MALICIOUS

Classifications: Spyware, Keylogger

Threat Names: Agent Tesla, Agent Tesla v3, Mal/Generic-S, C2/Generic-A, Trojan.GenericKD.47057587

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe**
ID	#2780293
MD5	768a1127c119149f96a29c0d0c0b56ec
SHA1	afe86ab8d4a8b5b092e95f1cb2ae563f5ea5867d
SHA256	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af
File Size	860.50 KB
Report Created	2021-09-27 17:45 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (26 rules, 72 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	2	Spyware
	• Rule "AgentTesla_HTML_Message" from ruleset "Malware" has matched on layer 4 network traffic to IP "208.91.199.223:587". • Rule "AgentTesla_StringDecryption_v3" from ruleset "Malware" has matched on a memory dump for (process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Cyberfox, BlackHawk, TigerVNC, Pocomail, Opera, Flock, FTP Navigator, The Bat!, Opera Mail, SeaMo... ..., Ipswitch WS_FTP, Comodo IceDragon, FileZilla, Postbox, OpenVPN, Internet Explorer, Internet Download Manager, CoreFTP, k-Meleon.			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected the sample itself as "Trojan.GenericKD.47057587".			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
4/5	Reputation	Contacts known malicious IP address	1	-
	• Reputation analysis labels the contacted IP address 208.91.198.143 as "C2/Generic-A".			
3/5	Input Capture	Monitors keyboard input	1	Keylogger
	• (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe installs system wide "WH_KEYBOARD_LL" hook(s) to monitor keystrokes.			
2/5	Data Collection	Reads sensitive browser data	9	-
	• (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of web browser "Opera" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of web browser "Flock" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of web browser "BlackHawk" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of web browser "k-Meleon" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of web browser "Comodo IceDragon" by file.			
2/5	Data Collection	Reads sensitive mail data	7	-
	• (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of mail application "Postbox" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of mail application "IncrediMail" by registry. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of mail application "The Bat!" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of mail application "Opera Mail" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of mail application "Pocomail" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file.			
2/5	Data Collection	Reads sensitive ftp data	5	-

Score	Category	Operation	Count	Classification
		• (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of ftp application "Ipswitch WS_FTP" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of ftp application "FTP Navigator" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of ftp application "CoreFTP" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of ftp application "CoreFTP" by registry. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of ftp application "FileZilla" by file.		
2/5	Data Collection	Reads sensitive application data	6	-
		• (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of application "WinSCP" by registry. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of application "OpenVPN" by registry. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of application "SeaMonkey" by file. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of application "TightVNC" by registry. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of application "TigerVNC" by registry. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to read sensitive data of application "Internet Download Manager" by registry.		
2/5	Discovery	Queries OS version via WMI	1	-
		• (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe queries OS version via WMI.		
2/5	Discovery	Executes WMI query	2	-
		• (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe executes WMI query: select * from Win32_OperatingSystem. • (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe executes WMI query: SELECT * FROM Win32_Processor.		
2/5	Discovery	Collects hardware properties	1	-
		• (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe queries hardware properties via WMI.		
2/5	Anti Analysis	Tries to detect virtual machine	1	-
		• Multiple processes are possibly trying to detect a VM via rdtsc.		
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
		• (Process #1) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe modifies memory of (process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe.		
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
		• (Process #1) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe alters context of (process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe.		
1/5	Hide Tracks	Creates process with hidden window	1	-
		• (Process #1) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe starts (process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe with a hidden window.		
1/5	Obfuscation	Reads from memory of another process	1	-
		• (Process #1) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe reads from (process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
		• (Process #1) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.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) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe enables process privilege "SeDebugPrivilege".		

Score	Category	Operation	Count	Classification
1/5	Discovery	Possibly does reconnaissance	22	-

- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "Flock" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "Postbox" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "WS_FTP" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "Qualcomm Eudora" by registry.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "Mozilla Firefox" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "WinSCP" by registry.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "icecat" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "blackHawk" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "SeaMonkey" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "FTP Navigator" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "The Bat!" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "CoreFTP" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "Opera Mail" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "Pocomail" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "RealVNC" by registry.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "TightVNC" by registry.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "TigerVNC" by registry.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "Foxmail" by registry.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "FileZilla" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "k-Meleon" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "Cyberfox" by file.
- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to gather information about application "Comodo IceDragon" by file.

Score	Category	Operation	Count	Classification
1/5	Network Connection	Performs DNS request	1	-

- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe resolves host name "smtp.vern-group.com" to IP "208.91.199.223".

Score	Category	Operation	Count	Classification
1/5	Network Connection	Connects to remote host	1	-

- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe opens an outgoing TCP connection to host "208.91.199.223:587".

Score	Category	Operation	Count	Classification
1/5	Network Connection	Tries to connect using an uncommon port	1	-

- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe tries to connect to TCP port 587 at 208.91.199.223.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	1	-

- (Process #2) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe resolves 50 API functions by name.

Score	Category	Operation	Count	Classification
1/5	Execution	Executes itself	1	-

- (Process #1) 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe.

Mitre ATT&CK Matrix

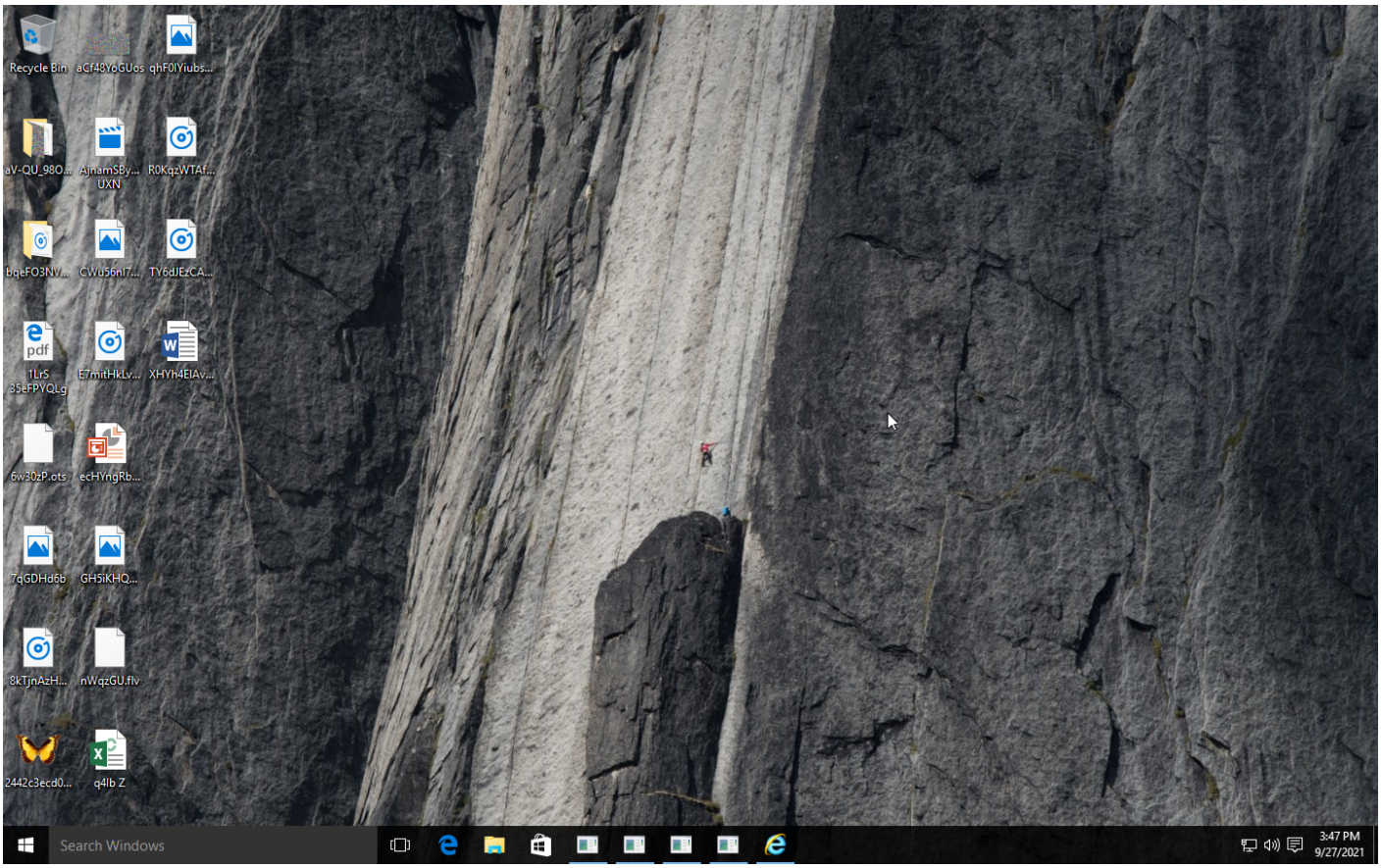
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1179 Hooking	#T1179 Hooking	#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File 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			
				#T1497 Virtualization/ Sandbox Evasion	#T1003 Credential Dumping	#T1082 System Information Discovery		#T1056 Input Capture			
					#T1056 Input Capture	#T1497 Virtualization/ Sandbox Evasion					
					#T1179 Hooking	#T1124 System Time Discovery					

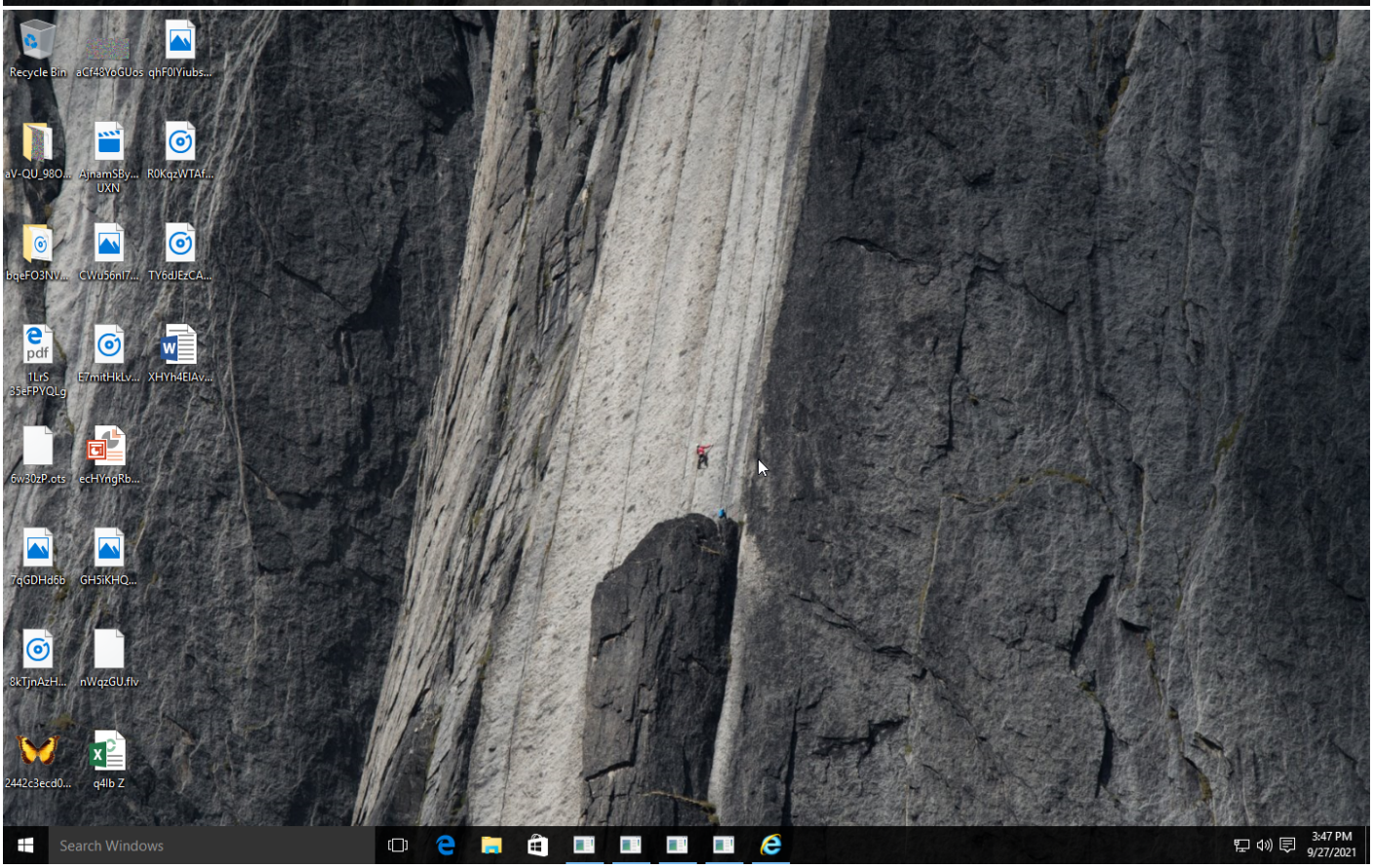
Sample Information

ID	#2780293
MD5	768a1127c119149f96a29c0d0c0b56ec
SHA1	afe86ab8d4a8b5b092e95f1cb2ae563f5ea5867d
SHA256	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af
SSDeep	12288:goSLU8CqriiULSX7yUrMjgY6WDWzjXbdarHOsnoaLOAmQsaypSL+jQHmLDsBhvs8:3blFJ9F9lPV3X2hM3akNQF+0F+2
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe
File Size	860.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-27 17:45 (UTC+2)
Analysis Duration	00:03:54
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	1
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	3


Recycle Bin
aCf48YoGUos
qhF0lYiubs...
aV-QU_98O...
AjnamSBy...
UXN
R0kqzWTAf...
bqeFO3NV...
CWu56nI7...
TY6dJEzCA...
1LrS
35eFPYQLg
E7mitHkLv...
XHYh4ElAv...
6w30zP.ots
ecHYngRb...
7qGDHd6b
GH5iKHQ...
8kTjnAzH...
nWqzGU.flv
2442c3ecd0...
q4lb Z
Search Windows
3:47 PM
9/27/2021



Screenshots truncated

NETWORK

General

1.22 KB total sent

892 bytes total received

1 ports 587

2 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

2 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	smtp.vern-group.com, us2.smtp.mailhostbox.com	NoError	208.91.199.223, 208.91.198.143, 208.91.199.224, 208.91.199.225	us2.smtp.mailhostbox.com	NA
-	smtp.vern-group.com	-	208.91.199.223, 208.91.198.143, 208.91.199.224, 208.91.199.225		NA

BEHAVIOR

Process Graph

Process #1: 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 87594, Reason: Analysis Target
Unmonitor End Time	End Time: 166318, Reason: Terminated
Monitor duration	78.72s
Return Code	0
PID	5024
Parent PID	1600
Bitness	32 Bit

Host Behavior

Type	Count
Module	46
Window	6
Registry	3
File	1
Process	1
-	3
-	7

Process #2: 2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 164375, Reason: Child Process
Unmonitor End Time	End Time: 321139, Reason: Terminated by Timeout
Monitor duration	156.76s
Return Code	Unknown
PID	4836
Parent PID	5024
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	0x1244	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	0x1244	0x402000(4202496)	0x35a00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	0x1244	0x438000(4423680)	0x600	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	0x1244	0x43a000(4431872)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	0x1244	0x220008(2228232)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	0x1244 / 0x478		-	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\\tmpG486.tmp	860.50 KB	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af	✗

Host Behavior

Type	Count
Module	64
Window	6
System	38
Registry	96

Type	Count
User	4
-	21
File	179
COM	43
Environment	38
-	2
Mutex	2

Network Behavior

Type	Count
DNS	2
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\\tmpG486.tmp, C:\Users\RDhJ0CNFevzX\Desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	Sample File	860.50 KB	application/vnd.microsoft.portable-executable	Create, Write, Access, Delete	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe.config	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Read, Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	Sample File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\\tmpG486.tmp	Sample File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\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\Kometa\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\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\Roaming\Opera Software\Opera Stable	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data	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\Roaming\Ipswitch\WS_FTP\Sites\ws_ftp.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\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\Local\Google\Chrome\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Mailbird\Store\Store.db	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Folder.lst	Accessed File	Access	CLEAN
C:\cftp\Ftplist.txt	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\Mozilla\Firefox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\All Users\AppData\Roaming\FlashFXP\3quick.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FTPGetter\servers.xml	Accessed File	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\RDhJ0CNFevzX\AppData\Roaming\Mozilla\icecat\profiles.ini	Accessed File	Access	CLEAN
C:\Program Files (x86)\jDownloader\config\database.script	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHawk\profiles.ini	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\MySQL\Workbench\workbench_user_data.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\falkon\profiles\profiles.ini	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\The Bat!	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\CoreFTP\sites.idx	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\NordVPN	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Mail\Opera Mail\wand.dat	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\Waterfox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Pocomail\accounts.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:\Program Files (x86)\uvnc bvba\UltraVNC\ultravnc.ini	Accessed File	Access	CLEAN
C:\Program Files (x86)\UltraVNC\ultravnc.ini	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\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Trillian\users\global\accounts.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Comodo\IceDragon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\UCBrowser\	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\icecat\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\SeaMonkey\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Flock\Browser\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Postbox\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Comodo\IceDragon\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Waterfox\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHawk\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\	Accessed File	Access	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
smtp.vern-group.com	208.91.199.223, 208.91.198.143, 208.91.199.224, 208.91.199.225	-	DNS	CLEAN
us2.smtp.mailhostbox.com	208.91.198.143, 208.91.199.223, 208.91.199.224, 208.91.199.225	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
208.91.198.143	us2.smtp.mailhostbox.com, smtp.vern-group.com	United States	DNS	MALICIOUS
192.168.0.1	-	-	UDP, DNS	CLEAN
208.91.199.223	us2.smtp.mailhostbox.com, smtp.vern-group.com	United States	DNS, TCP	CLEAN
208.91.199.224	us2.smtp.mailhostbox.com, smtp.vern-group.com	United States	DNS	CLEAN
208.91.199.225	us2.smtp.mailhostbox.com, smtp.vern-group.com	United States	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_PERFORMANCE_DATA	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Qualcomm\Eudora\CommandLine	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\RimArts\B2\Settings	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\OpenVPN-GUI\configs	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites\Host	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesPort	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesUser	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesPW	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesName	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\vncserver	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\vncserver	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\WinVNC4	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\ORL\WinVNC3	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TightVNC\Server	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\TightVNC\Server	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TigerVNC\Server	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\TigerVNC\Server	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\FoxmailPreview	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_CURRENT_USER\Software\DownloadManager\Passwords	access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	CLEAN

Process

Process Name	Commandline	Verdict
2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	"C:\Users\RDhJ0CNFevzX\Desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe"	MALICIOUS
2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	"C:\Users\RDhJ0CNFevzX\Desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe"	MALICIOUS

YARA / AV

YARA (3)

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

Antivirus (1)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKD.47057587	C:\Users\RDhJ0CNFevzX\Desktop\2442c3ecd04264f108429a954275ee27986e00b79cbce6d07843dfefdf4d24af.exe	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 09:44:09+00:00
Built-in AV Database Records	10465934

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