MALICIOUS

Classifications: Spyware, Keylogger

Threat Names: SnakeKeylogger, Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe**
ID	#4189738
MD5	5ca02369b45067fe039314f38b286767
SHA1	b11ff0b977b16863c34dc35126f1d3d13ab5cc4f
SHA256	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154
File Size	470.00 KB
Report Created	2022-04-25 09:52 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (19 rules, 84 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	2	Keylogger, Spyware
	• Rule "SnakeKeylogger" from ruleset "Malware" has matched on the sample itself. • Rule "SnakeKeylogger" from ruleset "Malware" has matched on a memory dump for (process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: CentBrowser, Epic Privacy Browser, Chromium, 7Star, Maple Studio, Amigo, CocCoc, Pidgin, Orbitum,... ...putnik, Chrome Canary, FileZilla, Comodo Dragon, Microsoft Outlook, Chedot, Opera, Vivaldi, Google Chrome, Uran, Elements Browser.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
3/5	Input Capture	Monitors keyboard input	1	Keylogger
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe installs system wide "WH_KEYBOARD_LL" hook(s) to monitor keystrokes.			
2/5	Data Collection	Reads sensitive browser data	20	-
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Yandex Browser" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Amigo" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Kometa" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "CocCoc" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Orbitum" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Vivaldi" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Chromium" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "CentBrowser" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Chedot" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Comodo Dragon" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Torch" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Epic Privacy Browser" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Opera" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Uran" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "7Star" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Chrome Canary" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Maple Studio" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Sputnik" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of web browser "Elements Browser" by file.		
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of ftp application "FileZilla" by file.			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to read sensitive data of application "Pidgin" by file.			

Score	Category	Operation	Count	Classification
2/5	Anti Analysis	Delays execution	1	-
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe has a thread which sleeps more than 5 minutes.			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe is possibly trying to detect a VM via rdtsc.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe enables process privilege "SeDebugPrivilege".			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe creates mutex with name "Global\.net clr networking".			
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to gather information about application "FileZilla" by file. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to gather information about application "Pidgin" by file.			
1/5	Discovery	Reads system data	1	Spyware
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe reads Windows license key from registry.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe starts (process #2) netsh.exe with a hidden window.			
1/5	Discovery	Checks external IP address	1	-
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe checks external IP by asking IP info service at "http://checkip.dyndns.org/".			
1/5	Network Connection	Performs DNS request	2	-
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe resolves host name "checkip.dyndns.org" to IP "193.122.6.168". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe resolves host name "freegeoip.app" to IP "188.114.96.7".			
1/5	Network Connection	Connects to remote host	31	-

Score	Category	Operation	Count	Classification
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52257". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52300". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52309". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52316". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52325". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52339". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52345". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52360". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52377". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52399". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52405". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52413". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52422". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe accepts an incoming TCP connection from host "103.147.185.85:52429". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52257". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52300". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52309". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52316". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "132.226.247.73:80". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52325". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52339". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "188.114.96.7:443". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52345". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52360". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52377". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52399". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52405". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52413". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:21". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52422". • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe opens an outgoing TCP connection to host "103.147.185.85:52429".			
1/5	Network Connection	Tries to connect using an uncommon port	14	-
	• (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52257 at 103.147.185.85. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52300 at 103.147.185.85. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52309 at 103.147.185.85. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52316 at 103.147.185.85. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52325 at 103.147.185.85. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52339 at 103.147.185.85. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52345 at 103.147.185.85. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52360 at 103.147.185.85. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52377 at 103.147.185.85. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52399 at 103.147.185.85. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52405 at 103.147.185.85. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52413 at 103.147.185.85. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52422 at 103.147.185.85. • (Process #1) 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe tries to connect to TCP port 52429 at 103.147.185.85.			

Mitre ATT&CK Matrix

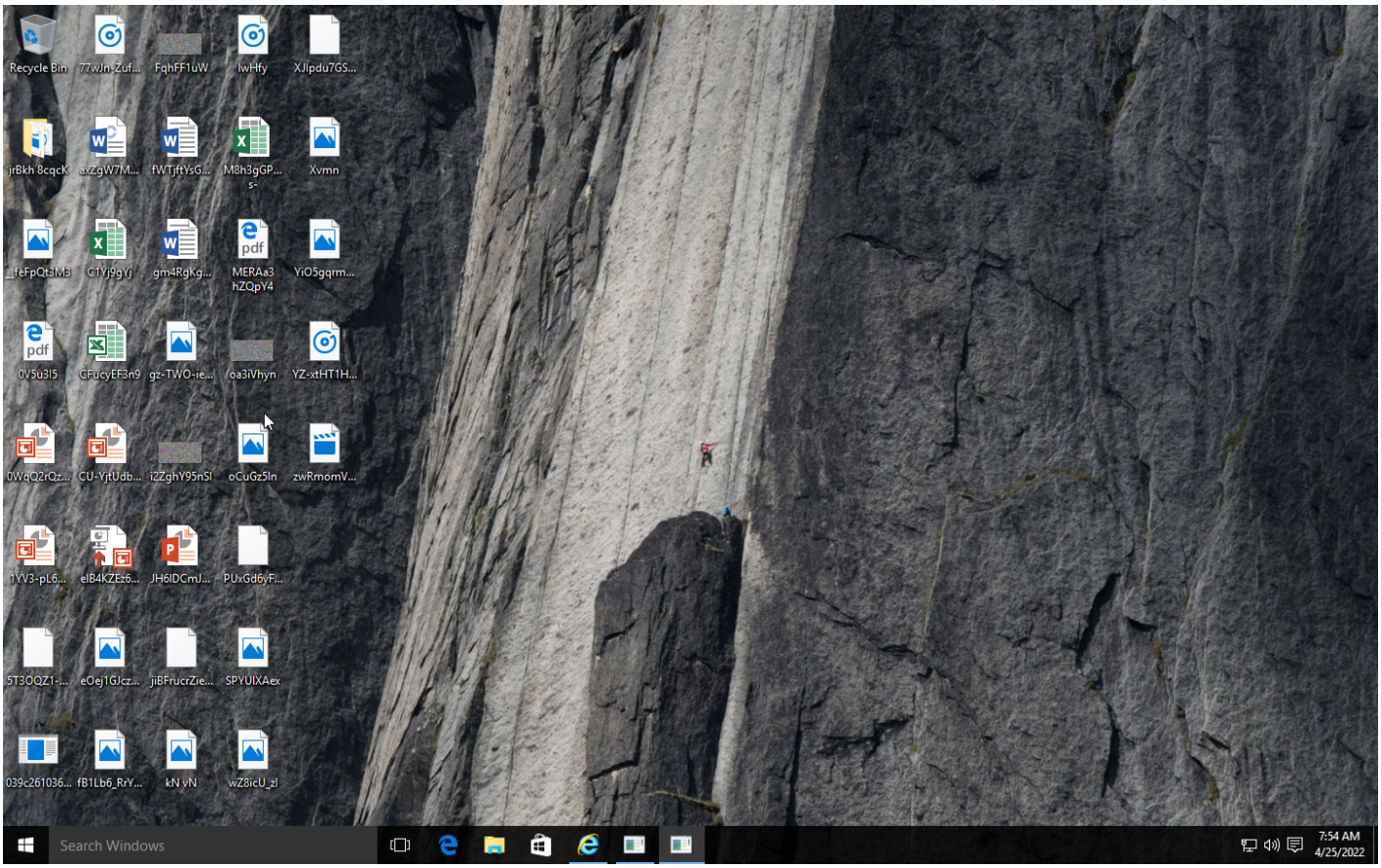
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1179 Hooking	#T1179 Hooking	#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection	#T1065 Uncommonly Used Port		
				#T1497 Virtualization/ Sandbox Evasion	#T1214 Credentials in Registry	#T1012 Query Registry		#T1005 Data from Local System			
					#T1056 Input Capture	#T1082 System Information Discovery		#T1056 Input Capture			
					#T1179 Hooking	#T1497 Virtualization/ Sandbox Evasion					
						#T1124 System Time Discovery					
						#T1016 System Network Configuration Discovery					

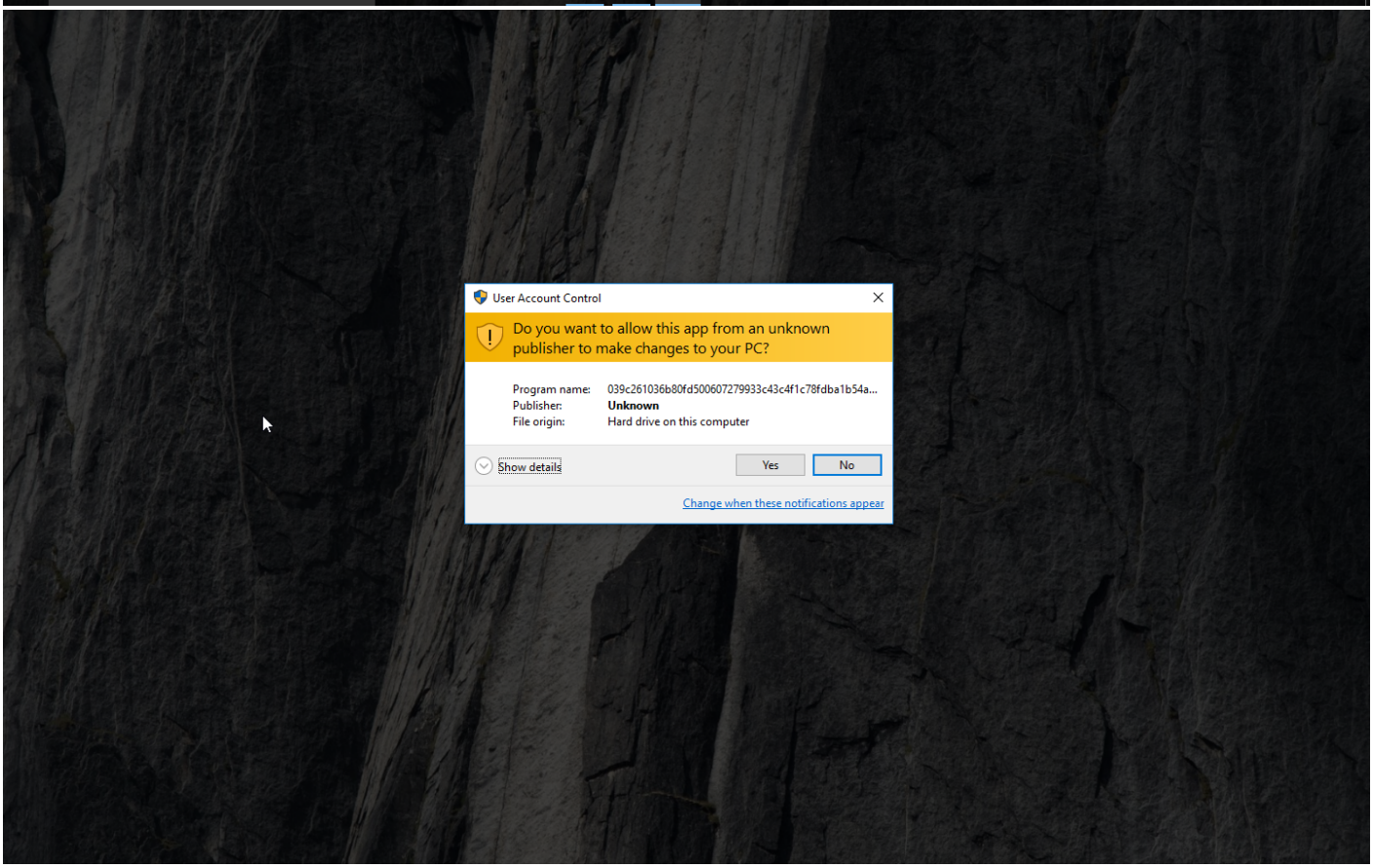
Sample Information

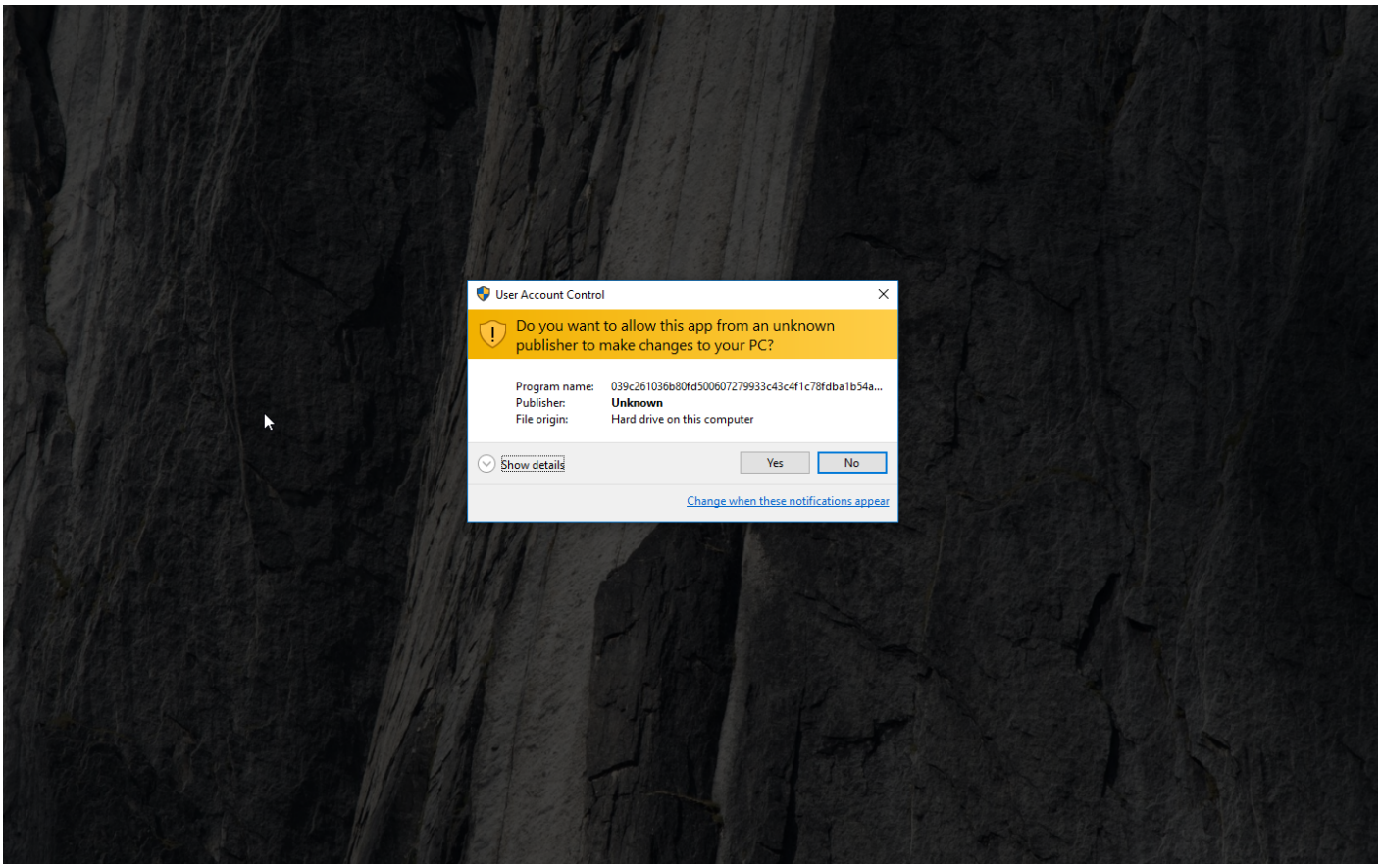
ID	#4189738
MD5	5ca02369b45067fe039314f38b286767
SHA1	b11ff0b977b16863c34dc35126f1d3d13ab5cc4f
SHA256	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154
SSDeep	12288:eR3E3HDei3oXA2jCXgXLz/HQOqzjW/NP:eRU3Hq6oXA2jBXHnqzjG
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe
File Size	470.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

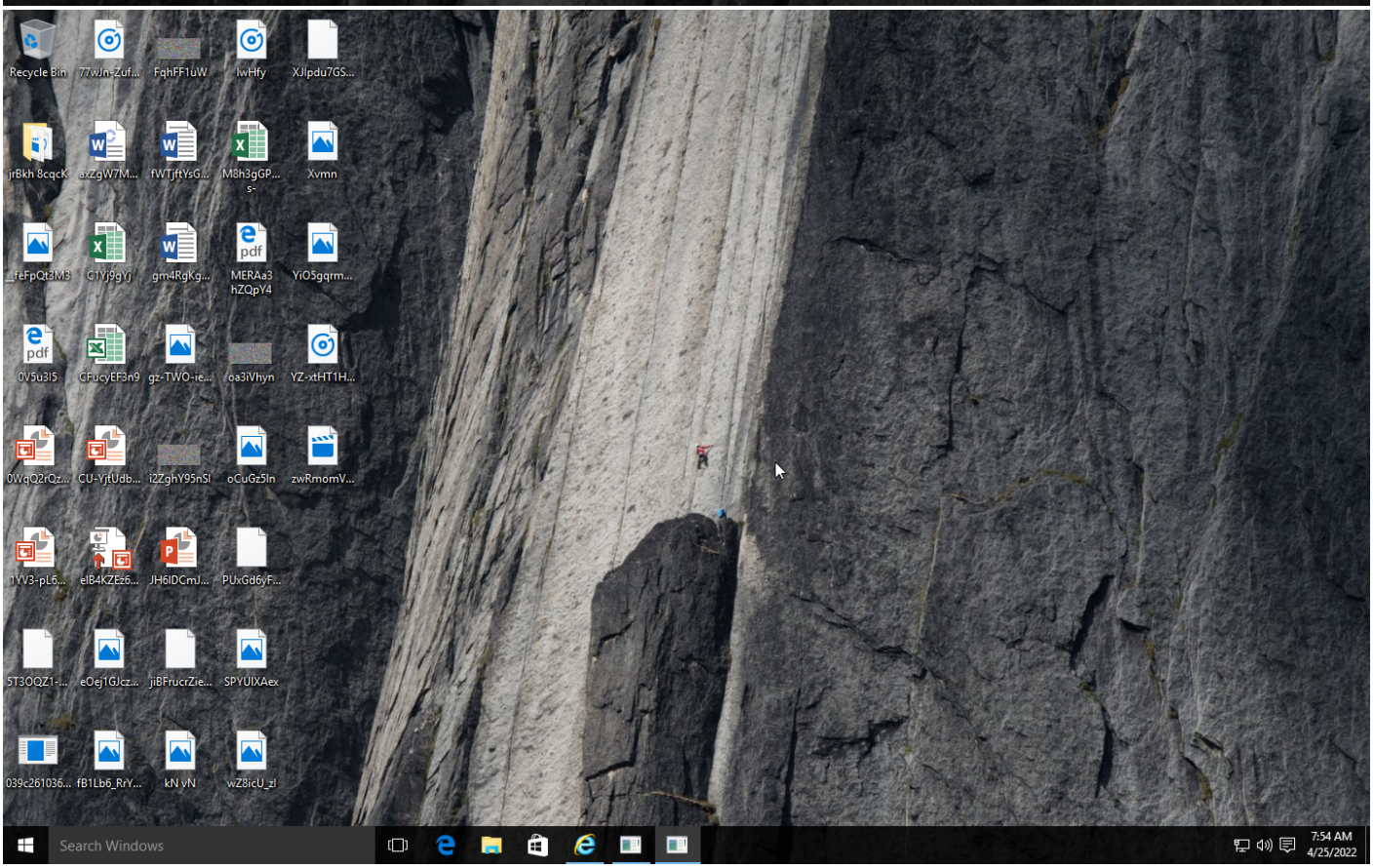
Analysis Information

Creation Time	2022-04-25 09:52 (UTC+2)
Analysis Duration	00:03:56
Termination Reason	Timeout
Number of Monitored Processes	2
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	2


Recycle Bin
Search Windows
7:54 AM
4/25/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 039c261036b80fd500607279933c43c4f1c78fdba1b54a...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

11.39 KB total sent

14.34 KB total received

17 ports 52257, 52377, 52325, 52422, 52360, 52300, 52429, 52399, 80, 52339, 21, 52309, 52405, 52345, 443, 52316, 52413

4 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 2 servers

2 sessions, 1.72 KB sent, 10.03 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://checkip.dyndns.org/	-	-		0 bytes	NA
GET	https://freegeoip.app/xml/84.182.255.145	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	checkip.dyndns.org, checkip.dyndns.com	NoError	193.122.6.168, 193.122.130.0, 132.226.247.73, 158.101.44.242, 132.226.8.169	checkip.dyndns.com	NA
A	freegeoip.app	NoError	188.114.96.7, 188.114.97.7		NA

BEHAVIOR

Process Graph

Process #1: 039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 86543, Reason: Analysis Target
Unmonitor End Time	End Time: 321777, Reason: Terminated by Timeout
Monitor duration	235.23s
Return Code	Unknown
PID	1624
Parent PID	1184
Bitness	32 Bit

Host Behavior

Type	Count
Module	27
System	167
User	15
Process	1
Registry	83
File	125
Mutex	25
-	17
Environment	3
-	3
Window	15

Network Behavior

Type	Count
HTTP	2
HTTPS	1
DNS	2
TCP	17

Process #2: netsh.exe

ID	2
File Name	c:\windows\syswow64\netsh.exe
Command Line	"netsh" wlan show profile
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 190417, Reason: Child Process
Unmonitor End Time	End Time: 229329, Reason: Terminated
Monitor duration	38.91s
Return Code	1
PID	4300
Parent PID	1624
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
039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154	C:\Users\RDhJ0CNFevzX\Desktop\039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	Sample File	470.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
System Paging File	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data\Default\Ya Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Xpom\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Nichrome\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Slimjet\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\GhostBrowser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Xvast\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\SuperBird\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Browser\Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data\Default\Login Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\UCBrowser\User Data_i18n\Default\UC Login Data.18	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Blisk\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera\Opera\profile\wand.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\.purple\accounts.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Liebao7\User Data\Default\EncryptedStorage	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\AVAST Software\Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kinza\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BlackHawk\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MFC42u.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome SxS\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\SalamWeb\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\discord\Local Storage\leveldb\	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\machine.config	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://checkip.dyndns.org	-	132.226.247.73	-	GET	CLEAN
https://freegeoip.app/xml/84.182.255.145	-	188.114.96.7	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
checkip.dyndns.org	193.122.130.0, 158.101.44.242, 132.226.247.73, 132.226.8.169, 193.122.6.168	-	DNS, HTTP	CLEAN
checkip.dyndns.com	193.122.130.0, 158.101.44.242, 132.226.247.73, 132.226.8.169, 193.122.6.168	-	DNS	CLEAN
freegeoip.app	188.114.96.7, 188.114.97.7	-	DNS, HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
103.147.185.85	-	Vietnam	TCP	CLEAN
132.226.247.73	checkip.dyndns.org, checkip.dyndns.com	Brazil	DNS, TCP, HTTP	CLEAN
188.114.96.7	freegeoip.app	Colombia	DNS, TCP, HTTPS	CLEAN
193.122.6.168	checkip.dyndns.org, checkip.dyndns.com	Germany	DNS	CLEAN
193.122.130.0	checkip.dyndns.org, checkip.dyndns.com	United States	DNS	CLEAN
158.101.44.242	checkip.dyndns.org, checkip.dyndns.com	United States	DNS	CLEAN
132.226.8.169	checkip.dyndns.org, checkip.dyndns.com	Japan	DNS	CLEAN
188.114.97.7	freegeoip.app	Colombia	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Global\.net clr networking	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\Library	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\IsMultiInstance	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\First Counter	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\CategoryOptions	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\FileMappingSize	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\Counter Names	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727\SchUseStrongCrypto	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Foxmail.url.mailto\Shell\open\command	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\DigitalProductID	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetSh	access	netsh.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	CLEAN

Process

Process Name	Commandline	Verdict
039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	"C:\Users\RDhJ0CNFevzX\Desktop\039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe"	MALICIOUS
netsh.exe	"netsh" wlan show profile	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	SnakeKeylogger	Snake Keylogger	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154.exe	Keylogger, Spyware	5/5
Malware	SnakeKeylogger	Snake Keylogger	Memory Dump	-	Keylogger, 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	4.4.1
Dynamic Engine Version	4.4.1 / 01/14/2022 05:06
Static Engine Version	4.4.1.0 / 2022-01-14 04:00:58
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.16 / 2022-03-11 16:16:43
Smart Memory Dumping Rules Version	4.4.1.6 / 2021-12-14 15:06:27
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.19 / 2022-03-31 10:55:59
YARA Built-in Ruleset Version	4.4.1.19

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows