MALICIOUS

Classifications: Spyware | Injector

Threat Names: AgentTesla.v3

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe**
ID	#5068102
MD5	9c8721d5f0dfcb5893766810fc016b1b
SHA1	097e2d6bd75f55fee4ba991696d15bbd0f73137f
SHA256	22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054
File Size	825.50 KB
Report Created	2022-08-05 16:20 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (23 rules, 69 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Agent Tesla configuration was extracted	1	Spyware
	• A configuration for Agent Tesla was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
	• Rule "AgentTesla_StringDecryption_v3" from ruleset "Malware" has matched on a memory dump for (process #2) msbuild.exe.			
5/5	_data_collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Flock, FTP Navigator, Internet Download Manager, Mozilla Thunderbird, Opera Mail, FileZilla, Ipsw... ...er, SeaMonkey, Comodo IceDragon, Postbox, Opera, OpenVPN, CoreFTP, k-Meleon, Mozilla Firefox, Cyberfox, WinSCP, Microsoft Outlook.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) 22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe modifies memory of (process #2) msbuild.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #1) 22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe alters context of (process #2) msbuild.exe.			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
2/5	Defense Evasion	Sends control codes to connected devices	3	-
	• (Process #4) wmiprvse.exe controls device "\\.\{9E8A7ED5-49C8-421B-A782-D46C28931105}" through API DeviceIOControl. • (Process #4) wmiprvse.exe controls device "\\.\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}" through API DeviceIOControl. • (Process #4) wmiprvse.exe controls device "\\.\{E96D977E-F067-4CE9-924D-F6E0A04729E4}" through API DeviceIOControl.			
2/5	_data_collection	Reads sensitive browser data	9	-
	• (Process #2) msbuild.exe tries to read sensitive data of web browser "Opera" by file. • (Process #2) msbuild.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault. • (Process #2) msbuild.exe tries to read sensitive data of web browser "BlackHawk" by file. • (Process #2) msbuild.exe tries to read sensitive data of web browser "k-Meleon" by file. • (Process #2) msbuild.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #2) msbuild.exe tries to read sensitive data of web browser "Flock" by file. • (Process #2) msbuild.exe tries to read sensitive data of web browser "Comodo IceDragon" by file. • (Process #2) msbuild.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #2) msbuild.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	_data_collection	Reads sensitive application data	6	-
	• (Process #2) msbuild.exe tries to read sensitive data of application "Internet Download Manager" by registry. • (Process #2) msbuild.exe tries to read sensitive data of application "SeaMonkey" by file. • (Process #2) msbuild.exe tries to read sensitive data of application "OpenVPN" by registry. • (Process #2) msbuild.exe tries to read sensitive data of application "TightVNC" by registry. • (Process #2) msbuild.exe tries to read sensitive data of application "TigerVNC" by registry. • (Process #2) msbuild.exe tries to read sensitive data of application "WinSCP" by registry.			
2/5	_data_collection	Reads sensitive mail data	7	-

Score	Category	Operation	Count	Classification
	• (Process #2) msbuild.exe tries to read sensitive data of mail application "The Bat!" by file. • (Process #2) msbuild.exe tries to read sensitive data of mail application "Postbox" by file. • (Process #2) msbuild.exe tries to read sensitive data of mail application "Pocomail" by file. • (Process #2) msbuild.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file. • (Process #2) msbuild.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry. • (Process #2) msbuild.exe tries to read sensitive data of mail application "Opera Mail" by file. • (Process #2) msbuild.exe tries to read sensitive data of mail application "IncrediMail" by registry.			
2/5	_data_collection	Reads sensitive ftp data	4	-
	• (Process #2) msbuild.exe tries to read sensitive data of ftp application "CoreFTP" by registry. • (Process #2) msbuild.exe tries to read sensitive data of ftp application "Ipswitch WS_FTP" by file. • (Process #2) msbuild.exe tries to read sensitive data of ftp application "FTP Navigator" by file. • (Process #2) msbuild.exe tries to read sensitive data of ftp application "FileZilla" by file.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #2) msbuild.exe queries OS version via WMI.			
2/5	Discovery	Executes WMI query	2	-
	• (Process #2) msbuild.exe executes WMI query: select * from Win32_OperatingSystem. • (Process #2) msbuild.exe executes WMI query: SELECT * FROM Win32_Processor.			
2/5	Discovery	Collects hardware properties	1	-
	• (Process #2) msbuild.exe queries hardware properties via WMI.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) 22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe starts (process #1) 22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe reads from (process #1) 22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.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) msbuild.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Possibly does reconnaissance	22	-

Score	Category	Operation	Count	Classification
	• (Process #2) msbuild.exe tries to gather information about application "The Bat!" by file. • (Process #2) msbuild.exe tries to gather information about application "Postbox" by file. • (Process #2) msbuild.exe tries to gather information about application "blackHawk" by file. • (Process #2) msbuild.exe tries to gather information about application "Foxmail" by registry. • (Process #2) msbuild.exe tries to gather information about application "SeaMonkey" by file. • (Process #2) msbuild.exe tries to gather information about application "k-Meleon" by file. • (Process #2) msbuild.exe tries to gather information about application "Cyberfox" by file. • (Process #2) msbuild.exe tries to gather information about application "Flock" by file. • (Process #2) msbuild.exe tries to gather information about application "WS_FTP" by file. • (Process #2) msbuild.exe tries to gather information about application "Pocomail" by file. • (Process #2) msbuild.exe tries to gather information about application "Comodo IceDragon" by file. • (Process #2) msbuild.exe tries to gather information about application "FlashFXP" by file. • (Process #2) msbuild.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #2) msbuild.exe tries to gather information about application "Qualcomm Eudora" by registry. • (Process #2) msbuild.exe tries to gather information about application "RealVNC" by registry. • (Process #2) msbuild.exe tries to gather information about application "TightVNC" by registry. • (Process #2) msbuild.exe tries to gather information about application "TigerVNC" by registry. • (Process #2) msbuild.exe tries to gather information about application "icecat" by file. • (Process #2) msbuild.exe tries to gather information about application "FTP Navigator" by file. • (Process #2) msbuild.exe tries to gather information about application "Opera Mail" by file. • (Process #2) msbuild.exe tries to gather information about application "WinSCP" by registry. • (Process #2) msbuild.exe tries to gather information about application "FileZilla" by file.		
1/5	Network Connection	Performs DNS request	1	-
	• (Process #2) msbuild.exe resolves host name "webmail.keeprojects.in" to IP "103.195.185.58".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #2) msbuild.exe opens an outgoing TCP connection to host "103.195.185.58:587".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #2) msbuild.exe tries to connect to TCP port 587 at 103.195.185.58.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #2) msbuild.exe resolves 50 API functions by name.			

Malware Configuration: AgentTesla

Metadata	Key	Extracted Value
Email Address	Tags Value Tags Value	Sender quality@keeprojects.in Recipient uuc7470@gmail.com
URL	Url Tags Username Password	webmail.keeprojects.in SMTP Server quality@keeprojects.in quality#@!
Encryption Key	Key Algorithm	qg== XOR

Mitre ATT&CK Matrix

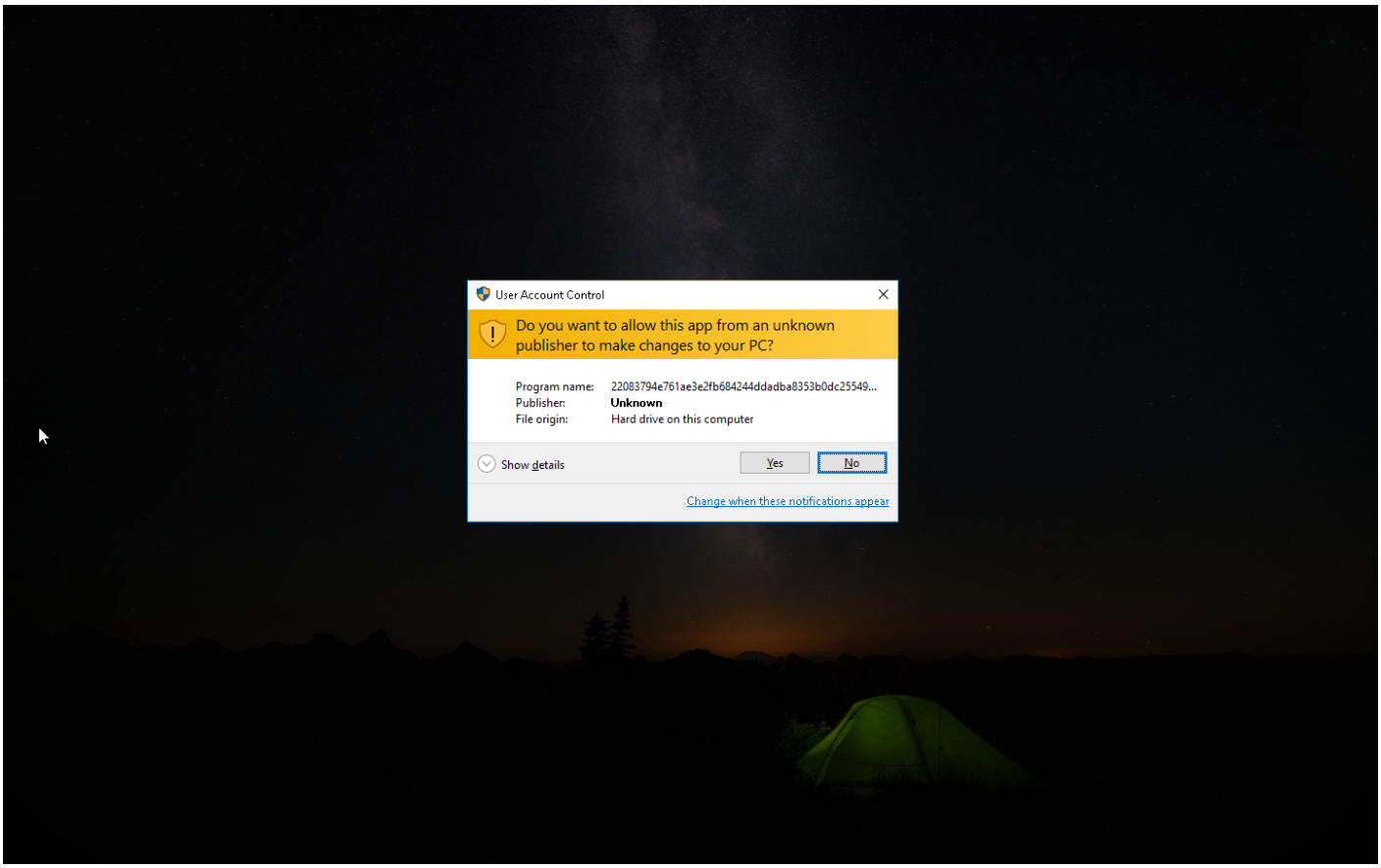
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#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					

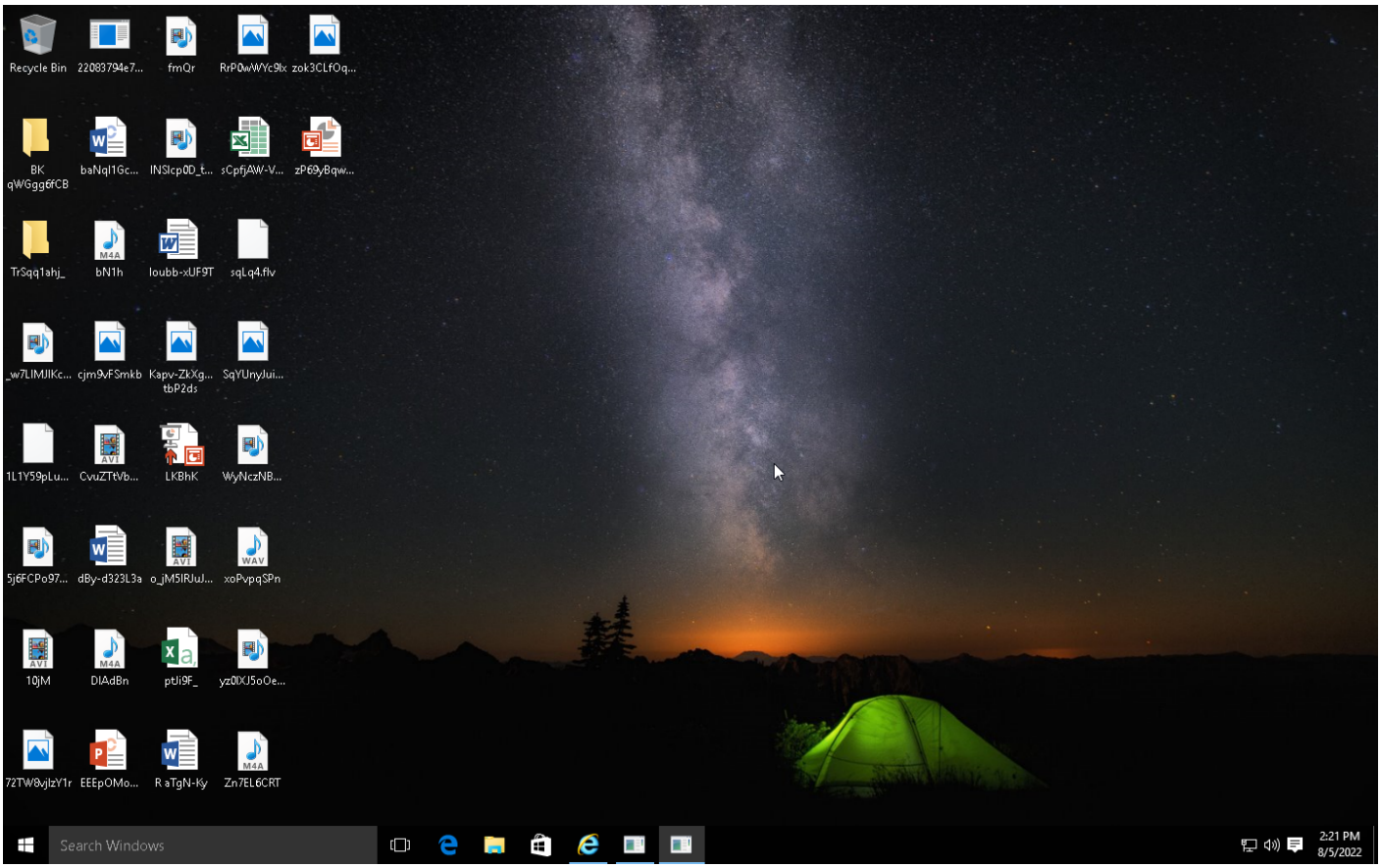
Sample Information

ID	#5068102
MD5	9c8721d5f0dfcb5893766810fc016b1b
SHA1	097e2d6bd75f55fee4ba991696d15bbd0f73137f
SHA256	22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054
SSDeep	12288:OxjlkBlh6kLw/997uWi+bLtVo80FuYAMrovCSePuv:AsiAJJb3o8zsIh
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe
File Size	825.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 16:20 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	1


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 22083794e761ae3e2fb684244ddadba8353b0dc25549...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
22083794e7...
fmQr
RrP0wWYc9lx
zok3CLfOq...
BK qWGgg6fCB
baNq1Gc...
INSlcp0D_t...
sCpfjAW-V...
zP69yBqw...
TrSqq1ahj_
bN1h
loubb-xUF9T
sqLq4.flv
_w7LIMJIKc...
cjm9vFSmkb
Kapv-ZkXg...
tbP2ds
SqYUnyJui...
1L1Y59pLu...
CvuZTtVb...
LKBhK
WyNczNB...
5j6FCPo97...
dBy-d323L3a
o_jM5IRJuJ...
xoPvpqSPn
10jM
DlAdBn
ptJi9F_
yz0KJ5oOe...
72TW8vjlzY1r
EEEpOMo...
R aTgN-Ky
Zn7EL6CRT
Search Windows
2:21 PM
8/5/2022

NETWORK

General

1.41 KB total sent

1.34 KB total received

2 ports 587, 53

2 contacted IP addresses

1 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	webmail.keeprojects.in	NO_ERROR	103.195.185.58		NA

BEHAVIOR

Process Graph

Process #1: 22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 66361, Reason: Analysis Target
Unmonitor End Time	End Time: 141740, Reason: Terminated
Monitor duration	75.38s
Return Code	0
PID	5012
Parent PID	1972
Bitness	32 Bit

Host Behavior

Type	Count
Module	72
Window	6
Registry	4
File	19
Process	1
-	3
-	7

Process #2: msbuild.exe

ID	2
File Name	c:\windows\microsoft.net\framework\v4.0.30319\msbuild.exe
Command Line	"{path}"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 138976, Reason: Child Process
Unmonitor End Time	End Time: 306465, Reason: Terminated by timeout
Monitor duration	167.49s
Return Code	Unknown
PID	2044
Parent PID	5012
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\22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe	0x1398	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe	0x1398	0x402000(4202496)	0x33c00	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe	0x1398	0x436000(4415488)	0x600	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe	0x1398	0x438000(4423680)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe	0x1398	0x228008(2261000)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe	0x1398 / 0xc7c	0x435bee(4414446)	-	✔	1

Host Behavior

Type	Count
-	22
Registry	98
File	142
User	4
Module	63
System	33
COM	34
Environment	23

Type	Count
-	2
Mutex	2
-	1
Window	3

Network Behavior

Type	Count
DNS	1
TCP	1

Process #3: svchost.exe

ID	3
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 151726, Reason: RPC Server
Unmonitor End Time	End Time: 306465, Reason: Terminated by timeout
Monitor duration	154.74s
Return Code	Unknown
PID	864
Parent PID	2044
Bitness	64 Bit

Process #4: wmiprvse.exe

ID	4
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 151726, Reason: RPC Server
Unmonitor End Time	End Time: 306465, Reason: Terminated by timeout
Monitor duration	154.74s
Return Code	Unknown
PID	4208
Parent PID	864
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Registry	4
Module	20
File	5
-	6

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054	C:\Users\RDhJ0CNFevzX\Desktop\22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe	Sample File	825.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe	Sample File, VM File	-	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\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\Local\Elements Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files (x86)\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Trillian\users\global\accounts.dat	Accessed File	Access	CLEAN
\\.\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}	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\Psi\profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\ProgramData\FlashFXP\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Claws-mail	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\profiles.ini	Accessed File	Access	CLEAN
C:\Program Files\Private Internet Access\data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\uvnc bvba\UltraVNC\ultravnc.ini	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Psi+\profiles	Accessed File	Access	CLEAN
C:\Private Internet Access\data	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe.Config	Accessed File	Access, Read	CLEAN
\\.\{E25A642B-6CEB-4194-8F83-8BC82AF94F5A}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Mail\Opera Mail\wand.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Credentials\	Accessed File	Access	CLEAN
\\.\{E96D977E-F067-4CE9-924D-F6E0A04729E4}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\NordVPN	Accessed File	Access	CLEAN
C:\Program Files (x86)\jDownloader\config\database.script	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Folder.lst	Accessed File	Access	CLEAN
\\.\{9E8A7ED5-49C8-421B-A782-D46C28931105}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
C:\Storage\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FTPGetter\servers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FlashFXP\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Waterfox\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\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHawk\profiles.ini	Accessed File	Access	CLEAN
C:\cftp\Ftplist.txt	Accessed File	Access	CLEAN
C:\FTP Navigator\Ftplist.txt	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\icecat\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data	Accessed File	Access	CLEAN
\\.\{017EF944-8C88-42C3-8F92-C8F7B6022F8D}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Mailbird\Store\Store.db	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Postbox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Flock\Browser\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\The Bat!	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\plutil.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\UltraVNC\ultravnc.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Comodo\IceDragon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Claws-mail\clawsrc	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data	Accessed File	Access	CLEAN
C:\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Pocomail\accounts.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Protect\S-1-5-21-1560258661-3990802383-1811730007-1000\1c1d304f-aa8f-4534-b2cb-33b61c83ed15	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\falkon\profiles\profiles.ini	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\eM Client	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://webmail.keeprojects.in	-	103.195.185.58	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
webmail.keeprojects.in	103.195.185.58	-	TCP, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
103.195.185.58	webmail.keeprojects.in	India	TCP, DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
-	delete, access	msbuild.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\DownloadManager\Passwords	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TightVNC\Server	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TigerVNC\Server	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\vncserver	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\TigerVNC\Server	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\FoxmailPreview	access	msbuild.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	msbuild.exe, 22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\vncserver	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	msbuild.exe, 22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\ORL\WinVNC3	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\WinVNC4	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Qualcomm\Eudora\CommandLine	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\FTPWare\COREFTP\Sites	access	msbuild.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\TightVNC\Server	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	msbuild.exe, 22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	msbuild.exe, 22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\OpenVPN-GUI\configs	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\RimArts\B2\Settings	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	msbuild.exe	CLEAN

Process

Process Name	Commandline	Verdict
22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe	"C:\Users\RDhJ0CNFevzX\Desktop\22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054.exe"	MALICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
msbuild.exe	"{path}"	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	AgentTesla_StringDecryption_v3	Agent Tesla v3 string decryption	Memory Dump	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.14 / 2022-08-03 12:19:21
YARA Built-in Ruleset Version	4.6.1.10

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	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