MALICIOUS

Classifications: Exploit | Dropper | Downloader | Spyware

Threat Names: Lokibot | Mal/Generic-S | C2/Generic-A

Verdict Reason: -

Sample Type	**Excel Document**
File Name	**_2201S_BUSAN_HOCHIMINH_.xlsx**
ID	#3468448
MD5	cf8b307caa943326ee808bb3cb02deee
SHA1	705c25adbdb7b805e47566540b3804eba178e7da
SHA256	cbe84e2c523fd51dabb1365df50415ffc51f8159c36798061742f08ba5d31b9b
File Size	187.24 KB
Report Created	2022-02-10 08:45 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (29 rules, 71 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	3	Spyware
	• Rule "Lokibot" from ruleset "Malware" has matched on a memory dump for (process #7) xmtxpy.exe. • Rule "Lokibot" from ruleset "Malware" has matched on a memory dump for (process #6) xmtxpy.exe. • Rule "Lokibot" from ruleset "Malware" has matched on the function strings for (process #7) xmtxpy.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Opera Mail, KiTTY, FileZilla, Trojita, Internet Explorer, SecureFX, IncrediMail, QtWeb Internet B... ...Commander, LinasFTP, NCH Classic FTP, WinChips, BlazeFTP, PuTTY, FAR Manager, NCH Fling, Microsoft Outlook, FTP Navigator, Pidgin.			
4/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #6) xmtxpy.exe reads from (process #7) xmtxpy.exe.			
4/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
4/5	Defense Evasion	Document is encrypted with default password	1	-
	• _2201S_BUSAN_HOCHIMINH_.xlsx is encrypted with the default "VelvetSweatshop" password.			
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S". • Reputation analysis labels a file which was only downloaded to memory as "Mal/Generic-S".			
4/5	Reputation	Contacts known malicious URL	1	-
	• Reputation analysis labels the URL "http://asiaoil.bar//bobby/five/fre.php" which was contacted by (process #7) xmtxpy.exe as "C2/Generic-A".			
4/5	Exploit	Possible exploitation attempt	1	Exploit
	• Office document may try to exploit a common vulnerability or exposure (CVE): CVE-2018-0798.			
4/5	Network Connection	Performs DNS request	2	-
	• (Process #7) xmtxpy.exe resolves host name "asiaoil.bar" to IP "104.21.49.244". • (Process #7) xmtxpy.exe resolves host name "[illegible]" to IP "-".			
4/5	Network Connection	Connects to remote host	1	-
	• (Process #7) xmtxpy.exe opens an outgoing TCP connection to host "104.21.49.244:80".			
4/5	Network Connection	Downloads file	1	Downloader
	• (Process #7) xmtxpy.exe downloads file via http from http://asiaoil.bar//bobby/five/fre.php.			
4/5	Network Connection	Downloads executable	1	Downloader
	• (Process #2) eqnedt32.exe downloads executable via http from http://198.46.132.195/windowSSH/.win32.exe.			
4/5	Network Connection	Attempts to connect through HTTP	2	-

Score	Category	Operation	Count	Classification
	• (Process #2) eqnedt32.exe connects to "http://198.46.132.195/windowSSH/.win32.exe". • (Process #7) xmtxpy.exe failed to connect to "http://asiaoil.bar//bobby/five/fre.php".			
4/5	Execution	Document tries to create process	1	-
	• Document creates (process #4) vbc.exe.			
4/5	Execution	Executes dropped PE file	1	Dropper
	• Executes dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\xmtxpy.exe".			
4/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #6) xmtxpy.exe alters context of (process #7) xmtxpy.exe.			
3/5	Discovery	Reads system data	1	-
	• (Process #7) xmtxpy.exe reads the cryptographic machine GUID from registry.			
3/5	Anti Analysis	Delays execution	1	-
	• (Process #7) xmtxpy.exe has a thread which sleeps more than 5 minutes.			
3/5	YARA	Suspicious content matched by YARA rules	4	-
	• Rule "Shellcode_Find_kernel32_PEB" from ruleset "Generic" has matched on the dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\xmtxpy.exe". • Rule "Shellcode_Find_kernel32_PEB" from ruleset "Generic" has matched on the dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\nsu2FBB.tmp". • Rule "Shellcode_Find_kernel32_PEB" from ruleset "Generic" has matched on a memory dump for (process #6) xmtxpy.exe. • Rule "Shellcode_Find_kernel32_PEB" from ruleset "Generic" has matched on a memory dump for (process #7) xmtxpy.exe.			
3/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	2	-
	• (Process #6) xmtxpy.exe makes a direct system call to "NtWriteVirtualMemory". • (Process #6) xmtxpy.exe makes a direct system call to "NtResumeThread".			
2/5	Discovery	Possibly does reconnaissance	14	-
	• (Process #7) xmtxpy.exe tries to gather information about application "Mozilla Firefox" by registry. • (Process #7) xmtxpy.exe tries to gather information about application "Comodo IceDragon" by registry. • (Process #7) xmtxpy.exe tries to gather information about application "Safari" by registry. • (Process #7) xmtxpy.exe tries to gather information about application "K-Meleon" by registry. • (Process #7) xmtxpy.exe tries to gather information about application "Mozilla SeaMonkey" by registry. • (Process #7) xmtxpy.exe tries to gather information about application "Mozilla Flock" by registry. • (Process #7) xmtxpy.exe tries to gather information about application "Cyberfox" by registry. • (Process #7) xmtxpy.exe tries to gather information about application "Total Commander" by registry. • (Process #7) xmtxpy.exe tries to gather information about application "NetScape" by registry. • (Process #7) xmtxpy.exe tries to gather information about application "Default Programs" by registry. • (Process #7) xmtxpy.exe tries to gather information about application "Bitvise SSH Client" by registry. • (Process #7) xmtxpy.exe tries to gather information about application "SecureFX" by registry. • (Process #7) xmtxpy.exe tries to gather information about application "Postbox" by registry. • (Process #7) xmtxpy.exe tries to gather information about application "Trojita" by registry.			
2/5	Data Collection	Reads sensitive browser data	3	-
	• (Process #7) xmtxpy.exe tries to read sensitive data of web browser "QtWeb Internet Browser" by registry. • (Process #7) xmtxpy.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault. • (Process #7) xmtxpy.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by registry.			

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

- (Process #7) xmtxpy.exe tries to read sensitive data of application "Pidgin" by file.
- (Process #7) xmtxpy.exe tries to read sensitive data of application "Bitvise SSH Client" by registry.
- (Process #7) xmtxpy.exe tries to read sensitive data of application "KiTTY" by registry.
- (Process #7) xmtxpy.exe tries to read sensitive data of application "PuTTY" by registry.
- (Process #7) xmtxpy.exe tries to read sensitive data of application "WinChips" by registry.

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive ftp data	10	-

- (Process #7) xmtxpy.exe tries to read sensitive data of ftp application "LinasFTP" by registry.
- (Process #7) xmtxpy.exe tries to read sensitive data of ftp application "FileZilla" by file.
- (Process #7) xmtxpy.exe tries to read sensitive data of ftp application "BlazeFTP" by file.
- (Process #7) xmtxpy.exe tries to read sensitive data of ftp application "BlazeFTP" by registry.
- (Process #7) xmtxpy.exe tries to read sensitive data of ftp application "Total Commander" by registry.
- (Process #7) xmtxpy.exe tries to read sensitive data of ftp application "FAR Manager" by registry.
- (Process #7) xmtxpy.exe tries to read sensitive data of ftp application "SecureFX" by registry.
- (Process #7) xmtxpy.exe tries to read sensitive data of ftp application "NCH Fling" by registry.
- (Process #7) xmtxpy.exe tries to read sensitive data of ftp application "NCH Classic FTP" by registry.
- (Process #7) xmtxpy.exe tries to read sensitive data of ftp application "FTP Navigator" by file.

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

- (Process #7) xmtxpy.exe tries to read sensitive data of mail application "Pocomail" by file.
- (Process #7) xmtxpy.exe tries to read sensitive data of mail application "IncrediMail" by registry.
- (Process #7) xmtxpy.exe tries to read sensitive data of mail application "Opera Mail" by file.
- (Process #7) xmtxpy.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.
- (Process #7) xmtxpy.exe tries to read sensitive data of mail application "Trojita" by registry.

Score	Category	Operation	Count	Classification
2/5	Heuristics	Contains known suspicious class identifier	1	-

- Office document contains suspicious class identifier for ActiveX object "Equation2" (CLSID {0002CE02-0000-0000-C000-000000000046}).

Score	Category	Operation	Count	Classification
2/5	Execution	Drops PE file	1	-

- (Process #4) vbc.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\xmtxpy.exe".

Score	Category	Operation	Count	Classification
1/5	Mutex	Creates mutex	1	-

- (Process #7) xmtxpy.exe creates mutex with name "B7274519EDDE9BDC8AE51348".

Score	Category	Operation	Count	Classification
1/5	Heuristics	Contains suspicious meta data	2	-

- Office document was created using a pirated version of Microsoft Office.
- Office document contains below average content data.

Score	Category	Operation	Count	Classification
-	Trusted	Known clean file	2	-

- File "C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.lck" is a known clean file.
- File "c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778" is a known clean file.

Mitre ATT&CK Matrix

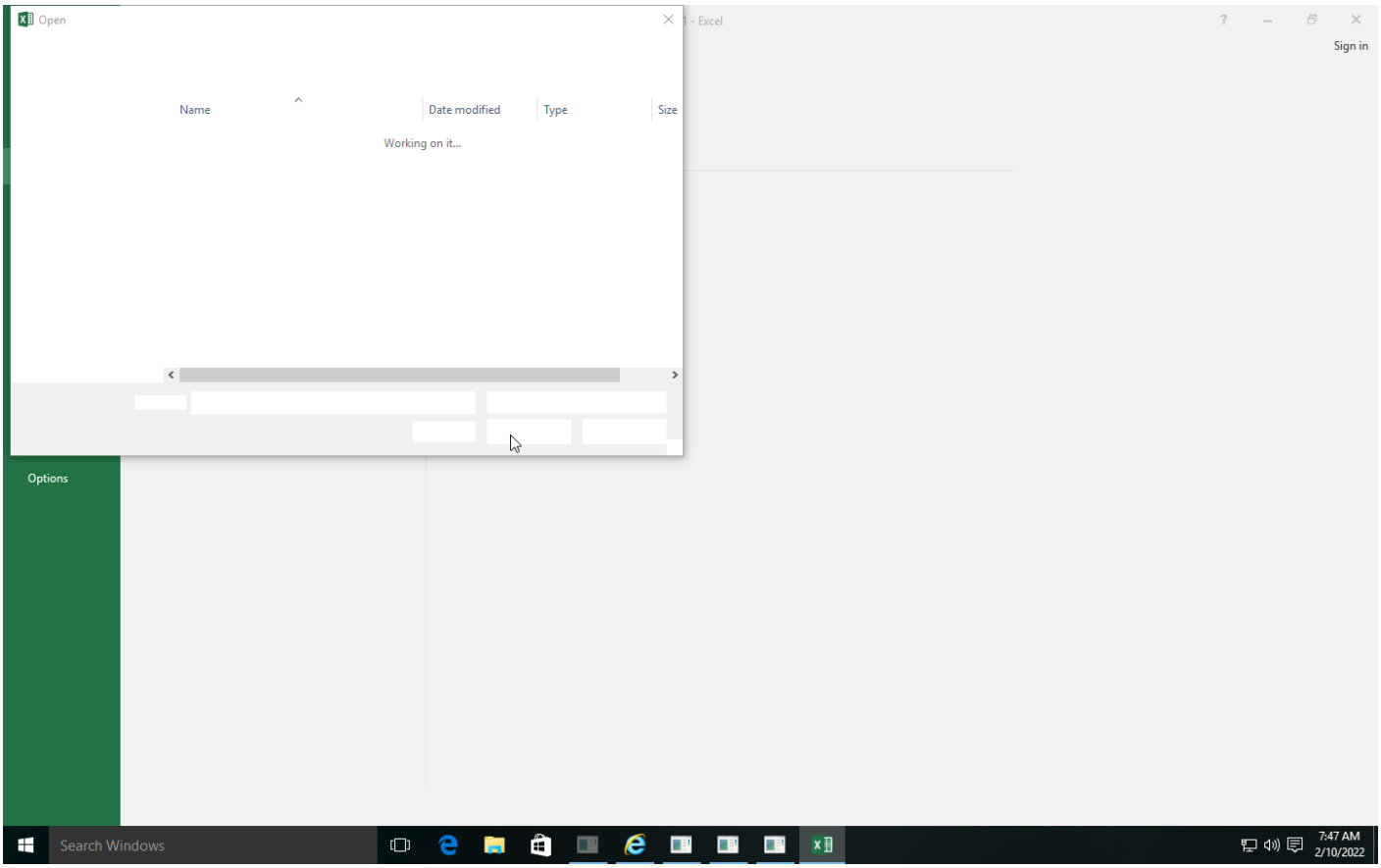
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1203 Exploitation for Client Execution			#T1027 Obfuscated Files or Information	#T1214 Credentials in Registry	#T1082 System Information Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol		
					#T1003 Credential Dumping	#T1012 Query Registry		#T1005 Data from Local System	#T1105 Remote File Copy		
					#T1081 Credentials in Files	#T1217 Browser Bookmark Discovery					
						#T1083 File and Directory Discovery					

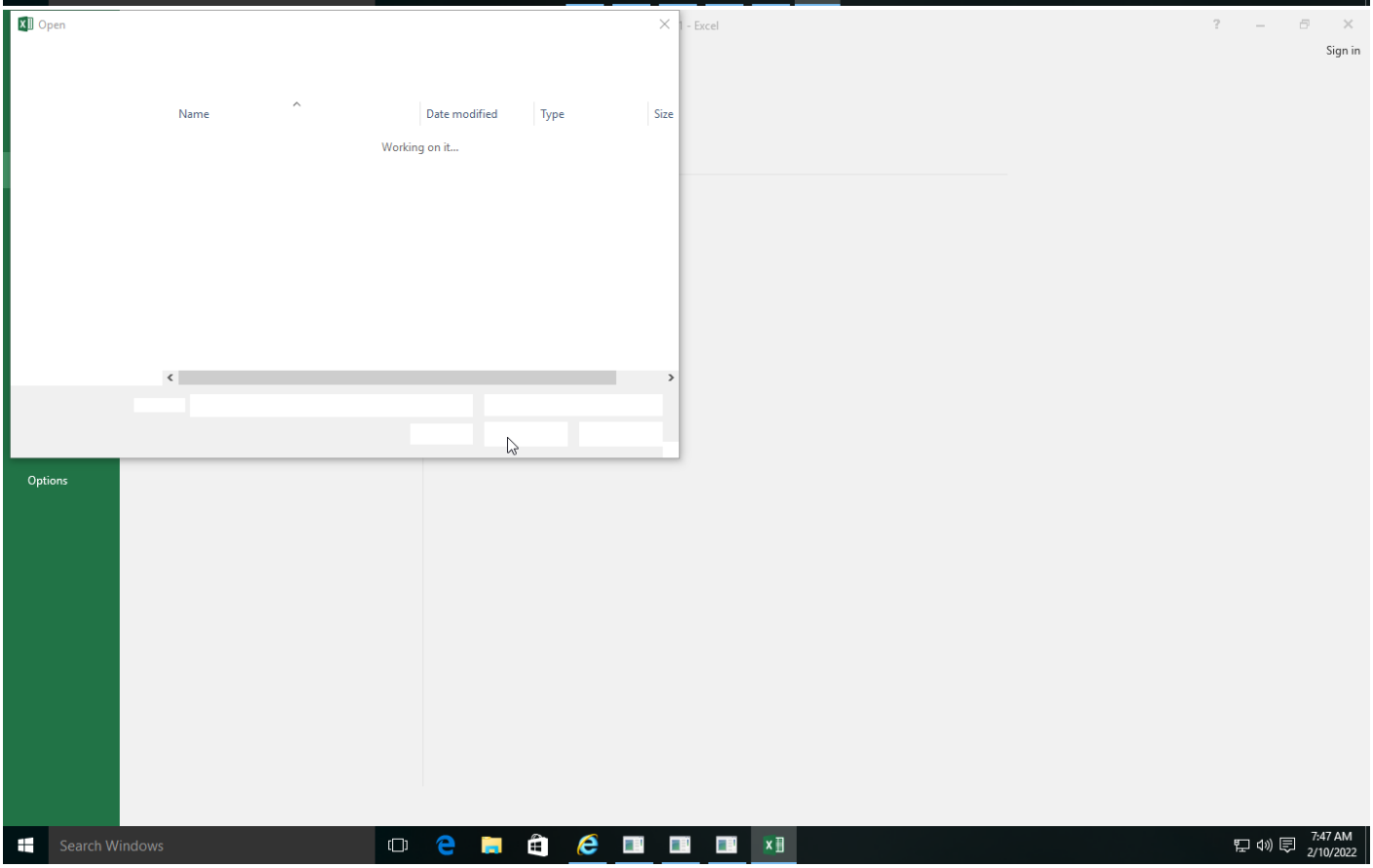
Sample Information

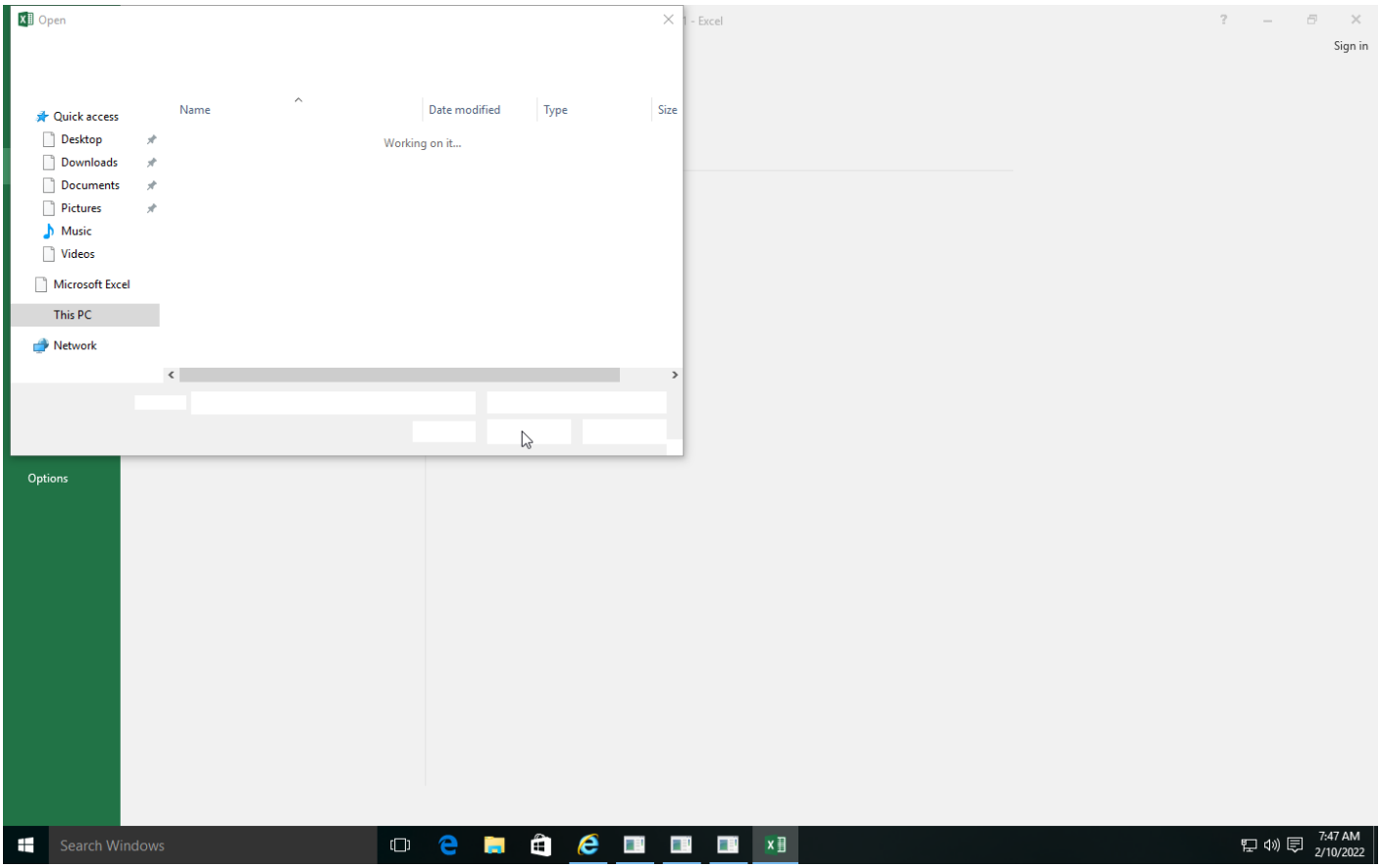
ID	#3468448
MD5	cf8b307caa943326ee808bb3cb02deee
SHA1	705c25adbdb7b805e47566540b3804eba178e7da
SHA256	cbe84e2c523fd51dabb1365df50415ffc51f8159c36798061742f08ba5d31b9b
SSDeep	3072:W3x5yiKm7/AJj6GEOux8NBVuVnDcq3QT0PyYC9v1EFVW3NdR31od+xXfwsRYXn0D:uam7/AJ6GsWBVuV4MaB9voVWdT3iWPws
File Name	_2201S_BUSAN_HOCHIMINH_.xlsx
File Size	187.24 KB
Sample Type	Excel Document
Has Macros	✓

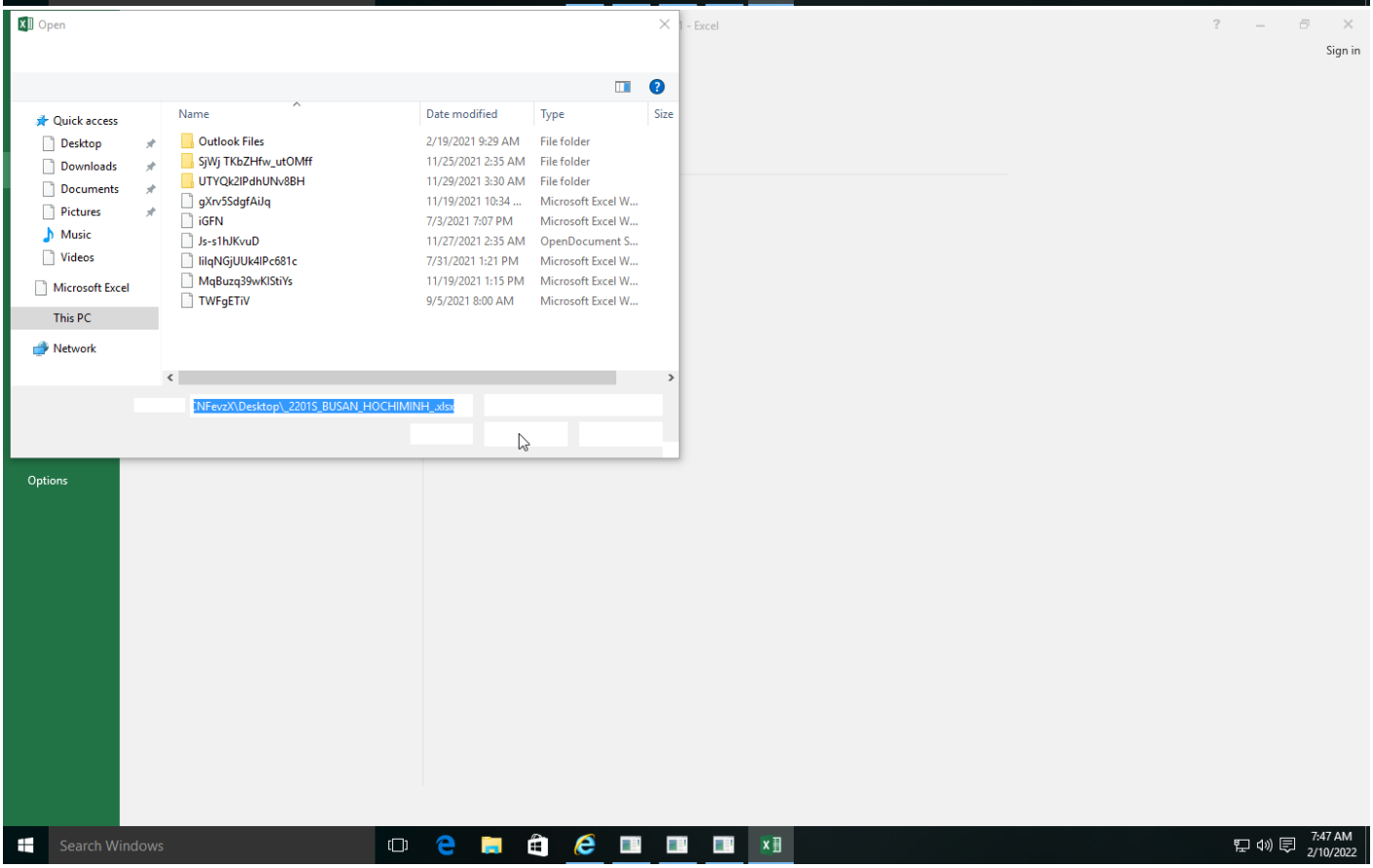
Analysis Information

Creation Time	2022-02-10 08:45 (UTC+1)
Analysis Duration	00:03:29
Termination Reason	Timeout
Number of Monitored Processes	6
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	30


Open
Name
Date modified
Type
Size
Working on it...
- Excel
Sign in
Options
Search Windows
7:47 AM
2/10/2022


Open
Name
Date modified
Type
Size
Working on it...
- Excel
Sign in
Options
Search Windows
7:47 AM
2/10/2022





Screenshots truncated

NETWORK

General

35.24 KB total sent

345.00 KB total received

1 ports 80

3 contacted IP addresses

0 URLs extracted

5 files downloaded

0 malicious hosts detected

DNS

120 DNS requests for 2 domains

1 nameservers contacted

59 total requests returned errors

HTTP/S

2 URLs contacted, 2 servers

62 sessions, 35.24 KB sent, 345.00 KB received

HTTP Requests

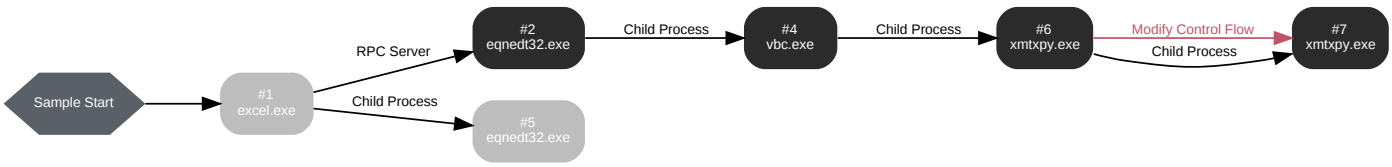
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://198.46.132.195/windowSSH/.win32.exe	-	-		0 bytes	NA
POST	http://asiaoil.bar//bobby/five/fre.php	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	asiaoil.bar	NoError	104.21.49.244, 172.67.197.66		NA
-	[illegible]	-			NA

BEHAVIOR

Process Graph



Process #1: excel.exe

ID	1
File Name	c:\program files (x86)\microsoft office\root\office16\excel.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 113996, Reason: Analysis Target
Unmonitor End Time	End Time: 323407, Reason: Terminated by Timeout
Monitor duration	209.41s
Return Code	Unknown
PID	5072
Parent PID	1560
Bitness	32 Bit

Process #2: eqnedt32.exe

ID	2
File Name	c:\program files (x86)\microsoft office\root\vfs\programfilescommonx86\microsoft shared\equation\eqnedt32.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Root\VFS\ProgramFilesCommonX86\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 150144, Reason: RPC Server
Unmonitor End Time	End Time: 169289, Reason: Terminated
Monitor duration	19.14s
Return Code	0
PID	4308
Parent PID	624
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	288.21 KB	9cbed5eff56e1c08b6040c8ab4977e76528d59368d9d0550626b5380513ecb7b	✖

Host Behavior

Type	Count
Module	6
File	1
Process	1

Network Behavior

Type	Count
HTTP	1
TCP	1

Process #4: vbc.exe

ID	4
File Name	c:\users\public\vbc.exe
Command Line	"C:\Users\Public\vbc.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 166406, Reason: Child Process
Unmonitor End Time	End Time: 235267, Reason: Terminated
Monitor duration	68.86s
Return Code	0
PID	1776
Parent PID	4308
Bitness	32 Bit

Dropped Files (5)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsr4335.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\2v0cucir72x	214.46 KB	2f62f941918151fced3ad854b37dcda1e40e91432d772781ebc2118e28987b41	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\npotbzd	4.74 KB	05fb79420aada2c2199cabad68f4d6483127d2d803a5fd4e755008e78a977931	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\xmtxpy.exe	122.50 KB	de398be02d5abe9c8bce84380ac5303ea00fc00820a50cad007220f24538b3de	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsu2FBB.tmp	346.55 KB	6b105fd88793034bdd4a7b6a45e7ec131c36c20d8faabc4b4aea557c905c73d5	✗

Host Behavior

Type	Count
Module	8
File	218
System	39
Process	1

Process #5: eqnedt32.exe

ID	5
File Name	c:\program files (x86)\microsoft office\root\vfs\programfilescommonx86\microsoft shared\equation\eqnedt32.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesCommonX86\Microsoft Shared\EQUATION\eqnedt32.exe" -Embedding
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 168578, Reason: Child Process
Unmonitor End Time	End Time: 224616, Reason: Terminated
Monitor duration	56.04s
Return Code	0
PID	4260
Parent PID	5072
Bitness	32 Bit

Process #6: xmtxpy.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\xmtxpy.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\xmtxpy.exe C:\Users\RDHJ0C~1\AppData\Local\Temp\npotbzd
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 177858, Reason: Child Process
Unmonitor End Time	End Time: 232897, Reason: Terminated
Monitor duration	55.04s
Return Code	0
PID	4620
Parent PID	1776
Bitness	32 Bit

Host Behavior

Type	Count
Module	39
File	30
Environment	1
Process	1
-	3
-	8

Process #7: xmtxpy.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\xmtxpy.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\xmtxpy.exe C:\Users\RDHJ0C~1\AppData\Local\Temp\npotbzd
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 189759, Reason: Child Process
Unmonitor End Time	End Time: 323407, Reason: Terminated by Timeout
Monitor duration	133.65s
Return Code	Unknown
PID	4680
Parent PID	4620
Bitness	32 Bit

Injection Information (1)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\xmtxpy.exe	0x1210 / 0x125c	0x77c08fe0(2009108448)	-	✓	1

Dropped Files (5)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.exe	122.50 KB	de398be02d5abe9c8bce84380ac5303ea00fc00820a50cad007220f24538b3de	✗
-	53 bytes	e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	✗
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.hdb	4 bytes	859ffdca62ee0971821a4b2dedfc023d0f9a021391b5ac336ddb49d53d28330e	✗
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.lck	1 bytes	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b	✗
-	53 bytes	353fd628b7f6e7d426e5d6a27d1bc3ac22fa7f812e7594cf2ec5ca1175785b50	✗

Host Behavior

Type	Count
Module	2607
Registry	181
Mutex	1
File	304
System	87
User	9

Network Behavior

Type	Count
HTTP	61
DNS	120
TCP	61

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
de398be02d5abe9c8bce84380ac5303ea00fc00820a50cad007220f24538b3de	C:\Users\RDHJ0C~1\AppData\Local\Temp\xmtxpy.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.exe	Dropped File	122.50 KB	application/vnd.microsoft.portable-executable	Delete, Create, Write, Access	MALICIOUS
cbe84e2c523fd51dabb1365df50415ffc51f8159c36798061742f08ba5d31b9b	C:\Users\RDhJ0CNFevzX\Desktop_2201S_BUSAN_HOCHIMINH_.xlsx	Sample File	187.24 KB	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	-	MALICIOUS
9cbed5eff56e1c08b6040c8ab4977e76528d59368d9d0550626b5380513ecb7b	C:\Users\Public\vbc.exe	Downloaded File	288.21 KB	application/vnd.microsoft.portable-executable	Create, Read, Access	MALICIOUS
1ddf22074128c6541046c57222fa25eda04e10bdde8aede2df8a7926d59e7a23	oleObject1.bin	Embedded File	4.00 KB	application/CDFV2	-	MALICIOUS
6b105fd88793034bdd4a7b6a45e7ec131c36c20d8faabc4b4aea557c905c73d5	C:\Users\RDHJ0C~1\AppData\Local\Temp\nsu2FBB.tmp	Dropped File	346.55 KB	application/octet-stream	Create, Write, Read, Access	SUSPICIOUS
2f62f941918151fced3ad854b37dcda1e40e91432d772781ebc2118e28987b41	C:\Users\RDHJ0C~1\AppData\Local\Temp\2v0cucir72x	Dropped File	214.46 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
05fb79420aada2c2199cabad68f4d6483127d2d803a5fd4e755008e78a977931	C:\Users\RDHJ0C~1\AppData\Local\Temp\npotbzd	Dropped File	4.74 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	53 bytes	application/octet-stream	-	CLEAN
859ffdca62ee0971821a4b2dedfc023d0f9a021391b5ac336ddb49d53d28330e	C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.hdb	Dropped File	4 bytes	text/plain	Delete, Create, Write, Access	CLEAN
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b	C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.lck	Dropped File	1 bytes	application/octet-stream	Delete, Create, Write, Access	CLEAN
353fd628b7f6e7d426e5d6a27d1bc3ac22fa7f812e7594cf2ec5ca1175785b50	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	53 bytes	application/octet-stream	-	CLEAN
ec2c7040cc528e8384c37004c4c413a73233a6821d135d8eeb1ead6076d372cc	-	Downloaded File	288 bytes	application/octet-stream	-	CLEAN
095de8b22345a3703729f7e8ed1de0cffd328bdf6d323776faef2631daed7d1f	-	Downloaded File	186 bytes	application/octet-stream	-	CLEAN
9811b34e5885a16e5001187e9065a0886c709e028e2eff8a485374dcaf0bc6ed	-	Downloaded File	159 bytes	application/octet-stream	-	CLEAN
c64510503435c2143bad854faba7891308b4b089d140449ceb903620fea45d6a	-	Downloaded File	23 bytes	application/octet-stream	-	CLEAN
403eda0b532b8964e3240031906b9d10b0d2ffc3df7025b3c7a65a3d4e7a9f2b	Microsoft_Office_Word_Macro-Enabled_Document1.docm	Embedded File	57.91 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	-	CLEAN
7861ce5882eb2985e9144920e16e3d227d71d4c749acf9d57ed57274a750f5a9	image1.jpeg	Embedded File	47.33 KB	image/jpeg	-	CLEAN
338ef0cea9c9fbe583576b40f34a872167f28dd3d090b94eaf96e5765381f25f	-	Embedded File	1.50 KB	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b77a19a2f45cbee79da939f995dbd54905ded5cb31e7db6a6be40a7f6882f966	image1.png	Embedded File	2.58 KB	image/png	-	CLEAN
5cd7ea78de365089dddf47770cdecf82e1a6195c648f0db38d5dcac26b5c4fa5	image2.jpeg	Embedded File	4.29 KB	image/jpeg	-	CLEAN
e26f068512948bce56b02285018bb72f13eea9659b3d98acc8eebb79c42a9969	image3.png	Embedded File	5.27 KB	image/png	-	CLEAN
88a52f8a0bde5931db11729d197431148ee9223b2625d8016aef0b1a510eff4c	image4.png	Embedded File	11.04 KB	image/png	-	CLEAN
461babbdffdcc6f4cd3e3c2c97b50ddac4800b90ddba35f1e00e16c149a006fd	image5.png	Embedded File	9.96 KB	image/png	-	CLEAN
5dac97fdbd2c2d5dfdd60bf45f498bb6b218d8bfb97d0609738d5e250ebbb7e0	image6.png	Embedded File	3.66 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\Public\vbc.exe	Downloaded File	Create, Read, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsf2FAB.tmp	Accessed File	Delete, Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsu2FBB.tmp	Dropped File	Create, Write, Read, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsr4335.tmp	Accessed File	Delete, Create, 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\2v0cucir72x	Dropped File	Create, Write, Read, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\npotbzd	Dropped File	Create, Write, Read, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\xmtxpy.exe	Dropped File	Delete, Create, Write, Access	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Read, Access	CLEAN
C:\	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsr4335.tmp\	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.hdb	Dropped File	Delete, Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.lck	Dropped File	Delete, Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.exe	Dropped File	Create, Write, Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://asiaoil.bar//bobby/five/fre.php	-	104.21.49.244	-	POST	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://198.46.132.195/windowSSH/.win32.exe	-	198.46.132.195	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
asiaoil.bar	172.67.197.66, 104.21.49.244	-	DNS, HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
104.21.49.244	asiaoil.bar	-	DNS, HTTP, TCP	MALICIOUS
192.168.0.1	-	-	DNS, UDP	CLEAN
198.46.132.195	-	United States	HTTP, TCP	CLEAN
172.67.197.66	asiaoil.bar	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
B7274519EDDE9BDC8AE51348	access	xmtxpy.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\CurrentVersion	read, access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\ComodoGroup\IceDragon\Setup\SetupPath	read, access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Apple Computer, Inc.\Safari\InstallDir	read, access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\K-Meleon\CurrentVersion	read, access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\mozilla.org\SeaMonkey\CurrentVersion	read, access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\SeaMonkey\CurrentVersion	read, access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Flock\CurrentVersion	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\QtWeb.NET\QtWeb Internet Browser\AutoComplete	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2	access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\8pecxstudios\Cyberfox86\RootDir	read, access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\8pecxstudios\Cyberfox\Path	read, access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Pale Moon\CurrentVersion	read, access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Waterfox\CurrentVersion	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\LinasFTP\Site Manager	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\FlashPeak\BlazeFtp\Settings\LastPassword	read, access	xmtxpy.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Ghisler\Total Commander\FtpIniName	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\AppDataLow	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\IM Providers	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Netscape	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\ODBC	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\RegisteredApplications	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Wow6432Node	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Classes	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Far\Plugins\FTP\Hosts	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Far2\Plugins\FTP\Hosts	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Bitvise\BvSshClient\LastUsedProfile	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\VanDyke\SecureFX\Config Path	read, access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\NCH Software\Fling\Accounts	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\NCH Software\Fling\Accounts	access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\NCH Software\ClassicFTP\FTPAccounts	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\NCH Software\ClassicFTP\FTPAccounts	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\9bis.com\KiTTY\Sessions	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions	access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\SimonTatham\PuTTY\Sessions	access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\9bis.com\KiTTY\Sessions	access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Thunderbird\CurrentVersion	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\IncrediMail\Identities	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Martin Prikryl	access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Martin Prikryl	access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Postbox\Postbox\CurrentVersion	read, access	xmtxpy.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\FossaMail\CurrentVersion	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\WinChips\UserAccounts	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook	access	xmtxpy.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Email Address	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	xmtxpy.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User Name	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Server	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User Name	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Email Address	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP User Name	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Server	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Server	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User Name	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP User	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Server URL	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail User Name	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Server	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Port	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Port	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Port	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password2	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password2	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password2	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Password2	read, access	xmtxpy.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password2	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001	access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\Email	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\flaska.net\trojita\imap.auth.pass	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\flaska.net\trojita\msa.smtp.auth.pass	read, access	xmtxpy.exe	CLEAN
HKEY_CURRENT_USER\[illegible]\9EDDE9	write, access	xmtxpy.exe	CLEAN

Process

Process Name	Commandline	Verdict
vbc.exe	"C:\Users\Public\vbc.exe"	MALICIOUS
xmtxpy.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\xmtxpy.exe C:\Users\RDHJ0C~1\AppData\Local\Temp\npotbzd	MALICIOUS
eqnedt32.exe	"C:\Program Files (x86)\Microsoft Office\Root\VFS\ProgramFilesCommonX86\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding	SUSPICIOUS
excel.exe	"C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE"	CLEAN
eqnedt32.exe	"C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesCommonX86\Microsoft Shared\EQUATION\eqnedt32.exe" -Embedding	CLEAN

YARA / AV

YARA (30)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Function Strings	function_strings_process_7.txt	Spyware	5/5
Generic	Shellcode_Find_kernel32_PEB	x86 code to find kernel32.dll using the PEB; possible shellcode	Dropped File	C:\Users\RDHJ0C~1\AppData\Local\Temp\xmtxpy.exe	-	3/5
Generic	Shellcode_Find_kernel32_PEB	x86 code to find kernel32.dll using the PEB; possible shellcode	Dropped File	C:\Users\RDHJ0C~1\AppData\Local\Temp\nsu2FBB.tmp	-	3/5
Generic	Shellcode_Find_kernel32_PEB	x86 code to find kernel32.dll using the PEB; possible shellcode	Memory Dump	-	-	3/5
Generic	Shellcode_Find_kernel32_PEB	x86 code to find kernel32.dll using the PEB; possible shellcode	Memory Dump	-	-	3/5
Generic	Shellcode_Find_kernel32_PEB	x86 code to find kernel32.dll using the PEB; possible shellcode	Memory Dump	-	-	3/5

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	4.4.1
Dynamic Engine Version	4.4.1 / 01/14/2022 05:06
Static Engine Version	4.4.1.0 / 2022-01-14 04:00:58
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.1.6 / 2021-12-14 15:06:27
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.8 / 2022-01-07 14:24:33
YARA Built-in Ruleset Version	4.4.1.10

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