MALICIOUS

Classifications: Keylogger, Spyware

Threat Names: Phoenix, Trojan.NSISX.Spy.Gen.4, DeepScan:Generic.MSIL.PasswordStealerA.47BAF09B

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe**
ID	#967530
MD5	fcce8f5a7e5fcdf78c02d6543c1af2bd
SHA1	b2ea7197933811fc65425d46324af8ee231117f3
SHA256	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0
File Size	318.29 KB
Report Created	2021-09-27 22:06 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (23 rules, 51 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Keylogger, Spyware
	• Rule "PhoenixKeylogger" from ruleset "Malware" has matched on the function strings for (process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Orbitum, Epic Privacy Browser, Pidgin, Torch, Yandex Browser, Vivaldi, FileZilla, 7Star, Kometa, ...Coc, Chromium, Chrome Canary, Elements Browser, Microsoft Outlook, Google Chrome, Comodo Dragon, Amigo, CentBrowser, Maple Studio.			
4/5	Antivirus	Malicious content was detected by heuristic scan	3	-
	• Built-in AV detected the sample itself as "Trojan.NSISX.Spy.Gen.4". • Built-in AV detected a memory dump of (process #1) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe as "DeepScan:Generic.MSIL.PasswordStealerA.47BAF09B". • Built-in AV detected a memory dump of (process #1) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe as "Generic.Malware.SPfVI.AEA83DC1".			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe reads the network adapters' addresses by API.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	Data Collection	Reads sensitive browser data	20	-
	• (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Yandex Browser" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Amigo" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Kometa" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "CocCoc" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Orbitum" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Vivaldi" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Chromium" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "CentBrowser" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Chedot" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Comodo Dragon" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Torch" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Epic Privacy Browser" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Opera" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Uran" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "7Star" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Chrome Canary" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Maple Studio" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Sputnik" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of web browser "Elements Browser" by file.			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of ftp application "FileZilla" by file.			
2/5	Data Collection	Reads sensitive application data	1	-

Score	Category	Operation	Count	Classification
	• (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to read sensitive data of application "Pidgin" by file.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe has a thread which sleeps more than 5 minutes.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe modifies memory of (process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe alters context of (process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	3	-
	• (Process #1) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe makes a direct system call to "NtUnmapViewOfSection". • (Process #1) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe makes a direct system call to "NtWriteVirtualMemory". • (Process #1) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe makes a direct system call to "NtResumeThread".			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe starts (process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe reads from (process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to gather information about application "FileZilla" by file. • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to gather information about application "Pidgin" by file.			
1/5	Discovery	Checks external IP address	1	-
	• (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe checks external IP by asking IP info service at "http://checkip.dyndns.org/".			
1/5	Execution	Drops PE file	1	-
	• (Process #1) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3BF.tmp\sbolbwplhfo.dll".			
1/5	Execution	Executes itself	1	-
	• (Process #1) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe.			
1/5	Network Connection	Performs DNS request	3	-

Score	Category	Operation	Count	Classification
		• (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe resolves host name "checkip.dyndns.org" to IP "132.226.247.73". • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe resolves host name "freegeoip.app" to IP "172.67.188.154". • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe resolves host name "mail.24310.gr" to IP "178.63.69.174".		
1/5	Network Connection	Connects to remote host	3	-
		• (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe opens an outgoing TCP connection to host "178.63.69.174:587". • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe opens an outgoing TCP connection to host "132.226.247.73:80". • (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe opens an outgoing TCP connection to host "172.67.188.154:443".		
1/5	Network Connection	Tries to connect using an uncommon port	1	-
		• (Process #2) 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe tries to connect to TCP port 587 at 178.63.69.174.		

Mitre ATT&CK Matrix

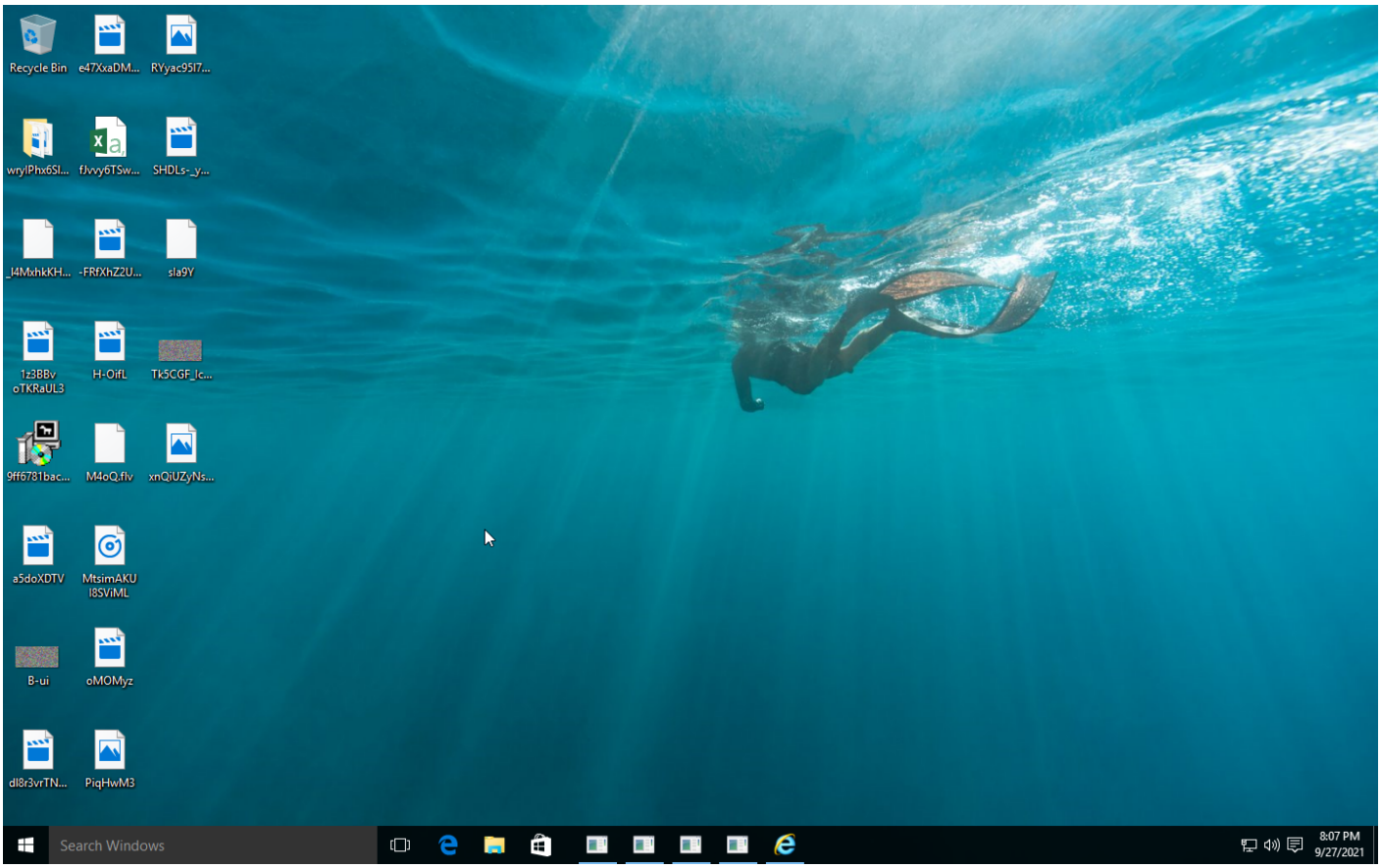
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1214 Credentials in Registry	#T1016 System Network Configuration Discovery		#T1119 Automated Collection	#T1065 Uncommonly Used Port		
				#T1045 Software Packing	#T1081 Credentials in Files	#T1012 Query Registry		#T1005 Data from Local System			
						#T1083 File and Directory Discovery					

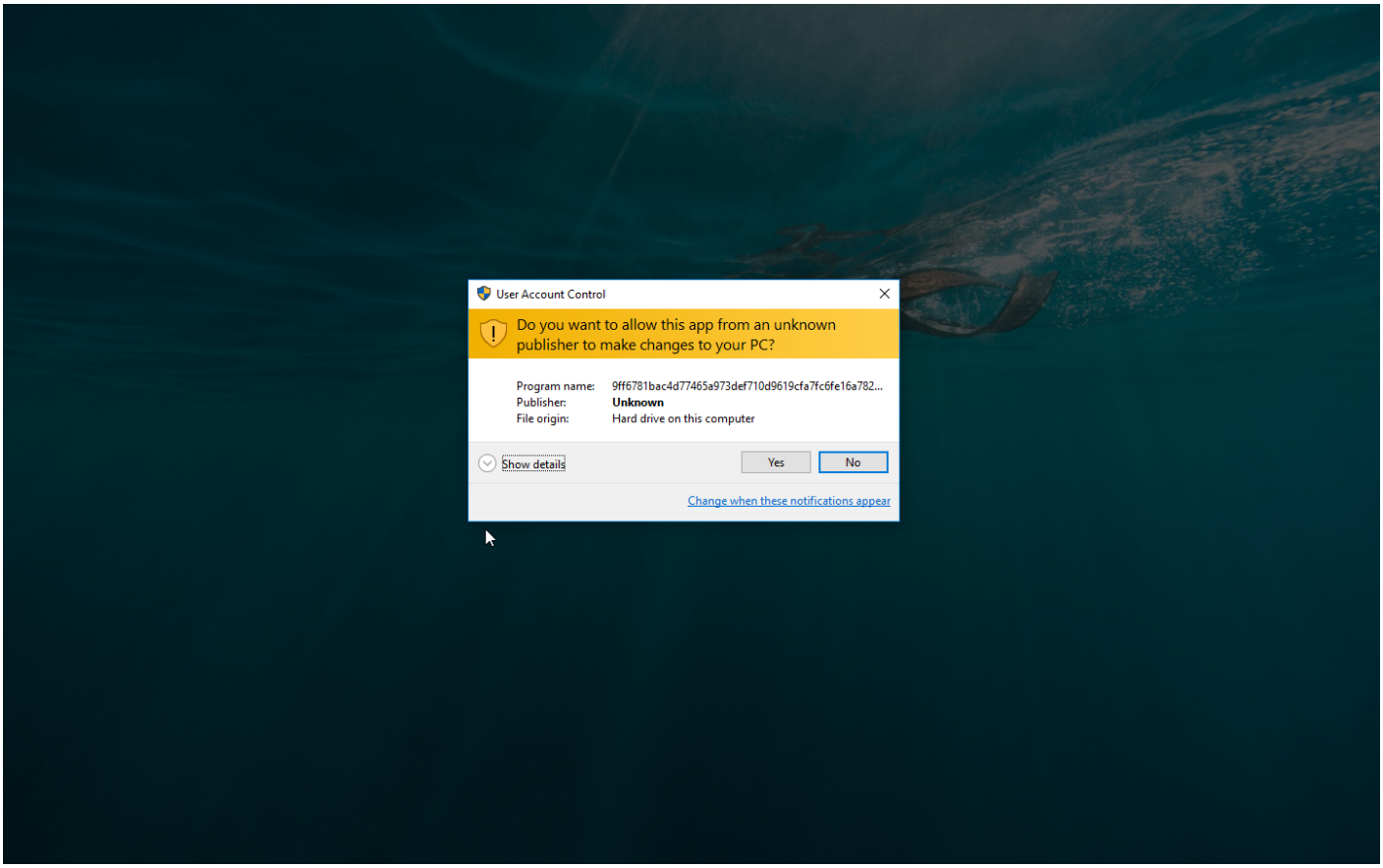
Sample Information

ID	#967530
MD5	fcce8f5a7e5fcdf78c02d6543c1af2bd
SHA1	b2ea7197933811fc65425d46324af8ee231117f3
SHA256	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0
SSDeep	6144:F8LxBs9fvNLROF9fYjzpeoG7DDCImlUR7WJDVcQTJ8iL2A03cu:/p1LQUj9eL7Slm87WJHJ8+2b3cu
ImpHash	b76363e9cb88bf9390860da8e50999d2
File Name	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe
File Size	318.29 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-27 22:06 (UTC+2)
Analysis Duration	00:04:00
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	2
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	1


Recycle Bin
e47XxaDM...
RYyac95I7...
wryIPhx6SI...
fJvvy6TSw...
SHDLs-_y...
_l4MxhkKH...
-FRfXhZ2U...
sla9Y
1z3BBv oTKRaUL3
H-OifL
Tk5CGF_Ic...
9ff6781bac...
M4oQ.flv
xnQiUZyNs...
a5doXDTV
MtsimAKU I8SViML
B-ui
oMOMyz
dl8r3vrTN...
PiqHwM3
Search Windows
8:07 PM
9/27/2021


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a782...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

NETWORK

General

51.51 KB total sent

23.19 KB total received

3 ports 80, 587, 443

4 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

7 DNS requests for 3 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 2 servers

2 sessions, 1.63 KB sent, 9.44 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/88.153.199.169	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	checkip.dyndns.org, checkip.dyndns.com	NoError	132.226.247.73, 216.146.43.70, 193.122.130.0, 158.101.44.242, 132.226.8.169, 216.146.43.71, 193.122.6.168	checkip.dyndns.com	NA
A	freegeoip.app	NoError	172.67.188.154, 104.21.19.200		NA
A	mail.24310.gr, 24310.gr	NoError	178.63.69.174	24310.gr	NA
-	checkip.dyndns.org	-	132.226.247.73, 216.146.43.70, 158.101.44.242, 132.226.8.169, 216.146.43.71, 193.122.130.0, 193.122.6.168		NA
-	mail.24310.gr	-	178.63.69.174		NA

BEHAVIOR

Process Graph

Process #1: 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 57827, Reason: Analysis Target
Unmonitor End Time	End Time: 100988, Reason: Terminated
Monitor duration	43.16s
Return Code	0
PID	1232
Parent PID	1636
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3BF.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\150qx0uurbj07478t	279.50 KB	4a32b80c0753d81b6675d53341fd77d1622c9ae376f2d6654fd2a20fb8e5749e	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3BF.tmp\sbolbwplhfo.dll	48.00 KB	7660cdd2db7356c36acb9d2472ac2c89ebdfd79eef56de9dbfed34fcde381790	✗

Host Behavior

Type	Count
System	57
Module	32
File	178
Process	1
-	3
-	9

Process #2: 9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe"
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 97079, Reason: Child Process
Unmonitor End Time	End Time: 304523, Reason: Terminated by Timeout
Monitor duration	207.44s
Return Code	Unknown
PID	2160
Parent PID	1232
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	0x4b0	0x400000(4194304)	0x400	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	0x4b0	0x401000(4198400)	0xac00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	0x4b0	0x40c000(4243456)	0x5a00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	0x4b0	0x412000(4268032)	0x800	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	0x4b0	0x414000(4276224)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	0x4b0	0x415000(4280320)	0x34a00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	0x4b0	0x20b008(2142216)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	0x4b0 / 0x60	0x772d8fe0(1999474656)	-	✓	1

Host Behavior

Type	Count
Module	32
File	125
System	49

Type	Count
Environment	12
User	77
Registry	75
-	17
Mutex	19
Window	6

Network Behavior

Type	Count
HTTP	2
HTTPS	1
DNS	7
TCP	20

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0	C:\Users\RDhJ0CNFevzX\Desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	Sample File	318.29 KB	application/vnd.microsoft.portable-executable	Read, Access	MALICIOUS
4a32b80c0753d81b6675d53341fd77d1622c9ae376f2d6654fd2a20fb8e5749e	C:\Users\RDHJ0C~1\AppData\Local\Temp\150qx0uurbj07478t	Dropped File	279.50 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
7660cdd2db7356c36acb9d2472ac2c89ebdfd79eef56de9dbfed34fcde381790	C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3BF.tmp\sbolbwplhfo.dll	Dropped File	48.00 KB	application/vnd.microsoft.portable-executable	Create, Access, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDHJ0C~1\AppData\Local\Temp\	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nspFDA3.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	Sample File	Read, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3BF.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Users	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\150qx0uurbj07478t	Dropped File	Read, Create, Access, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3BF.tmp\sbolbwplhfo.dll	Dropped File	Create, Access, Write	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Read, Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe.config	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\Google\Chrome\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

File Name	Category	Operations	Verdict
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
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

File Name	Category	Operations	Verdict
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:\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
C:\Users\RDhJ0CNFevzX\AppData\Roaming\discord\Local Storage\leveldb\	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/88.153.199.169	-	172.67.188.154	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
checkip.dyndns.org	132.226.247.73, 216.146.43.71, 193.122.6.168, 193.122.130.0, 132.226.8.169, 158.101.44.242, 216.146.43.70	-	DNS, HTTP	CLEAN
checkip.dyndns.com	132.226.247.73, 158.101.44.242, 216.146.43.71, 193.122.130.0, 132.226.8.169, 193.122.6.168, 216.146.43.70	-	DNS	CLEAN
freegeoip.app	104.21.19.200, 172.67.188.154	-	DNS, HTTPS	CLEAN
mail.24310.gr	178.63.69.174	-	DNS	CLEAN
24310.gr	178.63.69.174	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	DNS, UDP	CLEAN
178.63.69.174	24310.gr, mail.24310.gr	Germany	DNS, TCP	CLEAN
132.226.247.73	checkip.dyndns.org, checkip.dyndns.com	Brazil	DNS, HTTP, TCP	CLEAN
172.67.188.154	freegeoip.app	United States	DNS, HTTPS, TCP	CLEAN
216.146.43.70	checkip.dyndns.org, checkip.dyndns.com	United States	DNS	CLEAN
193.122.130.0	checkip.dyndns.org, checkip.dyndns.com	United States	DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
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
216.146.43.71	checkip.dyndns.org, checkip.dyndns.com	United States	DNS	CLEAN
193.122.6.168	checkip.dyndns.org, checkip.dyndns.com	Germany	DNS	CLEAN
104.21.19.200	freegeoip.app	-	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Foxmail.url.mailto\Shell\open\command	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	CLEAN

Process

Process Name	Commandline	Verdict
9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	"C:\Users\RDhJ0CNFevzX\Desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe"	MALICIOUS

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	PhoenixKeylogger	Phoenix Keylogger	Function Strings	function_strings_process_2.txt	Keylogger, Spyware	5/5

Antivirus (2)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.NSISX.Spy.Gen.4	C:\Users\RDhJ0CNFevzX\Desktop\9ff6781bac4d77465a973def710d9619cfa7fc6fe16a78225b7e22d3a89d0be0.exe	MALICIOUS
Memory Dump	DeepScan:Generic.MSIL.PasswordStealerA.47BAF09B	-	MALICIOUS

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	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-27 16:34:30+00:00
Built-in AV Database Records	10473840

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