" by file. • (Process #4) powershell_ise.exe tries to gather information about application "FTP Navigator" by file. • (Process #4) powershell_ise.exe tries to gather information about application "WS_FTP" by file. • (Process #4) powershell_ise.exe tries to gather information about application "RealVNC" by registry. • (Process #4) powershell_ise.exe tries to gather information about application "TightVNC" by registry. • (Process #4) powershell_ise.exe tries to gather information about application "TigerVNC" by registry. • (Process #4) powershell_ise.exe tries to gather information about application "Foxmail" by registry. • (Process #4) powershell_ise.exe tries to gather information about application "Postbox" by file. • (Process #4) powershell_ise.exe tries to gather information about application "FileZilla" by file. • (Process #4) powershell_ise.exe tries to gather information about application "blackHawk" by file.		
2/5	_data_collection	Reads sensitive ftp data	4	-
		• (Process #4) powershell_ise.exe tries to read sensitive data of ftp application "CoreFTP" by registry. • (Process #4) powershell_ise.exe tries to read sensitive data of ftp application "FTP Navigator" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of ftp application "Ipswitch WS_FTP" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of ftp application "FileZilla" by file.		
2/5	_data_collection	Reads sensitive mail data	7	-
		• (Process #4) powershell_ise.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of mail application "The Bat!" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of mail application "Pocomail" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of mail application "Opera Mail" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry. • (Process #4) powershell_ise.exe tries to read sensitive data of mail application "Postbox" by file. • (Process #4) powershell_ise.exe tries to read sensitive data of mail application "IncrediMail" by registry.		
2/5	Heuristics	Contains known suspicious class identifier	1	-
		• Office document contains suspicious class identifier for ActiveX object "Equation2" (CLSID {0002CE02-0000-0000-C000-000000000046}).		

Malware Configuration: AgentTesla

Metadata	Key	Extracted Value
Encryption Key	Key Algorithm	qg== XOR
URL	Url Tags	https://api.telegram.org/bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument Telegram
Other: Telegram Chat ID	Tags Value	Telegram -624834641

Mitre ATT&CK Matrix

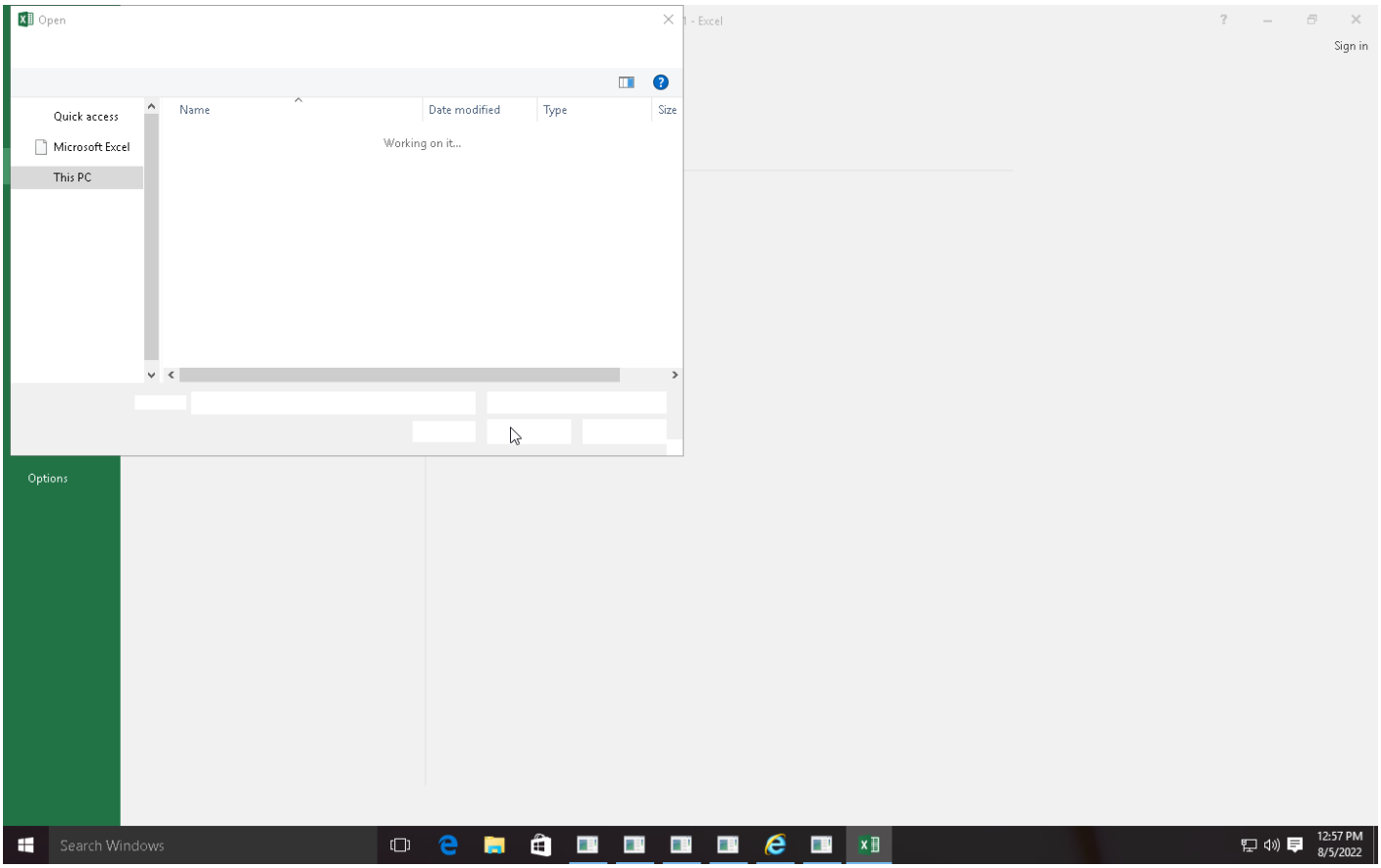
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1179 Hooking	#T1179 Hooking		#T1081 Credentials in Files	#T1016 System Network Configuration Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol	#T1048 Exfiltration Over Alternative Protocol	
	#T1203 Exploitation for Client Execution				#T1214 Credentials in Registry	#T1083 File and Directory Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
					#T1003 Credential Dumping	#T1012 Query Registry		#T1056 Input Capture	#T1032 Standard Cryptographic Protocol		
					#T1056 Input Capture	#T1082 System Information Discovery					
					#T1179 Hooking	#T1057 Process Discovery					

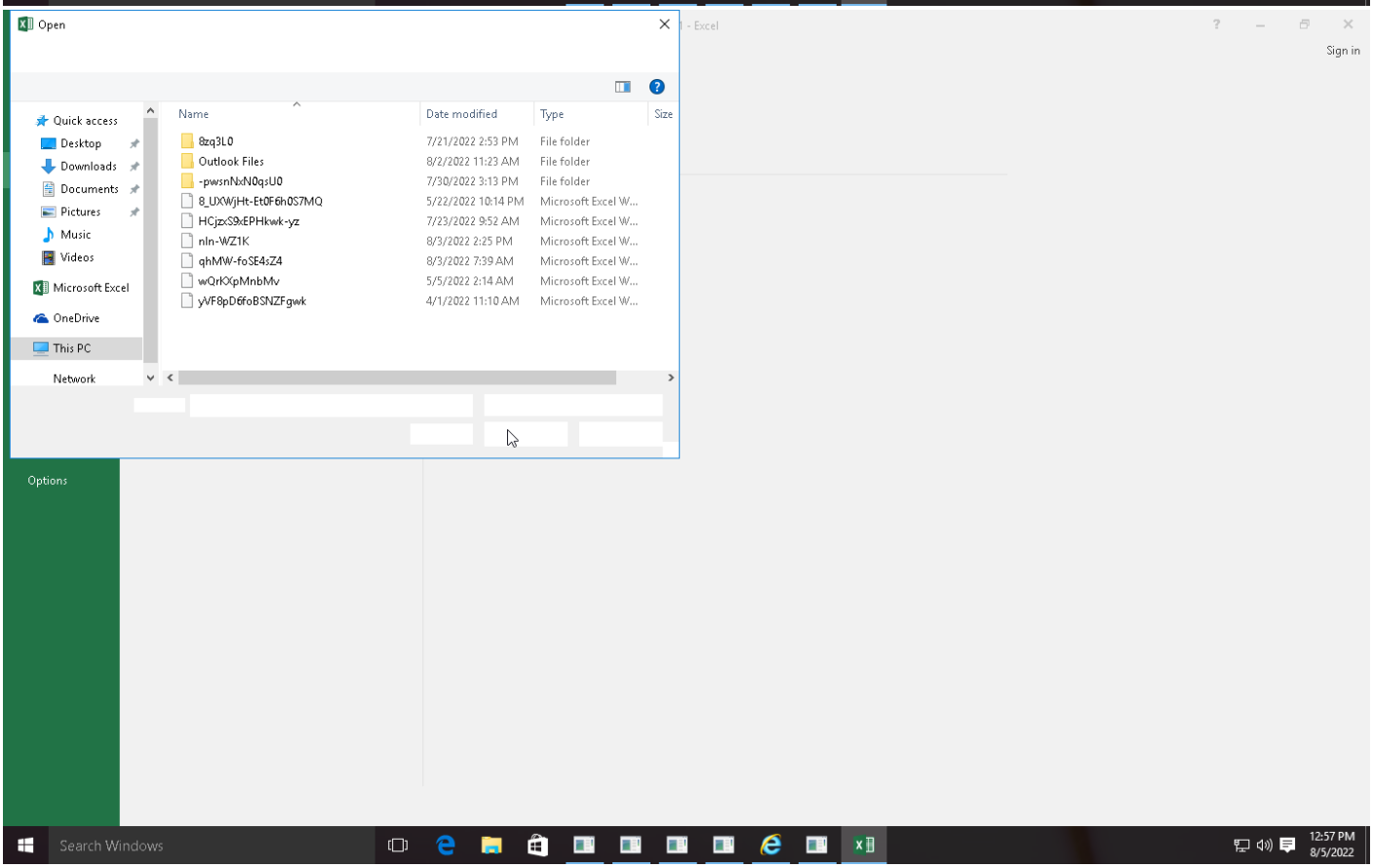
Sample Information

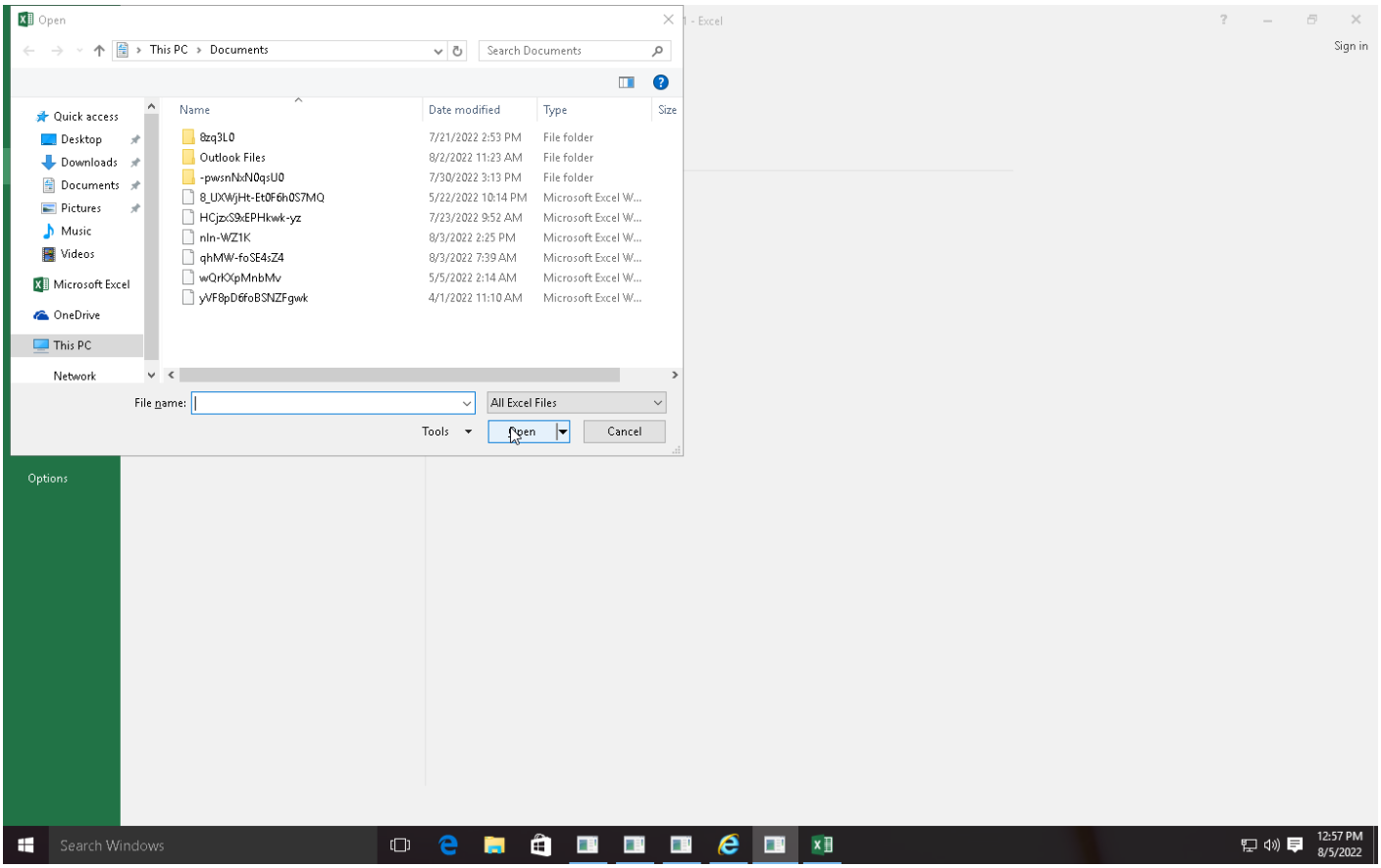
ID	#5067668
MD5	d0cd467a481799f5dc06a498e24ff4ad
SHA1	da919b490b8192eab7c577b4a85337d09eb56a9e
SHA256	831518fee7137eb607ad0fd8b629784dd692f981f6060465079945a13dba6c4c
SSDeep	49152:4yFhEeXk7Vs4O7VhPiiw176tK5fpiB+VkAT5H0T9DpZvIfp+INtJz:4uXmijhhPDwNgiBiBuTG1lx+IN3
File Name	831518fee7137eb607ad0fd8b629784dd692f981f6060465079945a13dba6c4c.xlsx
File Size	2753.01 KB
Sample Type	Excel Document
Has Macros	✔

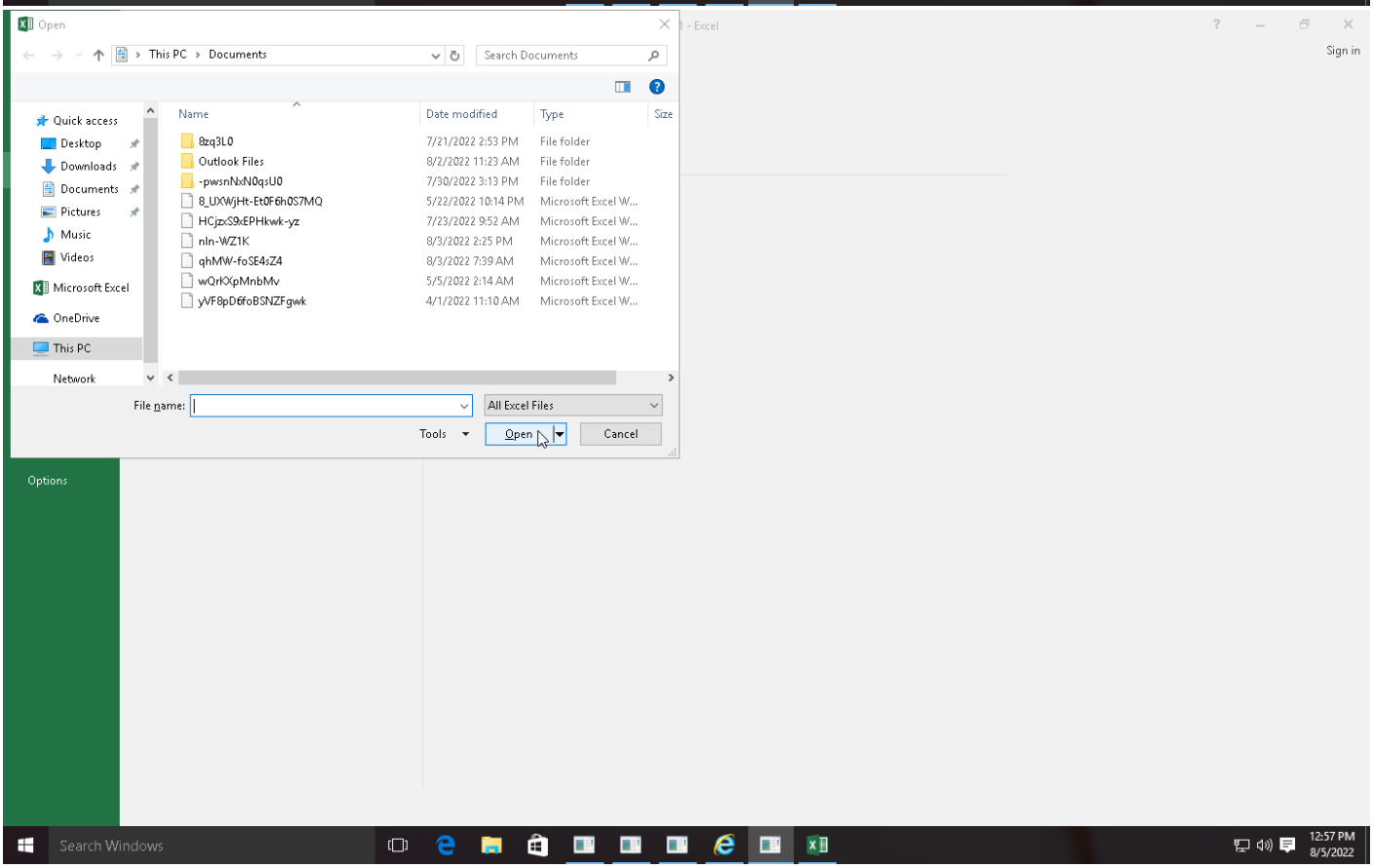
Analysis Information

Creation Time	2022-08-05 14:56 (UTC+2)
Analysis Duration	00:04:06
Termination Reason	Timeout
Number of Monitored Processes	6
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


Open
Quick access
Microsoft Excel
This PC
Name
Date modified
Type
Size
Working on it...
Options
Sign in
Search Windows
12:57 PM
8/5/2022


Open
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
Microsoft Excel
OneDrive
This PC
Network
Name
Date modified
Type
Size
8zq3L0 7/21/2022 2:53 PM File folder
Outlook Files 8/2/2022 11:23 AM File folder
-pwsnNxN0qsU0 7/30/2022 3:13 PM File folder
8_UXWjHt-Et0F6h0S7MQ 5/22/2022 10:14 PM Microsoft Excel W...
HCjzxS9xEPHkwk-yz 7/23/2022 9:52 AM Microsoft Excel W...
nln-WZ1K 8/3/2022 2:25 PM Microsoft Excel W...
qhMW-foSE4sZ4 8/3/2022 7:39 AM Microsoft Excel W...
wQrkXpMnbMv 5/5/2022 2:14 AM Microsoft Excel W...
yVF8pD6foBSNZFgwk 4/1/2022 11:10 AM Microsoft Excel W...
Options
Sign in
Search Windows
12:57 PM
8/5/2022





Screenshots truncated

NETWORK

General

9.55 KB total sent

332.90 KB total received

4 ports 80, 443, 53, 445

5 contacted IP addresses

0 URLs extracted

4 files downloaded

0 malicious hosts detected

DNS

3 DNS requests for 3 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

4 URLs contacted, 4 servers

4 sessions, 6.60 KB sent, 330.33 KB received

HTTP Requests

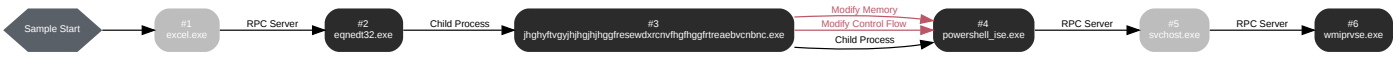
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://109.206.241.81/htdocs/zTALg.exe	-	-		0 bytes	NA
GET	https://pkusukoharjo.com/giving/qGTGx.exe	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/1001850193580392480/1002961152617222144/seven.dll	-	-		0 bytes	NA
POST	https://api.telegram.org/bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	api.telegram.org	NO_ERROR	149.154.167.220		NA
A	pkusukoharjo.com	NO_ERROR	136.243.86.20		NA
A	cdn.discordapp.com	NO_ERROR	162.159.135.233, 162.159.130.233, 162.159.134.233, 162.159.129.233, 162.159.133.233		NA

BEHAVIOR

Process Graph



Process #1: excel.exe

ID	1
File Name	c:\program files (x86)\microsoft office\office16\excel.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 62399, Reason: Analysis Target
Unmonitor End Time	End Time: 309137, Reason: Terminated by timeout
Monitor duration	246.74s
Return Code	Unknown
PID	4840
Parent PID	1972
Bitness	32 Bit

Process #2: eqnedt32.exe

ID	2
File Name	c:\program files (x86)\common files\microsoft shared\equation\eqnedt32.exe
Command Line	"C:\Program Files (x86)\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 96770, Reason: RPC Server
Unmonitor End Time	End Time: 127289, Reason: Terminated
Monitor duration	30.52s
Return Code	0
PID	3112
Parent PID	4840
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	8.50 KB	41bf0e9b141cb3541ce14ca9de7f606fd30c20e02ce95936f41fb728bd6c2232	✖

Host Behavior

Type	Count
Module	15
File	7
System	2
Environment	1
-	1
Mutex	2
Process	1

Network Behavior

Type	Count
HTTPS	1

Process #3: jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 115170, Reason: Child Process
Unmonitor End Time	End Time: 148478, Reason: Terminated
Monitor duration	33.31s
Return Code	1
PID	2996
Parent PID	3112
Bitness	32 Bit

Host Behavior

Type	Count
Registry	33
Module	752
Window	4
-	10
File	18
User	1
System	5
Environment	8
-	1
Process	1
-	3
-	7

Network Behavior

Type	Count
HTTP	1
HTTPS	1
DNS	1
TCP	2

Process #4: powershell_ise.exe

ID	4
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell_ise.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 146427, Reason: Child Process
Unmonitor End Time	End Time: 309137, Reason: Terminated by timeout
Monitor duration	162.71s
Return Code	Unknown
PID	4488
Parent PID	2996
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#3: c:\users\rdhj0cnfevzx\appdata\roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe	0x9e0	0x400000(4194304)	0x200	✔	1
Modify Memory	#3: c:\users\rdhj0cnfevzx\appdata\roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe	0x9e0	0x402000(4202496)	0x33c00	✔	1
Modify Memory	#3: c:\users\rdhj0cnfevzx\appdata\roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe	0x9e0	0x436000(4415488)	0x400	✔	1
Modify Memory	#3: c:\users\rdhj0cnfevzx\appdata\roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe	0x9e0	0x438000(4423680)	0x200	✔	1
Modify Memory	#3: c:\users\rdhj0cnfevzx\appdata\roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe	0x9e0	0x253008(2437128)	0x4	✔	1
Modify Control Flow	#3: c:\users\rdhj0cnfevzx\appdata\roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe	0x9e0 / 0x1184	0x435bce(4414414)	-	✔	1

Host Behavior

Type	Count
-	28
Registry	104
File	207
User	4
Module	72
System	69
COM	38
Environment	43

Type	Count
-	3
-	1
Window	6
Process	3
Keyboard	96

Network Behavior

Type	Count
HTTPS	1
DNS	1
TCP	1

Process #5: svchost.exe

ID	5
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: 150123, Reason: RPC Server
Unmonitor End Time	End Time: 309137, Reason: Terminated by timeout
Monitor duration	159.01s
Return Code	Unknown
PID	864
Parent PID	4488
Bitness	64 Bit

Process #6: wmiprvse.exe

ID	6
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: 150123, Reason: RPC Server
Unmonitor End Time	End Time: 309137, Reason: Terminated by timeout
Monitor duration	159.01s
Return Code	Unknown
PID	4220
Parent PID	864
Bitness	64 Bit

Host Behavior

Type	Count
System	10
Registry	6
Module	20
File	5
-	6

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
831518fee7137eb607ad0fd8b629784dd692f981f6060465079945a13dba6c4c	C:\Users\RDhJ0CNFevzX\Desktop\831518fee7137eb607ad0fd8b629784dd692f981f6060465079945a13dba6c4c.xlsx	Sample File	2753.01 KB	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	-	MALICIOUS
41bf0e9b141cb3541ce14ca9de7f606fd30c20e02ce95936f41fb728bd6c2232	C:\Users\RDhJ0CNFevzX\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe	Downloaded File	8.50 KB	application/vnd.microsoft.portable-executable	Access, Create	MALICIOUS
3cdf585582fd700e93ed92a047164e75dd9c566077f6a8439cb22bcda6eaa1e0	-	Downloaded File	209.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
653f8662e65e224b05605b256bb4f6de5f29f2b155dc4477635b8e43024503e4	image1.png	Extracted File	8.02 KB	image/png	-	CLEAN
07a1fc33a407e2501619398a477d2eae23a3c1739113171f566c0140c898116f	-	Extracted File	2937.52 KB	application/octet-stream	-	CLEAN
a3c9a7a1cdec5c9d295110e47dc2bb0298b736d3450b11d64391a927f3dfd537	-	Downloaded File	85.00 KB	application/vnd.microsoft.portable-executable	-	CLEAN
a88a085369275032efda07d3ad2e49bda80a25fd5263bb1571d28465d2b0986c	-	Downloaded File	649 bytes	application/json	-	CLEAN
02ea45ab816d1a7a04b5a026fb0303130a3ae47be3da47a9f67effb071015259	dbSYXB9S.Pu6cL	Extracted File	2963.50 KB	application/CDFV2	-	CLEAN
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	-	Modified File	128 bytes	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\831518fee7137eb607ad0fd8b629784dd692f981f6060465079945a13dba6c4c.xlsx	Sample File, VM File	-	MALICIOUS
C:\Windows\SYSTEM32\rasman.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\CRYPTBASE.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\IMM32.DLL	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Flock\Browser\	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data\Default\EncryptedStorage	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Postbox\	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\VERSION.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data	Accessed File	Access	CLEAN
C:\Windows\system32\apphelp.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files (x86)\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\GDI32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\combase.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ADVAPI32.dll	Accessed File	Access	CLEAN
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.10586.0_none_811bc0006c44242b\comctl32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\SspiCli.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Trillian\users\global\accounts.dat	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ole32.dll	Accessed File	Access	CLEAN
\\.\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\powrprof.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Ipswitch\WS_FTP\Sites\ws_ftp.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Psi\profiles	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\USER32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSVCR120_CLR0400.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\falkon\profiles\profiles.ini	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\ProgramData\FlashFXP\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Claws-mail	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\mskeyprotect.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\UCBrowser\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\profiles.ini	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\SYSTEM32\windows.storage.dll	Accessed File	Access	CLEAN
C:\Program Files\Private Internet Access\data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Waterfox\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\bcrypt.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\SHLWAPI.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ncrypt.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\uvnc bvba\UltraVNC\ultravnc.ini	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Psi+\profiles	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\CRYPT32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\uxtheme.dll	Accessed File	Access	CLEAN
C:\Private Internet Access\data	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell_ise.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\psapi.dll	Accessed File	Access	CLEAN
image1.png	-	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\	Accessed File	Access	CLEAN
\\.\{E25A642B-6CEB-4194-8F83-8BC82AF94F5A}	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\winhttp.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\NTASN1.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\shcore.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe	Accessed File, Downloaded File, Extracted File	Access, Create	CLEAN
C:\Windows\SYSTEM32\WINNSI.DLL	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	Accessed File	Access, Read	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Mail\Opera Mail\wand.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\SeaMonkey\	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Windows\System32\fwpuclnt.dll	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\rphr8qg5\qgtgx[1].exe	Downloaded File, Extracted File	-	CLEAN
C:\Windows\SYSTEM32\MSCOREE.DLL	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\schannel.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\NordVPN	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\jDownloader\config\database.script	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Comodo\IceDragon\	Accessed File	Access	CLEAN
\\.\{9E8A7ED5-49C8-421B-A782-D46C28931105}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\secur32.dll	Accessed File	Access	CLEAN
C:\Storage\	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FTPGetter\servers.xml	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSASN1.dll	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FlashFXP\	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\rasapi32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\msvbvm60.DLL	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Waterfox\profiles.ini	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\shell32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ondemandconnroutehelper.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\SYSTEM32\bcryptPrimitives.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\MySQL\Workbench\workbench_user_data.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
dbSYXB9S.Pu6cL	-	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN
C:\Windows\system32\dwmapi.dll	Accessed File	Access	CLEAN
C:\cftp\Ftplist.txt	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHawk\profiles.ini	Accessed File	Access	CLEAN
C:\FTP Navigator\Ftplist.txt	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\sechost.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\icecat\profiles.ini	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\NSI.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\IPHLPAPI.DLL	Accessed File	Access	CLEAN
\\.\{017EF944-8C88-42C3-8F92-C8F7B6022F8D}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Mailbird\Store\Store.db	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Postbox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Flock\Browser\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\profiles.ini	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ws2_32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\cfgmgr32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\The Bat!	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\KERNEL32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe.config	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\plutil.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\UltraVNC\ultravnc.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Comodo\IceDragon\profiles.ini	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\OLEAUT32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\KERNELBASE.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\RPCRT4.dll	Accessed File	Access	CLEAN
C:\Windows\system32\ncryptsslp.dll	Accessed File	Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://cdn.discordapp.com/attachments/1001850193580392480/1002961152617222144/seven.dll	-	162.159.130.233, 162.159.133.233, 162.159.135.233, 162.159.129.233, 162.159.134.233	-	GET	MALICIOUS
https://pkusukoharjo.com/giving/qGTGx.exe	-	136.243.86.20	-	GET	MALICIOUS
https://api.telegram.org/bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument	-	149.154.167.220	-	POST	MALICIOUS
http://109.206.241.81/htdocs/zTALg.exe	-	109.206.241.81	-	GET	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
pkusukoharjo.com	136.243.86.20	-	TCP, HTTPS, DNS	MALICIOUS
api.telegram.org	149.154.167.220	-	TCP, HTTPS, DNS	CLEAN
cdn.discordapp.com	162.159.130.233, 162.159.133.233, 162.159.135.233, 162.159.129.233, 162.159.134.233	-	TCP, HTTPS, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
162.159.135.233	cdn.discordapp.com	-	TCP, HTTPS, DNS	MALICIOUS
149.154.167.220	api.telegram.org	United Kingdom	TCP, HTTPS, DNS	MALICIOUS
109.206.241.81	-	United States	TCP, HTTP	MALICIOUS
162.159.133.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.130.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.129.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.134.233	cdn.discordapp.com	-	DNS	CLEAN
136.243.86.20	pkusukoharjo.com	Germany	TCP, HTTPS, DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
-	delete, access	eqnedt32.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\DownloadManager\Passwords	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TightVNC\Server	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TigerVNC\Server	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\vncserver	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\TigerVNC\Server	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	read, access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\FoxmailPreview	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\RimArts\B2\Settings	access	powershell_ise.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	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\vncserver	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\ORL\WinVNC3	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\DynamicDST	access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\WinVNC4	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Qualcomm\Eudora\CommandLine	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\FTPWare\COREFTP\Sites	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	read, access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\TightVNC\Server	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\OpenVPN-GUI\configs	access	powershell_ise.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions	access	powershell_ise.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	powershell_ise.exe	CLEAN

Process

Process Name	Commandline	Verdict
jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe	C:\Users\RDhJ0CNFevzX\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe	MALICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
eqnedt32.exe	"C:\Program Files (x86)\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding	SUSPICIOUS
powershell_ise.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe"	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
excel.exe	"C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE"	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	4.6.0
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