MALICIOUS

Classifications: Spyware

Threat Names: Agent Tesla | Agent Tesla v3 | Trojan.NSISX.Spy.Gen.2 | Gen:Variant.Fugrafa.108481

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe**
ID	#969561
MD5	71028a6ec414b1642243aa4981a3365f
SHA1	630b016a94f7bee220565d3b9a55a2ae8ef73c5a
SHA256	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918
File Size	310.05 KB
Report Created	2021-09-28 16:04 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (25 rules, 76 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	3	Spyware

- Rule "AgentTesla_HTML_Message" from ruleset "Malware" has matched on layer 4 network traffic to IP "185.104.29.70:587".
- Rule "AgentTesla_StringDecryption_v3" from ruleset "Malware" has matched on a memory dump for (process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe.
- Rule "AgentTesla_StringDecryption_v3" from ruleset "Malware" has matched on a memory dump for (process #1) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe.

Score	Category	Operation	Count	Classification
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware

- Tries to read sensitive data of: CoreFTP, Flock, Comodo IceDragon, Cyberfox, TightVNC, Internet Download Manager, Internet Explore... ... Mozilla Thunderbird, Postbox, Microsoft Outlook, SeaMonkey, BlackHawk, Internet Explorer, Opera Mail, The Bat!, WinSCP, TigerVNC.

Score	Category	Operation	Count	Classification
4/5	Antivirus	Malicious content was detected by heuristic scan	3	-

- Built-in AV detected the sample itself as "Trojan.NSISX.Spy.Gen.2".
- Built-in AV detected a memory dump of (process #1) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe as "Gen:Variant.Fugrafa.108481".
- Built-in AV detected a memory dump of (process #1) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe as "IL:Trojan.MSILZilla.1773".

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive browser data	9	-

- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of web browser "Opera" by file.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of web browser "k-Meleon" by file.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of web browser "Flock" by file.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of web browser "Comodo IceDragon" by file.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of web browser "Mozilla Firefox" by file.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of web browser "BlackHawk" by file.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of web browser "Cyberfox" by file.

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive mail data	7	-

- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of mail application "Pocomail" by file.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of mail application "Opera Mail" by file.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of mail application "IncrediMail" by registry.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of mail application "The Bat!" by file.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of mail application "Postbox" by file.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive application data	6	-

- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of application "WinSCP" by registry.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of application "Internet Download Manager" by registry.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of application "SeaMonkey" by file.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of application "OpenVPN" by registry.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of application "TightVNC" by registry.
- (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of application "TigerVNC" by registry.

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive ftp data	5	-

Score	Category	Operation	Count	Classification
	• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of ftp application "Ipswitch WS_FTP" by file. • (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of ftp application "CoreFTP" by file. • (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of ftp application "CoreFTP" by registry. • (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of ftp application "FileZilla" by file. • (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to read sensitive data of ftp application "FTP Navigator" by file.		
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe queries OS version via WMI.			
2/5	Discovery	Executes WMI query	2	-
	• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe executes WMI query: select * from Win32_OperatingSystem. • (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe executes WMI query: SELECT * FROM Win32_Processor.			
2/5	Discovery	Collects hardware properties	1	-
	• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe queries hardware properties via WMI.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe reads the network adapters' addresses by API.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe modifies memory of (process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe alters context of (process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	3	-
	• (Process #1) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe makes a direct system call to "NtUnmapViewOfSection". • (Process #1) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe makes a direct system call to "NtWriteVirtualMemory". • (Process #1) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe makes a direct system call to "NtResumeThread".			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe starts (process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe reads from (process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.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) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Possibly does reconnaissance	22	-

Score	Category	Operation	Count	Classification
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "Pocomail" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "WinSCP" by registry.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "Opera Mail" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "SeaMonkey" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "k-Meleon" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "WS_FTP" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "The Bat!" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "Flock" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "Postbox" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "Comodo IceDragon" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "Mozilla Firefox" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "CoreFTP" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "Qualcomm Eudora" by registry.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "FileZilla" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "Foxmail" by registry.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "blackHawk" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "icecat" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "RealVNC" by registry.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "TightVNC" by registry.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "TigerVNC" by registry.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "FTP Navigator" by file.		
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to gather information about application "Cyberfox" by file.		
1/5	Obfuscation	Resolves API functions dynamically	1	-
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe resolves 55 API functions by name.		
1/5	Network Connection	Performs DNS request	1	-
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe resolves host name "mail.globalmedical.nl" to IP "185.104.29.70".		
1/5	Network Connection	Connects to remote host	1	-
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe opens an outgoing TCP connection to host "185.104.29.70:587".		
1/5	Network Connection	Tries to connect using an uncommon port	1	-
		• (Process #2) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe tries to connect to TCP port 587 at 185.104.29.70.		
1/5	Execution	Drops PE file	1	-
		• (Process #1) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\nshEFEC.tmp\agyko.dll".		
1/5	Execution	Executes itself	1	-
		• (Process #1) 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe.		

Mitre ATT&CK Matrix

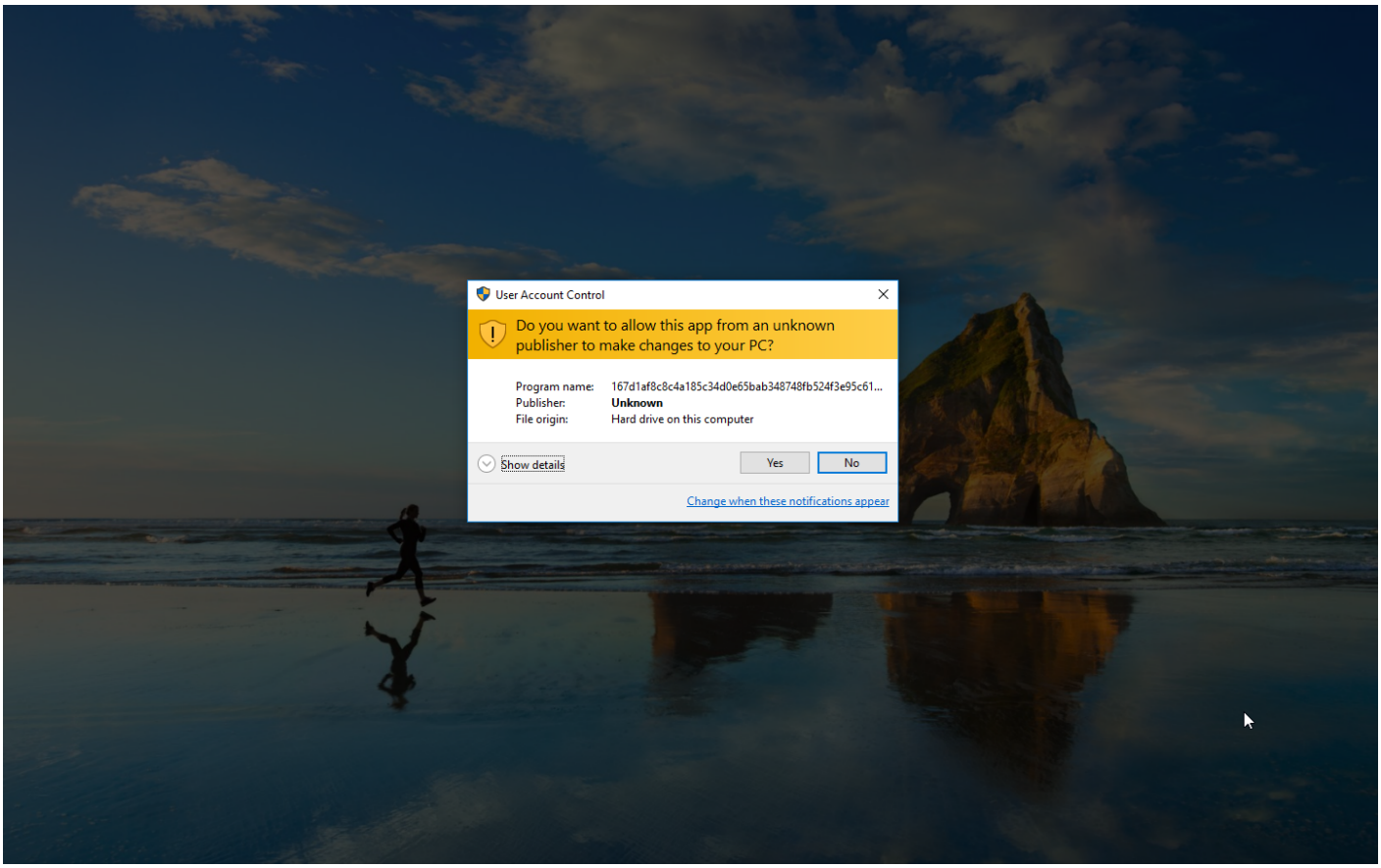
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection	#T1065 Uncommonly Used Port		
				#T1045 Software Packing	#T1214 Credentials in Registry	#T1012 Query Registry		#T1005 Data from Local System			
					#T1003 Credential Dumping	#T1082 System Information Discovery					
						#T1016 System Network Configuration Discovery					

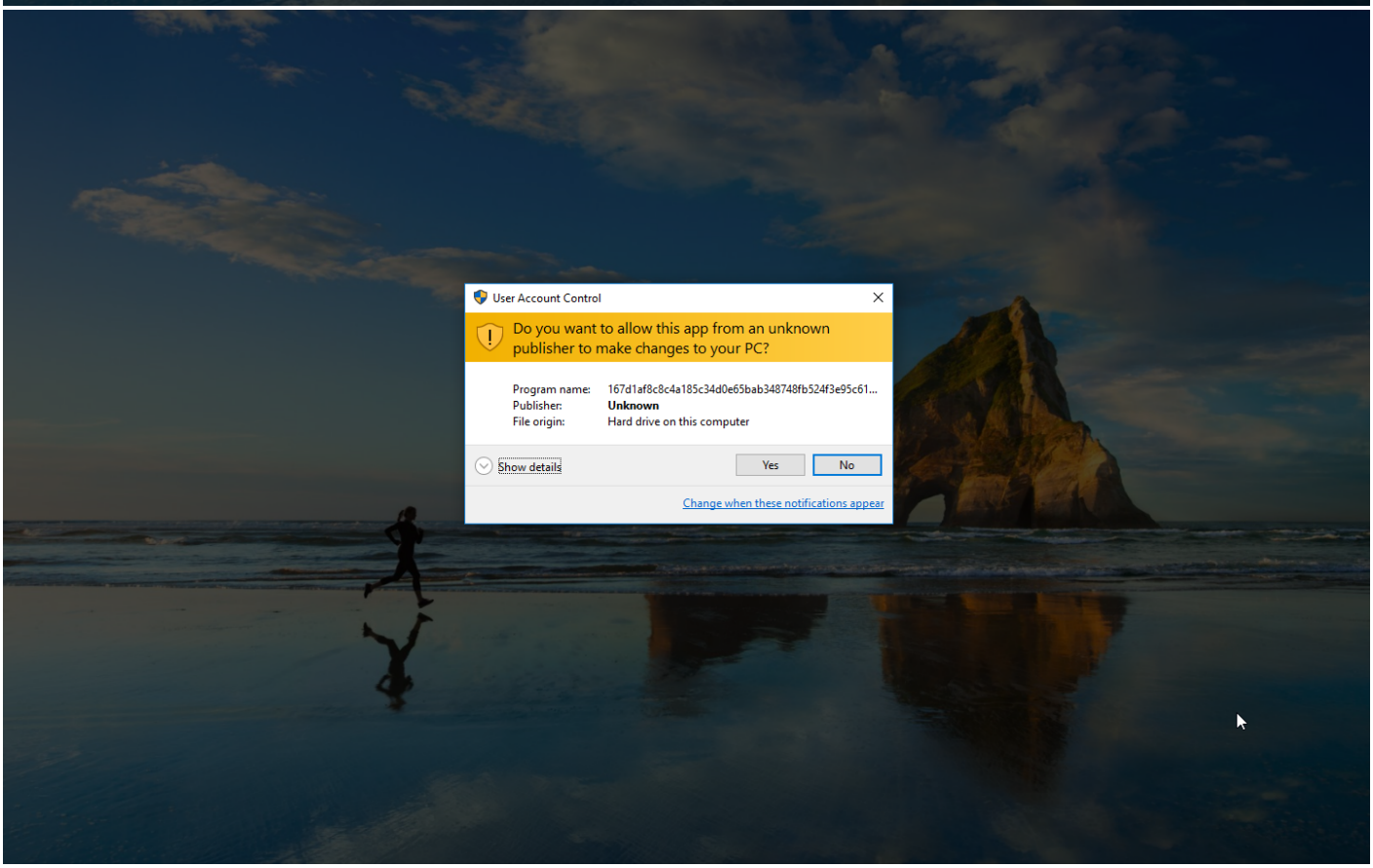
Sample Information

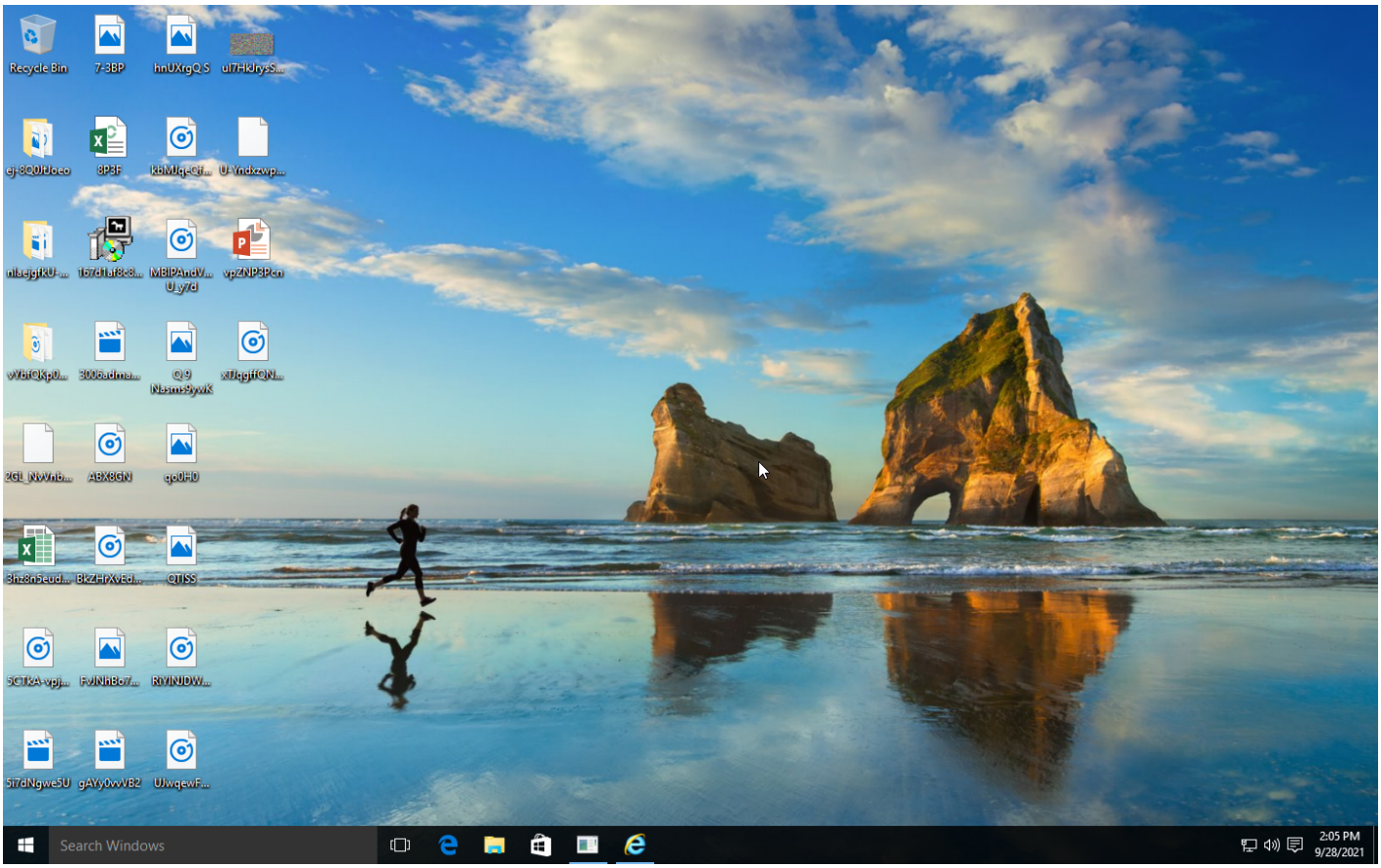
ID	#969561
MD5	71028a6ec414b1642243aa4981a3365f
SHA1	630b016a94f7bee220565d3b9a55a2ae8ef73c5a
SHA256	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918
SSDeep	6144:F8LxBsG3/D9BNOnAvOrA4WXnLHz6g2USzAmD5D96r:/G37sAv14WXnL21zAq96r
ImpHash	b76363e9cb88bf9390860da8e50999d2
File Name	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe
File Size	310.05 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

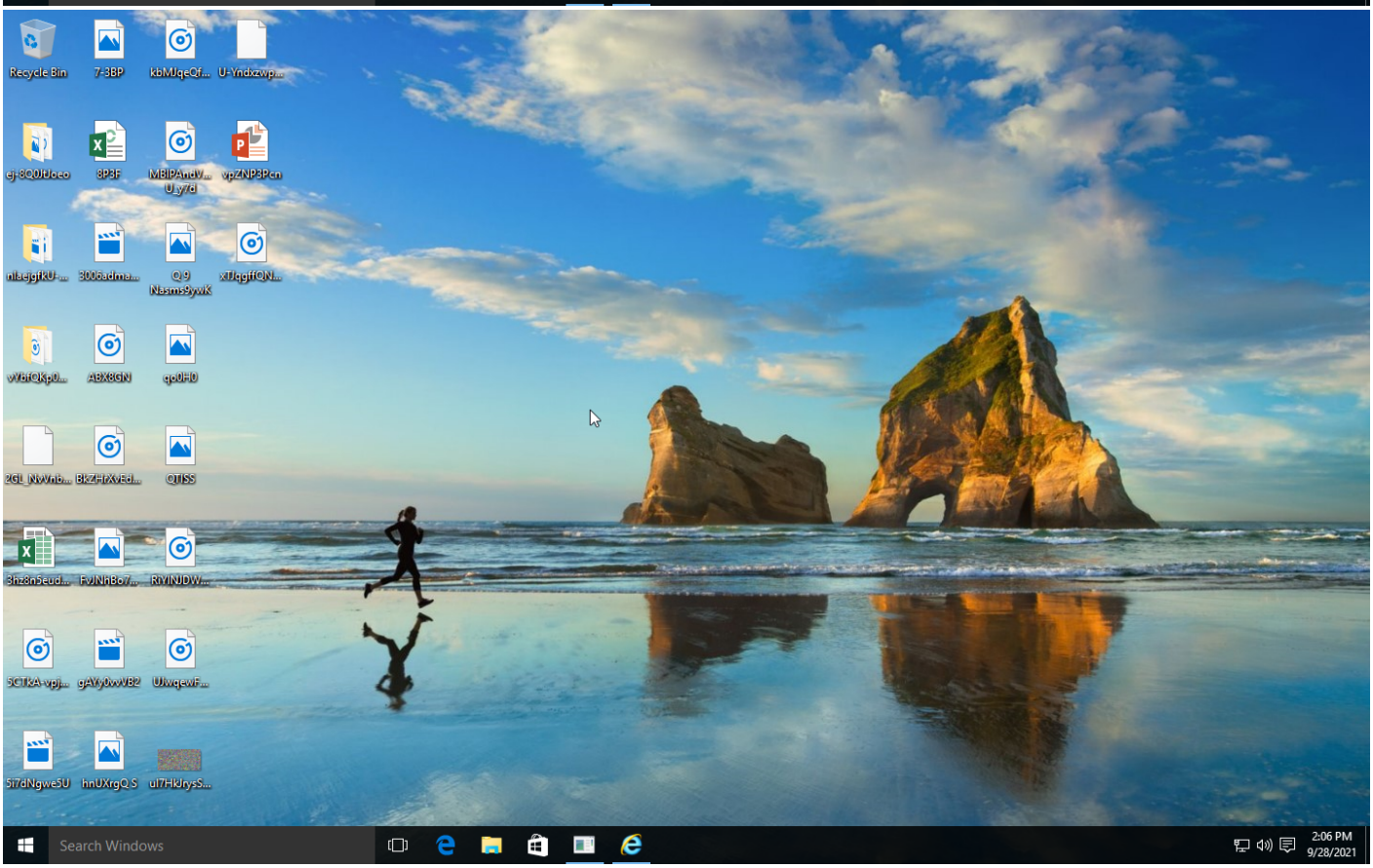
Analysis Information

Creation Time	2021-09-28 16:04 (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	12


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c61...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c61...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
7-3BP
hnUXrgQ.S
ui7HkJrysS...
ej-8QUJoeo
8P3F
kbMJqeQf...
U-Yndxzwp...
nLaejgfkU-...
167d1af8c8...
MBlPAndV...
U_y7d
vpZNP3Pcn
vVbfQKp0...
3006admia...
Q.9
Nasms9ywK
xfJqgffQN...
2GL_NvVnb...
ABX8GN
qo0HD
3hz8n5eud...
BkZHrXvEd...
QTlSS
5CTkA-vpj...
FvJNhBo7...
RtYlNJDW...
5i7dNgwe5U
gAYy0vvVB2
UJwqewF...
Search Windows
2:05 PM
9/28/2021


Recycle Bin
7-3BP
kbMJqeQf...
U-Yndxzwp...
ej-8QUJoeo
8P3F
MBlPAndV...
U_y7d
vpZNP3Pcn
nLaejgfkU-...
3006admia...
Q.9
Nasms9ywK
xfJqgffQN...
vVbfQKp0...
ABX8GN
qo0HD
2GL_NvVnb...
BkZHrXvEd...
QTlSS
3hz8n5eud...
FvJNhBo7...
RtYlNJDW...
5CTkA-vpj...
gAYy0vvVB2
UJwqewF...
5i7dNgwe5U
hnUXrgQ.S
ui7HkJrysS...
Search Windows
2:06 PM
9/28/2021

NETWORK

General

1.22 KB total sent

918 bytes total received

1 ports 587

2 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	mail.globalmedical.nl	NoError	185.104.29.70		NA

BEHAVIOR

Process Graph

Process #1: 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 62286, Reason: Analysis Target
Unmonitor End Time	End Time: 108804, Reason: Terminated
Monitor duration	46.52s
Return Code	0
PID	4908
Parent PID	1636
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\nshEFEC.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\lwp4r7ldzqpo26xd	286.00 KB	8b59db4a29e96b2178af1491631076557866ecd5af4df7cb1fe02dd7a2aae38d	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\nshEFEC.tmp\agyko.dll	47.00 KB	d8f687ba9eea4e69aeaad9cccafd1ecc9be0b1b09c88ab8a4b5728aba666c903	✗

Host Behavior

Type	Count
System	55
Module	32
File	176
Process	1
-	3
-	9

Process #2: 167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe"
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 104817, Reason: Child Process
Unmonitor End Time	End Time: 311085, Reason: Terminated by Timeout
Monitor duration	206.27s
Return Code	Unknown
PID	1624
Parent PID	4908
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\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	0x1318	0x400000(4194304)	0x400	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	0x1318	0x401000(4198400)	0xac00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	0x1318	0x40c000(4243456)	0x5a00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	0x1318	0x412000(4268032)	0x800	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	0x1318	0x414000(4276224)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	0x1318	0x415000(4280320)	0x36400	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	0x1318	0x2f3008(3092488)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	0x1318 / 0x7f4	0x772d8fe0(1999474656)	-	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\\tmpG692.tmp	310.05 KB	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918	✗

Host Behavior

Type	Count
Module	84
File	156
System	36
Environment	27
Window	6
Registry	96
User	4
-	6
COM	37
-	2
Mutex	2

Network Behavior

Type	Count
DNS	1
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\\tmpG692.tmp, C:\Users\RDhJ0CNFevzX\Desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	Sample File	310.05 KB	application/vnd.microsoft.portable-executable	Create, Read, Delete, Write, Access	MALICIOUS
8b59db4a29e96b2178af1491631076557866ecd5af4df7cb1fe02dd7a2aae38d	C:\Users\RDHJ0C~1\AppData\Local\Temp\lwp4r7ldzqpo26xd	Dropped File	286.00 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
d8f687ba9eea4e69aeaad9ccafd1ecc9be0b1b09c88ab8a4b5728aba666c903	C:\Users\RDHJ0C~1\AppData\Local\Temp\nshEFEC.tmp\agyko.dll	Dropped File	47.00 KB	application/vnd.microsoft.portable-executable	Write, Create, Access	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\nspEA0F.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	Sample File	Read, Delete, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nshEFEC.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\lwp4r7ldzqpo26xd	Dropped File	Write, Read, Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nshEFEC.tmp\agyko.dll	Dropped File	Write, Create, Access	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\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe.config	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\\tmpG692.tmp	Sample File	Write, Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Pocomail\accounts.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\MoonchiId Productions\Pale Moon\profiles.ini	Accessed File	Access	CLEAN
C:\cftp\Ftplist.txt	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Protect\S-1-5-21-1560258661-3990802383-1811730007-1000\be39cc84-e9bf-4c2d-a3a5-e953c9f3df24	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Claws-mail	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Claws-mail\clawsrc	Accessed File	Access	CLEAN
C:\Users\All Users\AppData\Roaming\FlashFXP\3quick.dat	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Mail\Opera Mail\wand.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\Folder.lst	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data\Default\EncryptedStorage	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Mailbird\Store\Store.db	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\MySQL\Workbench\workbench_user_data.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Ipswitch\WS_FTP\Sites\ws_ftp.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\The Bat!	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Flock\Browser\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Postbox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\NordVPN	Accessed File	Access	CLEAN
C:\Program Files\Private Internet Access\data	Accessed File	Access	CLEAN
C:\Private Internet Access\data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Comodo\IceDragon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\CoreFTP\sites.idx	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Storage\	Accessed File	Access	CLEAN
C:\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files (x86)\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Trillian\users\global\accounts.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHawk\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Waterfox\profiles.ini	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\plutil.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FTPGetter\servers.xml	Accessed File	Access	CLEAN
C:\Program Files (x86)\jDownloader\config\database.script	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\falkon\profiles\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\icecat\profiles.ini	Accessed File	Access	CLEAN
C:\Program Files (x86)\uvnc bvba\UltraVNC\ultravnc.ini	Accessed File	Access	CLEAN
C:\Program Files (x86)\UltraVNC\ultravnc.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Psi\profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Psi+\profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\eM Client	Accessed File	Access	CLEAN
C:\FTP Navigator\Ftplist.txt	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\profiles.ini	Accessed File	Access	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
mail.globalmedical.nl	185.104.29.70	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
185.104.29.70	mail.globalmedical.nl	Netherlands	DNS, TCP	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\DownloadManager\Passwords	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\RimArts\B2\Settings	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\OpenVPN-GUI\configs	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites\Host	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesPort	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesUser	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesPW	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesName	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Qualcomm\Eudora\CommandLine	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\FoxmailPreview	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\vncserver	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\vncserver	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\WinVNC4	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\ORL\WinVNC3	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TightVNC\Server	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\TightVNC\Server	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TigerVNC\Server	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN
HKEY_CURRENT_USER\Software\TigerVNC\Server	access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	CLEAN

Process

Process Name	Commandline	Verdict
167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	"C:\Users\RDhJ0CNFevzX\Desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe"	MALICIOUS

YARA / AV

YARA (12)

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

Antivirus (2)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.NSISX.Spy.Gen.2	C:\Users\RDhJ0CNFevzX\Desktop\167d1af8c8c4a185c34d0e65bab348748fb524f3e95c6136324f1e2d7e310918.exe	MALICIOUS
Memory Dump	Gen:Variant.Fugrafa.108481	-	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	2021-09-28 11:29:58+00:00
Built-in AV Database Records	10481709

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