MALICIOUS

Classifications: Spyware | Keylogger | Backdoor

Threat Names: Mal/Generic-S | AsyncRAT

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe**
ID	#6646108
MD5	c7fbe52e88456eabb4d4a1a1a0670cf4
SHA1	3b479f15645c31c7067c31aede6e1802093ac78b
SHA256	82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746
File Size	335.50 KB
Report Created	2023-01-19 00:45 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (28 rules, 98 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 #10) wwst.exe. • Rule "AsyncRAT" from ruleset "RATs" has matched on a memory dump for (process #8) windowsdatac.exe. • Rule "AsyncRAT" from ruleset "RATs" has matched on the dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\wwst.exe".			
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
	• Sample enumerates processes, queries network configuration, collects hardware information and collects operating system information which indicates system fingerprinting.			
5/5	Data Collection	Combination of other detections shows multiple input capture behaviors	1	Spyware
	• (Process #10) wwst.exe takes screenshots and potentially exfiltrates data.			
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels the sample itself as Mal/Generic-S. • Reputation analysis labels file "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\RunIt.exe" as Mal/Generic-S.			
3/5	Data Collection	Takes screenshot	1	-
	• (Process #10) wwst.exe takes a screenshot using BitBlt API.			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #10) wwst.exe tries to detect antivirus software via WMI query: "Select * from AntivirusProduct".			
2/5	Discovery	Executes WMI query	11	-
	• (Process #3) wwst.exe executes WMI query: SELECT * FROM Win32_Processor. • (Process #3) wwst.exe executes WMI query: SELECT * FROM Win32_VideoController. • (Process #3) wwst.exe executes WMI query: SELECT ExecutablePath, ProcessID FROM Win32_Process. • (Process #10) wwst.exe executes WMI query: SELECT * FROM Win32_Processor. • (Process #10) wwst.exe executes WMI query: SELECT * FROM Win32_VideoController. • (Process #10) wwst.exe executes WMI query: SELECT ExecutablePath, ProcessID FROM Win32_Process. • (Process #10) wwst.exe executes WMI query: SELECT * FROM Win32_PnPEntity WHERE (PNPClass = 'Image' OR PNPClass = 'Camera'). • (Process #10) wwst.exe executes WMI query: SELECT * FROM win32_operatingsystem. • (Process #10) wwst.exe executes WMI query: Select * from AntivirusProduct. • (Process #10) wwst.exe executes WMI query: Select * From Win32_ComputerSystem. • (Process #10) wwst.exe executes WMI query: Select ProcessorId From Win32_processor.			
2/5	Discovery	Collects hardware properties	2	-
	• (Process #3) wwst.exe queries hardware properties via WMI. • (Process #10) wwst.exe queries hardware properties via WMI.			
2/5	Discovery	Enumerates running processes	3	-

Score	Category	Operation	Count	Classification
	• (Process #3) wwst.exe enumerates running processes via WMI. • (Process #10) wwst.exe enumerates running processes via WMI. • (Process #10) wwst.exe enumerates running processes.			
2/5	Defense Evasion	Sends control codes to connected devices	1	-
	• (Process #12) wmiprvse.exe controls device "\\.\C:" through API DeviceIOControl.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #10) wwst.exe queries OS version via WMI.			
2/5	Network Connection	Sets up server that accepts incoming connections	1	Backdoor
	• (Process #10) wwst.exe starts a TCP server listening on port 49680.			
1/5	Persistence	Installs system startup script or application	3	-
	• (Process #1) 82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe adds "C:\ProgramData\WindowsDataC.exe" to Windows startup via registry. • (Process #4) runit.exe adds "C:\Users\RDHJ0C~1\AppData\Local\Temp\Rnts.exe" to Windows startup via registry. • (Process #9) runit.exe adds "C:\Users\RDHJ0C~1\AppData\Local\Temp\Rnts.exe" to Windows startup via registry.			
1/5	Privilege Escalation	Enables process privilege	4	-
	• (Process #3) wwst.exe enables process privilege "SeDebugPrivilege". • (Process #6) wmiprvse.exe enables process privilege "SeDebugPrivilege". • (Process #10) wwst.exe enables process privilege "SeDebugPrivilege". • (Process #12) wmiprvse.exe enables process privilege "SeDebugPrivilege".			
1/5	Hide Tracks	Changes folder appearance	12	-
	• (Process #3) wwst.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Desktop". • (Process #3) wwst.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents". • (Process #3) wwst.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures". • (Process #3) wwst.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Camera Roll". • (Process #3) wwst.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Downloads". • (Process #3) wwst.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Saved Pictures". • (Process #10) wwst.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Desktop". • (Process #10) wwst.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures". • (Process #10) wwst.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents". • (Process #10) wwst.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Downloads". • (Process #10) wwst.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Camera Roll". • (Process #10) wwst.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Saved Pictures".			
1/5	Discovery	Possibly does reconnaissance	14	-

Score	Category	Operation	Count	Classification
		• (Process #3) wwst.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #3) wwst.exe tries to gather information about application "k-Meleon" by file. • (Process #3) wwst.exe tries to gather information about application "Comodo IceDragon" by file. • (Process #3) wwst.exe tries to gather information about application "Cyberfox" by file. • (Process #3) wwst.exe tries to gather information about application "Pidgin" by file. • (Process #3) wwst.exe tries to gather information about application "Steam" by registry. • (Process #3) wwst.exe tries to gather information about application "FileZilla" by file. • (Process #10) wwst.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #10) wwst.exe tries to gather information about application "k-Meleon" by file. • (Process #10) wwst.exe tries to gather information about application "Comodo IceDragon" by file. • (Process #10) wwst.exe tries to gather information about application "Cyberfox" by file. • (Process #10) wwst.exe tries to gather information about application "Pidgin" by file. • (Process #10) wwst.exe tries to gather information about application "Steam" by registry. • (Process #10) wwst.exe tries to gather information about application "FileZilla" by file.		
1/5	Obfuscation	Reads from memory of another process	17	-
		• (Process #6) wmiprvse.exe reads from winlogon.exe. • (Process #6) wmiprvse.exe reads from lsass.exe. • (Process #6) wmiprvse.exe reads from svchost.exe. • (Process #6) wmiprvse.exe reads from dwm.exe. • (Process #6) wmiprvse.exe reads from (process #5) svchost.exe. • (Process #6) wmiprvse.exe reads from spoolsv.exe. • (Process #6) wmiprvse.exe reads from sihost.exe. • (Process #12) wmiprvse.exe reads from sihost.exe. • (Process #12) wmiprvse.exe reads from explorer.exe. • (Process #12) wmiprvse.exe reads from runtimebroker.exe. • (Process #12) wmiprvse.exe reads from shellexperiencehost.exe. • (Process #12) wmiprvse.exe reads from taskhostw.exe. • (Process #12) wmiprvse.exe reads from searchui.exe. • (Process #12) wmiprvse.exe reads from (process #8) windowsdatac.exe. • (Process #12) wmiprvse.exe reads from backgroundtaskhost.exe. • (Process #12) wmiprvse.exe reads from (process #9) runit.exe. • (Process #12) wmiprvse.exe reads from (process #10) wwst.exe.		
1/5	Input Capture	Monitors keyboard input	1	Keylogger
		• (Process #8) windowsdatac.exe frequently reads the state of a keyboard key by API.		
1/5	Hide Tracks	Creates process with hidden window	2	-
		• (Process #10) wwst.exe starts (process #13) cmd.exe with a hidden window. • (Process #10) wwst.exe starts (process #18) cmd.exe with a hidden window.		
1/5	Discovery	Reads system data	1	Spyware
		• (Process #10) wwst.exe reads Windows license key from registry.		
1/5	Network Connection	Performs DNS request	3	-
		• (Process #10) wwst.exe resolves host name "api.telegram.org" to IP "149.154.167.220". • (Process #10) wwst.exe resolves host name "icanhazip.com" to IP "104.18.114.97". • (Process #10) wwst.exe resolves host name "api.mylnikov.org" to IP "104.21.9.139".		
1/5	Network Connection	Connects to remote host	3	-

Score	Category	Operation	Count	Classification
		• (Process #10) wwst.exe opens an outgoing TCP connection to host "104.21.9.139:443". • (Process #10) wwst.exe opens an outgoing TCP connection to host "149.154.167.220:443". • (Process #10) wwst.exe opens an outgoing TCP connection to host "104.18.114.97:80".		
1/5	Discovery	Checks external IP address	1	-
		• (Process #10) wwst.exe checks external IP by asking IP info service at "http://icanhazip.com".		
1/5	Obfuscation	Resolves API functions dynamically	3	-
		• (Process #3) wwst.exe resolves 48 API functions by name. • (Process #10) wwst.exe resolves 58 API functions by name. • (Process #12) wmiprvse.exe resolves 83 API functions by name.		
1/5	Execution	Drops PE file	3	-
		• (Process #1) 82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\wwst.exe". • (Process #2) windowsdatac.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\RunIt.exe". • (Process #4) runit.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\Rnts.exe".		
1/5	Execution	Executes dropped PE file	2	-
		• Executes dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\wwst.exe". • Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\RunIt.exe".		
-	Trusted	Known clean file	10	-
		• Embedded file "Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\desktop.ini" is a known clean file. • Embedded file "C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini" is a known clean file. • Embedded file "C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\desktop.ini" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\msgid.dat" is a known clean file. • Embedded file "C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Downloads\desktop.ini" is a known clean file. • Embedded file "Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\EZSCq5D5osPMTO5bb2Q.jpg" is a known clean file. • Embedded file "Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Desktop\desktop.ini" is a known clean file. • Embedded file "Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\tH7ZiLMX-INDz2T4flA\5-DZJSZ32WSdJ.xls" is a known clean file. • Embedded file "Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\zuwnbRBCFb I.docx" is a known clean file. • Embedded file "C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini" is a known clean file.		

Malware Configuration: AsyncRAT

Metadata	Key	Extracted Value
Socket	Address Port Network Protocol C2 Listen	127.0.0.1 8808 tcp ✔ ✖
	Address Port Network Protocol C2 Listen	127.0.0.1 7707 tcp ✔ ✖
	Address Port Network Protocol C2 Listen	127.0.0.1 6606 tcp ✔ ✖
Mutex	Value	AsyncMutex_6SI8OkPnk
Other: Install	Value	✖
Other: Key	Tags Value	PBKDF2 Input Password VIfxfqryUTyZUBGDCBAvbYVYIsexIM7Z
Other: Salt	Value	v+seVvvNlzuyGQlkMKV4QwA9VkTSHmK51PGA5+bDOUE=
Other: Certificate	Value	MIIE9jCCAt6gAwIBAgIQAKQXqY8ZdB/modqi69mWGTANBgkqhkiG9w0BAQ0FADAcMRowGAYDVQQDDBFXb3JsZFdpbmQ…
Other: Serversignature	Value	J7XpD4w+JaFzTixc0nCmiRA4ZP4bPCIpEYYGofNxvC1+0OsFQr56oTWwQMosnOTB64TZRGSdXVHKzjVchQf7X5Uwu/KQ…
Other: Anti Analysis Enabled	Value	✖
Other: Telegram Chat ID	Value	806259874
Other: Telegram API Token	Value	5980420064:AAHGrlOU2WsgF90Pcyz-L7wrGgC_Cj54k4Q

Mitre ATT&CK Matrix

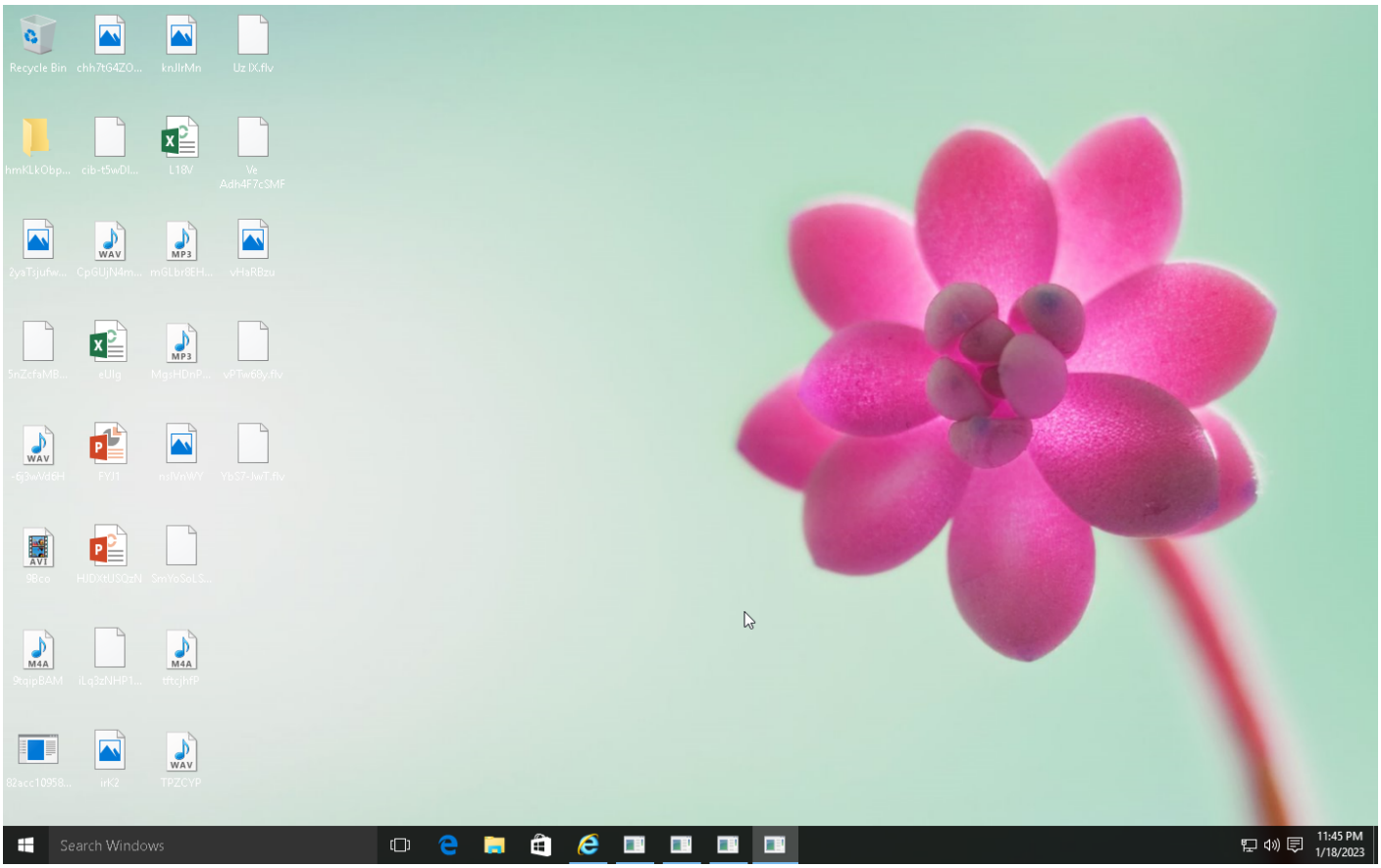
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1060 Registry Run Keys / Startup Folder		#T1112 Modify Registry	#T1056 Input Capture	#T1082 System Information Discovery		#T1056 Input Capture			
				#T1036 Masquerading		#T1083 File and Directory Discovery		#T1113 Screen Capture			
				#T1143 Hidden Window		#T1012 Query Registry		#T1119 Automated Collection			
				#T1045 Software Packing		#T1057 Process Discovery					
						#T1063 Security Software Discovery					
						#T1016 System Network Configuration Discovery					

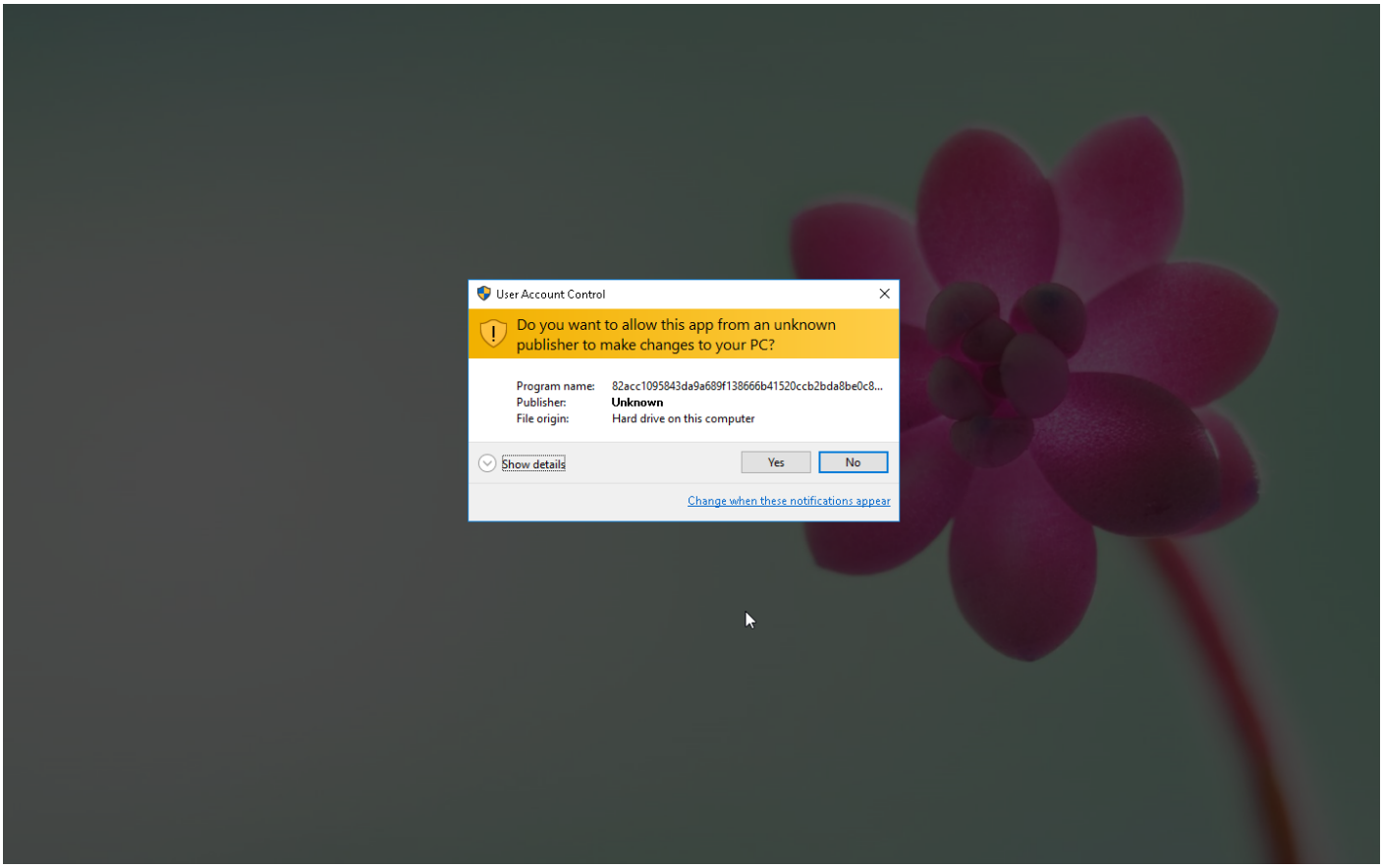
Sample Information

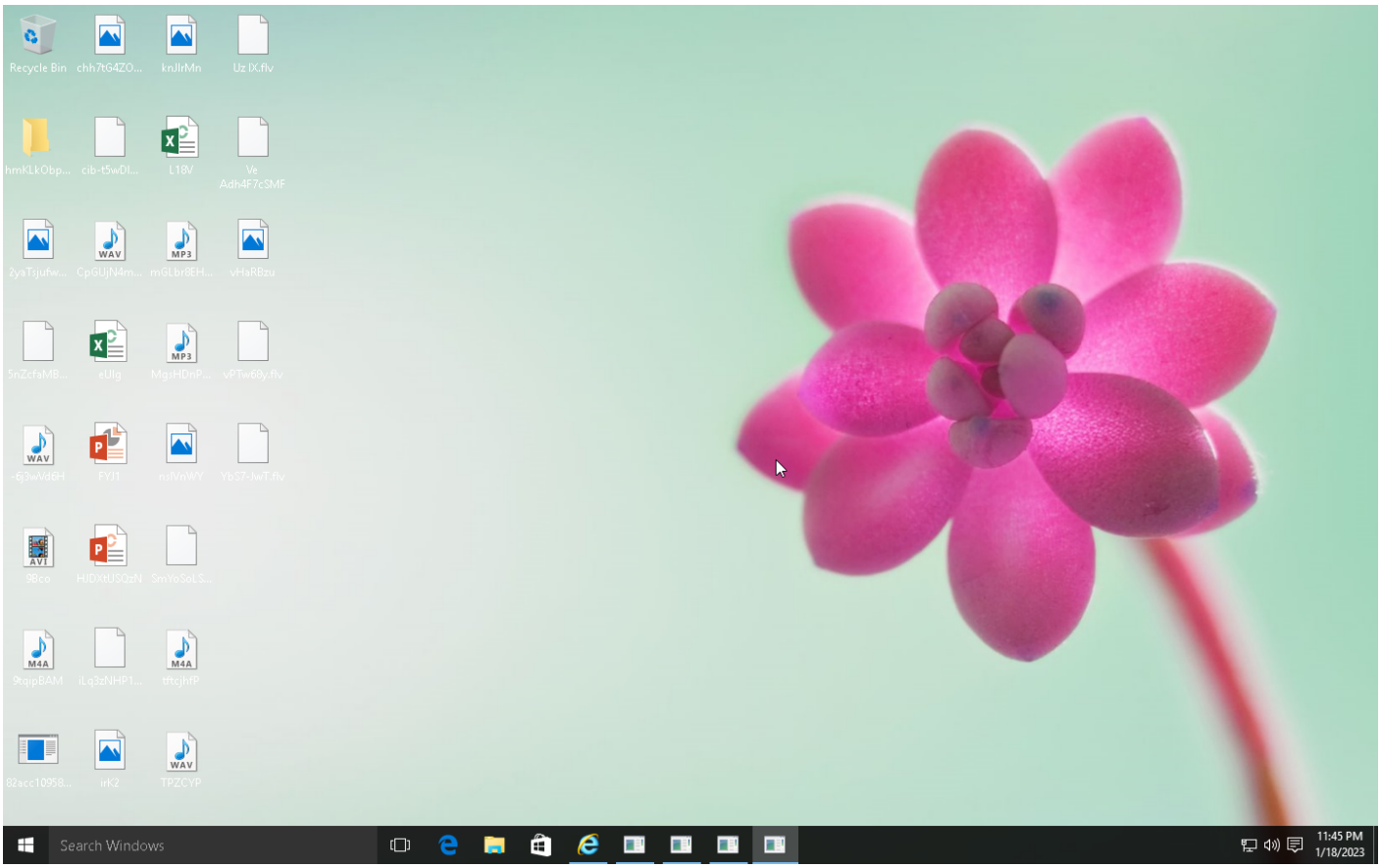
ID	#6646108
MD5	c7fbe52e88456eabb4d4a1a1a0670cf4
SHA1	3b479f15645c31c7067c31aede6e1802093ac78b
SHA256	82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746
SSDeep	6144:wcjrQ/rcaXeLfKqsmLjCkHhUcuS37N7E+rdR2cFoWIEh89dHHWtjunUU:wcjiuJsmXCkStSLNnRVFopEhAdH2tK
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe
File Size	335.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

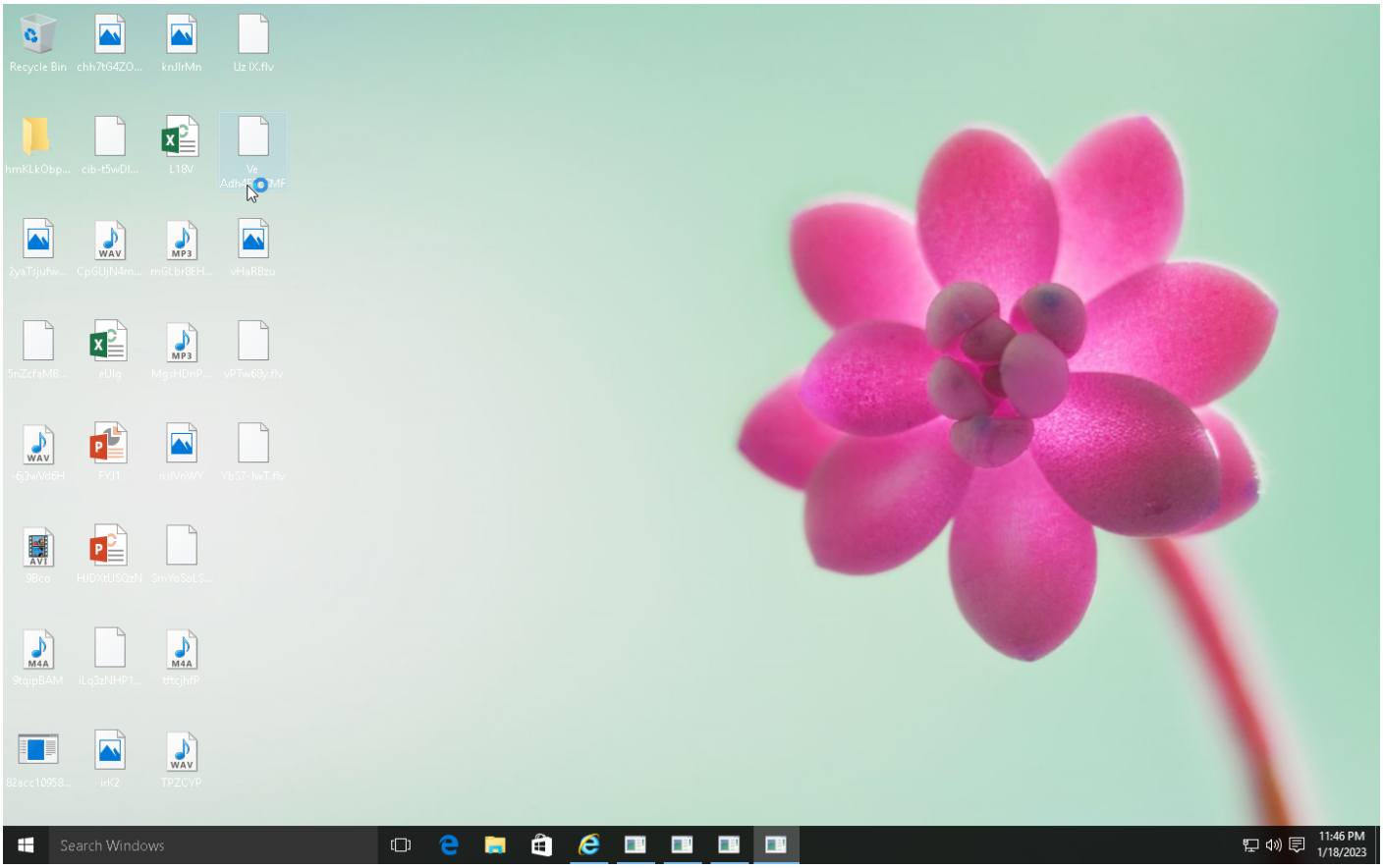
Analysis Information

Creation Time	2023-01-19 00:45 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	18
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	3


Search Windows
11:45 PM
1/18/2023


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 82acc1095843da9a689f138666b41520ccb2bda8be0c8...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

14.73 KB total sent

36.19 KB total received

4 ports 80, 443, 53, 445

4 contacted IP addresses

10 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

3 DNS requests for 3 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

5 sessions, 235 bytes sent, 690 bytes received

HTTP Requests

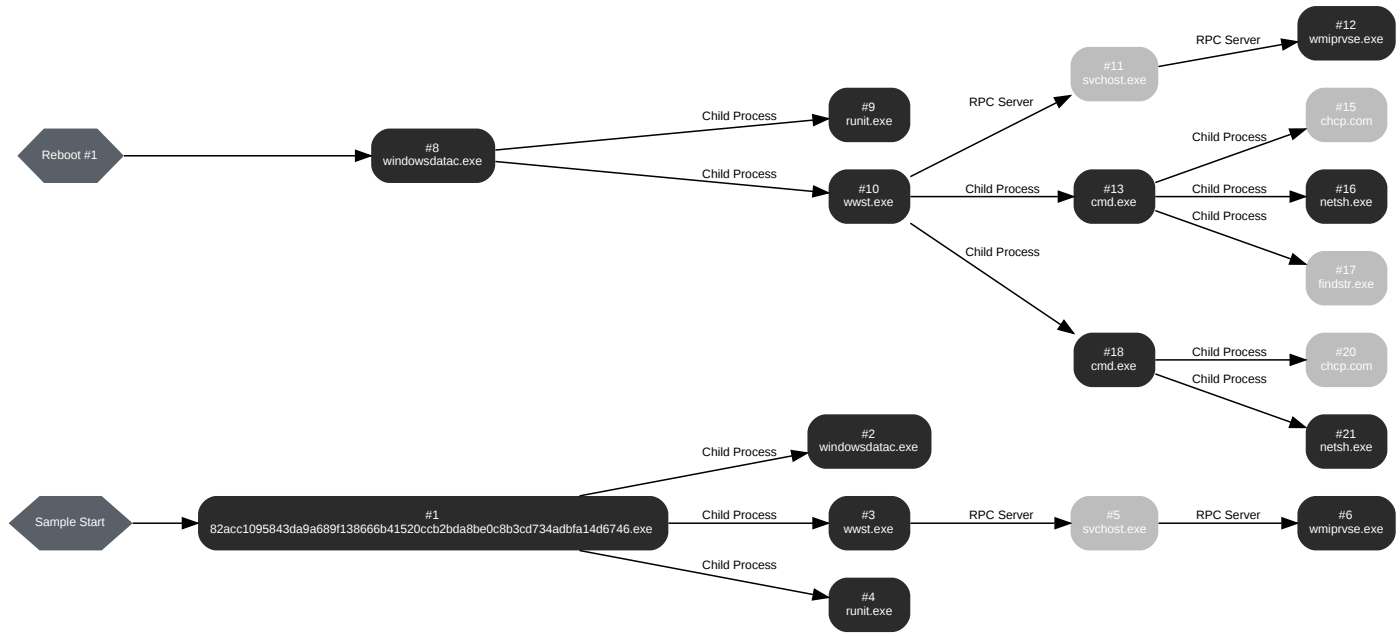
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://icanhazip.com	-	-		0 bytes	NA
GET	https://api.mylnikov.org/geolocation/wifi	-	-		0 bytes	NA
GET	https://api.telegram.org/bot5980420064:AAHGrIOU2WsgF90Pcyz-L7wrGgC_Cj54k4Q/sendMessage	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	api.telegram.org	NO_ERROR	149.154.167.220		NA
A	icanhazip.com	NO_ERROR	104.18.114.97, 104.18.115.97		NA
A	api.mylnikov.org	NO_ERROR	104.21.9.139, 172.67.160.130		NA

BEHAVIOR

Process Graph



Process #1: 82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 48417, Reason: Analysis Target
Unmonitor End Time	End Time: 288774, Reason: Terminated by timeout
Monitor duration	240.36s
Return Code	Unknown
PID	5060
Parent PID	1648
Bitness	64 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe	335.50 KB	82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\RunIt.exe	143.50 KB	9770561d2a27dbc16c230fe88af51f718d7d6274fcd63a3f109c381be848b4a9	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\wwst.exe	175.00 KB	82e62dbfd6aa5df5162e2a6a9cd5a0dfb97f94fb5f5bf531ca9f974ec0464ae2	✔

Host Behavior

Type	Count
Module	744
Window	24
Registry	7
System	15
File	18
Process	3
Environment	2
Keyboard	33

Process #2: windowsdatac.exe

ID	2
File Name	c:\programdata\windowsdatac.exe
Command Line	"C:\ProgramData\WindowsDataC.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 58768, Reason: Child Process
Unmonitor End Time	End Time: 288774, Reason: Terminated by timeout
Monitor duration	230.01s
Return Code	Unknown
PID	1852
Parent PID	5060
Bitness	64 Bit

Host Behavior

Type	Count
Module	744
Window	24
Registry	4
System	15
File	6
Environment	1
Keyboard	85

Process #3: wwst.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\wwst.exe
Command Line	"C:\Users\RDHJ0C~1\AppData\Local\Temp\wwst.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 58843, Reason: Child Process
Unmonitor End Time	End Time: 288774, Reason: Terminated by timeout
Monitor duration	229.93s
Return Code	Unknown
PID	3504
Parent PID	5060
Bitness	32 Bit

Dropped Files (18)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\desktop.ini	504 bytes	88856962cef670c087eda4e07d8f78465beeabb6143b96bd90f884a80af925b4	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	190 bytes	231a08caba1f9ba9f14bd3e46834288f3c351079fcedda15e391b724ac0c7ea8	✖
-	717 bytes	3299ac92e669eac1336e20080ea0e8eafe628be7bf70d1052f76535b102f6c7e	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\desktop.ini	402 bytes	cafec240d998e4b6e92ad1329cd417e8e9cbd73157488889fd93a542de4a4844	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\EZSCq5D5osPMTO5bb2Q.jpg	4.78 KB	f7fa19b5f4433cf9357d39a44f13d1f0d18ad75712d310ff62dd65febfad9e41	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Documents.txt	1.17 KB	e7cbfee9242347d0c5cb9f802e1dbd1ddc99843bb1d0cd1ca9d0a1d2d4752f92	✖
-	24 bytes	889ed51f9c16a4b989bda57957d3e132b1a9c117ee84e208207f2fa208a59483	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Desktop\desktop.ini	282 bytes	4b9d687ac625690fd026ed4b236dad1cac90ef69e7ad256cc42766a065b50026	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\System\Process.txt	187 bytes	f57da3677db49f6a086d463fe32959b6e98d438898dba0b5f11cbde4283d7c3d	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini	190 bytes	d01a7ef6233ef4ab3ea7210c0f2837931d334a20ae4d2a05ed03291e59e576c9	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\zuwnbRBCFb l.docx	4.74 KB	7bf7ac0b56dc7aa55cc3ef286f127a896986bac3f4119758ce06b33799222eb1	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\tH7ZiLMX-INDz2T4flA\5-DZJSZ32WSdJ.xls	2.68 KB	5ee93b4cee960c7a2d1e3eb2f5fc93ac3db2f75e87bf9c8a63cda5e391a47957	✖
-	1.10 KB	08140e2015405e6ec0d013013282ad6361c740c6f77cd7ba92c0d6282de2d43a	✖

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Desktop.txt	867 bytes	2bca829e78dedeb98e2989740f3cff605b6fd77720459ed3e92e5f386aa2531e	✖
-	25 bytes	8ddfc481b1b6ae30815ecce8a73755862f24b3bb7fdebdbf099e037d53eb082e	✖
-	766 bytes	d8d051624ec303be0ebeb95ec0e2df3680d832781afd243dac76b280f400925c	✖
-	26 bytes	582a0a96d76d3688fff52d48079910cba2b4fb53af678aa3bbfd872dd6c7466b	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Downloads\desktop.ini	282 bytes	b029393ea7b7cf644fb1c9f984f57c1980077562ee2e15d0ffd049c4c48098d3	✖

Host Behavior

Type	Count
Registry	29
File	397
-	3
User	3
Module	57
-	13
System	5
COM	19
-	5
Environment	3
Process	3

Process #4: runit.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\runit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\RunIt.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 59672, Reason: Child Process
Unmonitor End Time	End Time: 288774, Reason: Terminated by timeout
Monitor duration	229.10s
Return Code	Unknown
PID	3468
Parent PID	5060
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\Rnts.exe	143.50 KB	9770561d2a27dbc16c230fe88af51f718d7d6274fcd63a3f109c381be848b4a9	✖

Host Behavior

Type	Count
Module	413
Window	101
Registry	7
File	20
System	18
Environment	3
Keyboard	15

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: 83717, Reason: RPC Server
Unmonitor End Time	End Time: 288774, Reason: Terminated by timeout
Monitor duration	205.06s
Return Code	Unknown
PID	860
Parent PID	3504
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: 83717, Reason: RPC Server
Unmonitor End Time	End Time: 288774, Reason: Terminated by timeout
Monitor duration	205.06s
Return Code	Unknown
PID	4308
Parent PID	860
Bitness	64 Bit

Host Behavior

Type	Count
System	34
Registry	4
User	1
Process	62
-	98

Process #8: windowsdatac.exe

ID	8
File Name	c:\programdata\windowsdatac.exe
Command Line	"C:\ProgramData\WindowsDataC.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 148656, Reason: Autostart
Unmonitor End Time	End Time: 288774, Reason: Terminated by timeout
Monitor duration	140.12s
Return Code	Unknown
PID	2200
Parent PID	1612
Bitness	64 Bit

Host Behavior

Type	Count
Module	555
Window	24
Registry	5
System	13
File	18
Environment	2
Process	2
Keyboard	557

Process #9: runit.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\runit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\RunIt.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 155885, Reason: Child Process
Unmonitor End Time	End Time: 288774, Reason: Terminated by timeout
Monitor duration	132.89s
Return Code	Unknown
PID	2472
Parent PID	2200
Bitness	32 Bit

Host Behavior

Type	Count
Module	413
Window	101
Registry	8
File	21
System	15
Environment	3
Keyboard	2

Process #10: wwst.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\wwst.exe
Command Line	"C:\Users\RDHJ0C~1\AppData\Local\Temp\wwst.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 156216, Reason: Child Process
Unmonitor End Time	End Time: 288774, Reason: Terminated by timeout
Monitor duration	132.56s
Return Code	Unknown
PID	1040
Parent PID	2200
Bitness	32 Bit

Dropped Files (24)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\desktop.ini	504 bytes	88856962cef670c087eda4e07d8f78465beeabb6143b96bd90f884a80af925b4	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	190 bytes	231a08caba1f9ba9f14bd3e46834288f3c351079fcedda15e391b724ac0c7ea8	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Pictures.txt	717 bytes	3299ac92e669eac1336e20080ea0e8eafe628be7bf70d1052f76535b102f6c7e	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\desktop.ini	402 bytes	cafec240d998e4b6e92ad1329cd417e8e9cbd73157488889fd93a542de4a4844	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Documents.txt	1.17 KB	e7cbfee9242347d0c5cb9f802e1dbd1ddc99843bb1d0cd1ca9d0a1d2d4752f92	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Startup.txt	24 bytes	889ed51f9c16a4b989bda57957d3e132b1a9c117ee84e208207f2fa208a59483	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Desktop\desktop.ini	282 bytes	4b9d687ac625690fd026ed4b236dad1cac90ef69e7ad256cc42766a065b50026	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\WorldWind.jpg	54.68 KB	0ad037bc5d11bc2636bf22c28340d6506ceb30578c280a42ea38486451746c3b	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US.zip	44.30 KB	6b5607be36b30f57c0804238cb367029b1dde2bae631e222cff73e78d1af8d1c	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\tH7ZiLMX-INDz2T4flA\5-DZJSZ32WSdJ.xls	2.68 KB	5e52942d5055f54eb92e6ac6368d20d43e6e49bde17b76e59c4a3ee12072bc3c	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\ProductKey.txt	29 bytes	fe7d55816d270b2ad36fc2eca25fa1241092361d2f15397aeb5b6d1c95afd57c	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini	190 bytes	d01a7ef6233ef4ab3ea7210c0f2837931d334a20ae4d2a05ed03291e59e576c9	✖

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\Windows.txt	162 bytes	05cf654c11b6a75ebb02b17e930adb8bf3f4fbcf260f306faaaf4bd616e51b85	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\ScanningNetworks.txt	84 bytes	59b3120c5ce1a7d1819510272a927e1c8f1c95385213fccbcdd429ff3492040d	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Temp.txt	1.10 KB	08140e2015405e6ec0d013013282ad6361c740c6f77cd7ba92c0d6282de2d43a	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Desktop.txt	867 bytes	2bca829e78dedeb98e2989740f3cff605b6fd77720459ed3e92e5f386aa2531e	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\OneDrive.txt	25 bytes	8ddfc481b1b6ae30815ecce8a73755862f24b3bb7fdebdbf099e037d53eb082e	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Videos.txt	766 bytes	d8d051624ec303be0ebeb95ec0e2df3680d832781afd243dac76b280f400925c	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\msgid.dat	1 bytes	5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\Process.txt	1.49 KB	c09f26ae13fe965d31c3393fcaf7f3d0675b8fb831d52ffb9bf9e2413c1e830b	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Downloads.txt	26 bytes	582a0a96d76d3688fff52d48079910cba2b4fb53af678aa3bbfd872dd6c7466b	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\EZSCq5D5osPMTO5bb2Q.jpg	4.78 KB	c7e363455f4f22e2d4302f77d770edca28f99ecd8a94f31d4b7ec29eb6314dcf	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\zuwnbRBCFb l.docx	4.74 KB	b7d62c74925d6c6665dcf5c1dade5c2156c4edbc392b59d834a5ebc2f9f67b56	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Downloads\desktop.ini	282 bytes	b029393ea7b7cf644fb1c9f984f57c1980077562ee2e15d0ffd049c4c48098d3	✖

Host Behavior

Type	Count
Registry	43
File	845
-	11
User	3
Module	71
-	13
System	28
COM	128
-	49
Environment	13
Process	54
-	11
-	5

Network Behavior

Type	Count
HTTP	1
HTTPS	4
DNS	3
TCP	10

Process #11: svchost.exe

ID	11
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: 173647, Reason: RPC Server
Unmonitor End Time	End Time: 288774, Reason: Terminated by timeout
Monitor duration	115.13s
Return Code	Unknown
PID	864
Parent PID	1040
Bitness	64 Bit

Process #12: wmiprvse.exe

ID	12
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: 174297, Reason: RPC Server
Unmonitor End Time	End Time: 288774, Reason: Terminated by timeout
Monitor duration	114.48s
Return Code	Unknown
PID	2164
Parent PID	864
Bitness	64 Bit

Host Behavior

Type	Count
System	2750
Mutex	1
Module	766
Registry	16
File	3
-	5
User	32
-	1
Process	1952
-	2240

Process #13: cmd.exe

ID	13
File Name	c:\windows\syswow64\cmd.exe
Command Line	"cmd.exe" /C chcp 65001 && netsh wlan show profile | findstr All
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 221344, Reason: Child Process
Unmonitor End Time	End Time: 225061, Reason: Terminated
Monitor duration	3.72s
Return Code	1
PID	388
Parent PID	1040
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	26
Environment	31
System	1
Process	3

Process #15: chcp.com

ID	15
File Name	c:\windows\syswow64\chcp.com
Command Line	chcp 65001
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 221818, Reason: Child Process
Unmonitor End Time	End Time: 222979, Reason: Terminated
Monitor duration	1.16s
Return Code	0
PID	560
Parent PID	388
Bitness	32 Bit

Process #16: netsh.exe

ID	16
File Name	c:\windows\syswow64\netsh.exe
Command Line	netsh wlan show profile
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 222007, Reason: Child Process
Unmonitor End Time	End Time: 224681, Reason: Terminated
Monitor duration	2.67s
Return Code	1
PID	876
Parent PID	388
Bitness	32 Bit

Host Behavior

Type	Count
Module	41
Registry	19
System	9
File	4

Process #17: findstr.exe

ID	17
File Name	c:\windows\syswow64\findstr.exe
Command Line	findstr All
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 222105, Reason: Child Process
Unmonitor End Time	End Time: 224956, Reason: Terminated
Monitor duration	2.85s
Return Code	1
PID	932
Parent PID	388
Bitness	32 Bit

Process #18: cmd.exe

ID	18
File Name	c:\windows\syswow64\cmd.exe
Command Line	"cmd.exe" /C chcp 65001 && netsh wlan show networks mode=bssid
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 224614, Reason: Child Process
Unmonitor End Time	End Time: 227151, Reason: Terminated
Monitor duration	2.54s
Return Code	1
PID	1156
Parent PID	1040
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	27
System	1
Process	2

Process #20: chcp.com

ID	20
File Name	c:\windows\syswow64\chcp.com
Command Line	chcp 65001
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 224956, Reason: Child Process
Unmonitor End Time	End Time: 226750, Reason: Terminated
Monitor duration	1.79s
Return Code	0
PID	1192
Parent PID	1156
Bitness	32 Bit

Process #21: netsh.exe

ID	21
File Name	c:\windows\syswow64\netsh.exe
Command Line	netsh wlan show networks mode=bssid
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 225064, Reason: Child Process
Unmonitor End Time	End Time: 226922, Reason: Terminated
Monitor duration	1.86s
Return Code	1
PID	1416
Parent PID	1156
Bitness	32 Bit

Host Behavior

Type	Count
Module	41
Registry	19
System	9
File	4

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746	C:\Users\RDhJ0CNFevzX\Desktop\82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe, C:\ProgramData\WindowsDataC.exe	Sample File	335.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
9770561d2a27dbc16c230fe88af51f718d7d6274fcd63a3f109c381be848b4a9	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\RunIt.exe, C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\Rnts.exe	Dropped File	143.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
82e62dbfd6aa5df5162e2a6a9cd5a0dfb97f94fb5f5bf531ca9f974ec0464ae2	C:\Users\RDHJ0C~1\AppData\Local\Temp\wwst.exe, C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\wwst.exe	Dropped File	175.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
88856962cef670c087eda4e07d8f78465beeabb6143b96bd90f884a80af925b4	Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\desktop.ini, C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ... ...X\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\desktop.ini	Dropped File	504 bytes	text/plain	Access, Create, Read, Write	CLEAN
231a08caba1f9ba9f14bd3e46834288f3c351079fcedda15e391b724ac0c7ea8	C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\... ...r\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini, Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	Dropped File	190 bytes	text/plain	Access, Create, Read, Write	CLEAN
3299ac92e669eac1336e20080ea0e8eafe628be7bf70d1052f76535b102f6c7e	Directories\Pictures.txt, C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directori... ...tures.txt, c:\users\rdhj0cnfevzx\appdata\local\77d6f3ea3b56fc0f6b6f10284ad90596\rdhj0cnfevzx@xc64zb_en-us\directories\pictures.txt	Dropped File	717 bytes	text/plain	Access, Read	CLEAN
cafec240d998e4b6e92ad1329cd417e8e9cbd73157488889fd93a542de4a4844	C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\... ...zX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\desktop.ini, Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\desktop.ini	Dropped File	402 bytes	text/plain	Access, Create, Read, Write	CLEAN
f7fa19b5f4433cf9357d39a44f13d1f0d18ad75712d310ff62dd65febfad9e41	C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\EZSCq5D5osPMTO5bb2Q.jpg	Dropped File	4.78 KB	image/jpeg	Access, Create, Write	CLEAN
e7cbfee9242347d0c5cb9f802e1dbd1ddc99843bb1d0cd1ca9d0a1d2d4752f92	C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Documents.txt, C:\Users... ...evzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Documents.txt, Directories\Documents.txt	Dropped File	1.17 KB	text/plain	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
889ed51f9c16a4b989bda57957d3e132b1a9c117ee84e208207f2fa208a59483	C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Startup.txt, Directorie... ...tartup.txt, c:\users\rdhj0cnfevzx\appdata\local\77d6f3ea3b56fc0f6b6f10284ad90596\rdhj0cnfevzx@xc64zb_en-us\directories\startup.txt	Dropped File	24 bytes	text/plain	Access, Read	CLEAN
4b9d687ac625690fd026ed4b236dad1cac90ef69e7ad256cc42766a065b50026	Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Desktop\desktop.ini, C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0... ...zX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Desktop\desktop.ini	Dropped File	282 bytes	text/plain	Access, Create, Read, Write	CLEAN
f57da3677db49f6a086d463fe32959b6e98d438898dba0b5f11cbde4283d7c3d	C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\System\Process.txt	Dropped File	187 bytes	text/plain	Access, Create, Write	CLEAN
0ad037bc5d11bc2636bf22c28340d6506ceb30578c280a42ea38486451746c3b	System\WorldWind.jpg, C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\WorldWind.jpg	Dropped File	54.68 KB	image/jpeg	Access, Read	CLEAN
6b5607be36b30f57c0804238cb367029b1dde2bae631e222cff73e78d1af8d1c	C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US.zip	Dropped File	44.30 KB	application/zip	Access, Create, Read, Write	CLEAN
5e52942d5055f54eb92e6ac6368d20d43e6e49bde17b76e59c4a3ee12072bc3c	Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\tH7ZiLMX-lNDz2T4flA\5-DZJSZ32WSdJ.xls, C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e1... ...3ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\tH7ZiLMX-lNDz2T4flA\5-DZJSZ32WSdJ.xls	Dropped File	2.68 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
fe7d55816d270b2ad36fc2eca25fa1241092361d2f15397aeb5b6d1c95afd57c	C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\ProductKey.txt, System\ProductKey.txt	Dropped File	29 bytes	text/plain	Access, Create, Read	CLEAN
d01a7ef6233ef4ab3ea7210c0f2837931d334a20ae4d2a05ed03291e59e576c9	C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\... ...E-C\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini, Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini	Dropped File	190 bytes	text/plain	Access, Create, Read, Write	CLEAN
05cf654c11b6a75ebb02b17e930adb8bf3f4fbcf260f306faaaf4bd616e51b85	System\Windows.txt, C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\Windows.txt	Dropped File	162 bytes	text/plain	Access, Create, Read, Write	CLEAN
7bf7ac0b56dc7aa55cc3ef286f127a896986bac3f4119758ce06b33799222eb1	C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\zuwnbRBCFb l.docx	Dropped File	4.74 KB	application/zip	Access, Create, Write	CLEAN
59b3120c5ce1a7d1819510272a927e1c8f1c95385213fccbcdd429ff3492040d	System\ScanningNetworks.txt, C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\ScanningNetworks.txt	Dropped File	84 bytes	text/plain	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
5ee93b4cee960c7a2d1e3eb2f5fc93ac3db2f75e87bf9c8a63cda5e391a47957	C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\tH7ZiLMX-INDz2T4flA\5-DZJSZ32WSdJ.xls	Dropped File	2.68 KB	application/CDFV2	Access, Create, Write	CLEAN
08140e2015405e6ec0d013013282ad6361c740c6f77cd7ba92c0d6282de2d43a	Directories\Temp.txt, C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Temp.txt, c:\users\rdhj0cnfevzx\appdata\local\77d6f3ea3b56fc0f6b6f10284ad90596\rdhj0cnfevzx@xc64zb_en-us\directories\temp.txt	Dropped File	1.10 KB	text/plain	Access, Read	CLEAN
2bca829e78dedeb98e2989740f3cff605b6fd77720459ed3e92e5f386aa2531e	C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Desktop.txt, C:\Users\R... ...0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Desktop.txt, Directories\Desktop.txt	Dropped File	867 bytes	text/plain	Access, Create, Read, Write	CLEAN
8ddfc481b1b6ae30815ecce8a73755862f24b3bb7fdebdbf099e037d53eb082e	Directories\OneDrive.txt, C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directori... ...Drive.txt, c:\users\rdhj0cnfevzx\appdata\local\77d6f3ea3b56fc0f6b6f10284ad90596\rdhj0cnfevzx@xc64zb_en-us\directories\onedrive.txt	Dropped File	25 bytes	text/plain	Access, Read	CLEAN
d8d051624ec303be0ebeb95ec0e2df3680d832781afd243dac76b280f400925c	Directories\Videos.txt, C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Videos.txt, c:\users\rdhj0cnfevzx\appdata\local\77d6f3ea3b56fc0f6b6f10284ad90596\rdhj0cnfevzx@xc64zb_en-us\directories\videos.txt	Dropped File	766 bytes	text/plain	Access, Read	CLEAN
5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9	C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\msgid.dat	Dropped File	1 bytes	application/octet-stream	Access, Create, Write	CLEAN
c09f26ae13fe965d31c3393fcaf7f3d0675b8fb831d52ffb9bf9e2413c1e830b	C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\Process.txt, System\Process.txt	Dropped File	1.49 KB	text/plain	Access, Create, Read, Write	CLEAN
582a0a96d76d3688fff52d48079910cba2b4fb53af678aa3bbfd872dd6c7466b	C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Downloads.txt, Director... ...oads.txt, c:\users\rdhj0cnfevzx\appdata\local\77d6f3ea3b56fc0f6b6f10284ad90596\rdhj0cnfevzx@xc64zb_en-us\directories\downloads.txt	Dropped File	26 bytes	text/plain	Access, Read	CLEAN
c7e363455f4f22e2d4302f77d770edca28f99ecd8a94f31d4b7ec29eb6314dcf	Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\EZSCq5D5osPMTO5bb2Q.jpg, C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\EZSCq5D5osPMTO5bb2Q.jpg	Dropped File	4.78 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b7d62c74925d6c6665dcf5c1dade5c2156c4edbc392b59d834a5ebc2f9f67b56	Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\zuwnbRBCFb l.docx, C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\zuwnbRBCFb l.docx	Dropped File	4.74 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c54143f949176485168a3bbadbc868c8017762f0c5ece1cb158db5bf5ba07703	-	Downloaded File	16 bytes	text/plain	-	CLEAN
b029393ea7b7cf644fb1c9f984f57c1980077562ee2e15d0ffd049c4c48098d3	C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\...zX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Downloads\desktop.ini, Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Downloads\desktop.ini	Dropped File	282 bytes	text/plain	Access, Create, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe	Accessed File, Sample File	Access	MALICIOUS
C:\ProgramData\WindowsDataC.exe	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX	Accessed File	Access, Create	CLEAN
\\.\C:	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Desktop\desktop.ini	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a	Accessed File	Access, Create	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\ScanningNetworks.txt	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Browsers	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\Profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Downloads	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\history.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\tH7ZiLMX-INDz2T4flA	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber	Accessed File	Access, Create	CLEAN
C:\Windows\system32\WBEM\Logs\	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\K-Melon\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Wallets	Accessed File	Access, Create, Delete	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\77d6f3ea3b56fc0f6b6f10284ad90596\rdhj0cnfevzx@xc64zb_en-us\directories\downloads.txt	Dropped File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Pictures.txt	Accessed File, Dropped File	Access, Read	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\77d6f3ea3b56fc0f6b6f10284ad90596\rdhj0cnfevzx@xc64zb_en-us\directories\videos.txt	Dropped File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Wallets	Accessed File	Access, Create, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromodo\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp	Accessed File	Access	CLEAN
Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\desktop.ini	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Browser\Browser\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Waterfox\Profiles	Accessed File	Access	CLEAN
Directories\Startup.txt	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C	Accessed File	Access, Create	CLEAN
Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\System\Process.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Startup.txt	Accessed File, Dropped File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\tH7ZiLMX-INDz2T4flA\5-DZJSZ32WSdJ.xls	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\SYSTEM32\MFC42u.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\zuwnbRBCFb l.docx	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Directories	Accessed File	Access, Create	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures	Accessed File	Access, Create	CLEAN
Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\zuwnbRBCFbl.docx	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\OpenVPN Connect\profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Downloads	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Ethereum\keystore	Accessed File	Access	CLEAN
Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Desktop\desktop.ini	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Outlook Files	Accessed File	Access	CLEAN
Directories\Videos.txt	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Downloads\desktop.ini	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Discord\Local Storage\leveldb	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Temp.txt	Accessed File, Dropped File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\msgid.dat	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Telegram Desktop\tdata	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Documents.txt	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\desktop.ini	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\tH7ZiLMX-INDz2T4flA\5-DZJSZ32WSdJ.xls	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\Profiles	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDHJ0C~1\AppData\Local\Temp\wwst.exe	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures	Accessed File	Access	CLEAN
System\ProductKey.txt	Miscellaneous File	-	CLEAN
Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Exodus\exodus.wallet	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\Rnts.exe	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\WorldWind.jpg	Accessed File, Dropped File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Electrum\wallets	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\sitemanager.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\wwst.exe.config	Accessed File	Access	CLEAN
Directories\Documents.txt	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Desktop.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\ProgramData\WindowsDataC.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Documents.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\tH7ZiLMX-INDz2T4flA	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Mail.Ru\Atom\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\com.liberty.jaxx\IndexedDB\file__0.indexeddb.leveldb	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\DropBox	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
System\WorldWind.jpg	Miscellaneous File	-	CLEAN
Directories\Temp.txt	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\My Videos	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Maxthon3\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHaw\Profiles	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\EZSCq5D5osPMTO5bb2Q.jpg	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\desktop.ini	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google(x86)\Chrome\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\Profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596	Accessed File	Access, Create	CLEAN
System\Process.txt	Miscellaneous File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\77d6f3ea3b56fc0f6b6f10284ad90596\rdhj0cnfevzx@xc64zb_en-us\directories\pictures.txt	Dropped File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US.zip	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\desktop.ini	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Desktop.txt	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\User Data\	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\77d6f3ea3b56fc0f6b6f10284ad90596\rdhj0cnfevzx@xc64zb_en-us\directories\startup.txt	Dropped File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\EZSCq5D5osPMTO5bb2Q.jpg	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\RunIt.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Directories\Downloads.txt	Accessed File, Dropped File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Saved Pictures	Accessed File	Access, Create	CLEAN
System\ScanningNetworks.txt	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Nichrome\User Data\	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures	Accessed File	Access	CLEAN
Directories\Desktop.txt	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Desktop\desktop.ini	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\Process.txt	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Comodo\IceDragon\Profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Ubisoft Game Launcher	Accessed File	Access	CLEAN
Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Documents\tH7ZiLMX-INDz2T4flA\5-DZJSZ32WSdJ.xls	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrcompression.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\My Pictures	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Discord Canary\leveldb	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents	Accessed File	Access	CLEAN
System\Windows.txt	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\System\ProductKey.txt	Accessed File, Dropped File	Access, Create, Read	CLEAN
C:\Program Files\Windows Portable Devices\year-culture-then.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Uran\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US\Grabber\DRIVE-C\Users\RDhJ0CNFevzX\Downloads	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\77d6f3ea3b56fc0f6b6f10284ad90596\RDhJ0CNFevzX@XC64ZB_en-US	Accessed File	Access, Create	CLEAN
Directories\OneDrive.txt	Miscellaneous File	-	CLEAN
C:\Windows\SYSTEM32\RichEd20.DLL	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bytecoin	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\a064c843e183ccea646badeb280e154a\RDhJ0CNFevzX@XC64ZB_en-US\Browsers	Accessed File	Access, Create	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://api.telegram.org/bot5980420064:AAHGrlOU2WsgF90Pcyz-L7wrGgC_Cj54k4Q/getFile	-	149.154.167.220	-	-	MALICIOUS
http://127.0.0.1:7707	-	127.0.0.1	-	-	MALICIOUS
https://api.telegram.org/bot5980420064:AAHGrlOU2WsgF90Pcyz-L7wrGgC_Cj54k4Q/send	-	149.154.167.220	-	-	MALICIOUS
https://api.telegram.org/bot5980420064:AAHGrlOU2WsgF90Pcyz-L7wrGgC_Cj54k4Q/getUpdates	-	149.154.167.220	-	-	MALICIOUS
https://api.telegram.org/bot5980420064:AAHGrlOU2WsgF90Pcyz-L7wrGgC_Cj54k4Q/editMessageText	-	149.154.167.220	-	-	MALICIOUS
http://127.0.0.1:6606	-	127.0.0.1	-	-	MALICIOUS
https://api.telegram.org/bot5980420064:AAHGrlOU2WsgF90Pcyz-L7wrGgC_Cj54k4Q/sendMessage	-	149.154.167.220	-	-	MALICIOUS
http://127.0.0.1:8808	-	127.0.0.1	-	-	MALICIOUS
https://api.telegram.org/bot5980420064:AAHGrlOU2WsgF90Pcyz-L7wrGgC_Cj54k4Q/sendLocation	-	149.154.167.220	-	-	MALICIOUS
https://api.mylnikov.org/geolocation/wifi	-	104.21.9.139, 172.67.160.130	-	-	CLEAN
http://icanhazip.com	-	104.18.114.97, 104.18.115.97	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
icanhazip.com	104.18.114.97, 104.18.115.97	-	TCP, HTTP, DNS	CLEAN
api.telegram.org	149.154.167.220	-	TCP, HTTPS, DNS, TLS	CLEAN
api.mylnikov.org	104.21.9.139, 172.67.160.130	-	TCP, HTTPS, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
104.18.114.97	icanhazip.com	-	TCP, HTTP, DNS	CLEAN
172.67.160.130	api.mylnikov.org	United States	DNS	CLEAN
149.154.167.220	api.telegram.org	United Kingdom	TCP, HTTPS, DNS, TLS	CLEAN
104.18.115.97	icanhazip.com	-	DNS	CLEAN
127.0.0.1	-	-	-	CLEAN
104.21.9.139	api.mylnikov.org	-	TCP, HTTPS, DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
AsyncMutex_6SI8OkPnk	-	-	MALICIOUS
-	access	wmiprvse.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	wwst.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	wwst.exe, 82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe, windowsdatac.exe, runit.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\Description\System\CentralProcessor\0	access	wwst.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe, windowsdatac.exe, runit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe, windowsdatac.exe, runit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	wwst.exe	CLEAN
HKEY_CURRENT_USER\Software\Litecoin	access	wwst.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM	access, create	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	wwst.exe	CLEAN
HKEY_CURRENT_USER\Software	access	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	wwst.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\WindowsDataC.exe	write, access, read	82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe	CLEAN
HKEY_CURRENT_USER\Software\Dash	access	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetSh	access	netsh.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Santech Solutions\PerfWatso v. 32\1.0.0.0	access	runit.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	access, read	wwst.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\For users\mini_calculator\1.0.0.0	access	windowsdatac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Rnts.exe	write, access, read	runit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Valve\Steam	access	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\DigitalProductId	access, read	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\Description\System\CentralProcessor\0\Identifier	access, read	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Bitcoin	access	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	wwst.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access	82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe, runit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	access, read	wwst.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM\EnableObjectValidation	access, read	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe, windowsdatac.exe, runit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	wwst.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	wwst.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	wwst.exe	CLEAN

Process

Process Name	Commandline	Verdict
82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe	"C:\Users\RDhJ0CNFevzX\Desktop\82acc1095843da9a689f138666b41520ccb2bda8be0c8b3cd734adbfa14d6746.exe"	MALICIOUS
windowsdatac.exe	"C:\ProgramData\WindowsDataC.exe"	MALICIOUS
wwst.exe	"C:\Users\RDHJ0C~1\AppData\Local\Temp\wwst.exe"	MALICIOUS
runit.exe	"C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\RunIt.exe"	MALICIOUS
windowsdatac.exe	"C:\ProgramData\WindowsDataC.exe"	MALICIOUS
runit.exe	"C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\RunIt.exe"	MALICIOUS
wwst.exe	"C:\Users\RDHJ0C~1\AppData\Local\Temp\wwst.exe"	MALICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN
cmd.exe	"cmd.exe" /C chcp 65001 && netsh wlan show profile | findstr All	CLEAN
chcp.com	chcp 65001	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
findstr.exe	findstr All	CLEAN
cmd.exe	"cmd.exe" /C chcp 65001 && netsh wlan show networks mode=bssid	CLEAN
chcp.com	chcp 65001	CLEAN
netsh.exe	netsh wlan show networks mode=bssid	CLEAN
netsh.exe	netsh wlan show profile	CLEAN

YARA / AV

YARA (3)

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	Dropped File	C:\Users\RDHJ0C~1\AppData\Local\Temp\wwst.exe	Backdoor	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	4.7.1
Dynamic Engine Version	4.7.1 / 11/21/2022 04:40
Static Engine Version	4.7.1.0 / 2022-11-21 03:00:41
AV Exceptions Version	4.7.2.20 / 2022-12-15 11:43:19
Link Detonation Heuristics Version	4.7.2.20 / 2022-12-15 11:43:19
Smart Memory Dumping Rules Version	4.7.2.20 / 2022-12-15 11:43:19
Config Extractors Version	4.7.2.22 / 2023-01-05 11:05:11
Signature Trust Store Version	4.7.2.21 / 2023-01-03 15:44:56
VMRay Threat Identifiers Version	4.7.2.23 / 2023-01-07 18:36:42
YARA Built-in Ruleset Version	4.7.2.21

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	8.0.1710.11

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