MALICIOUS

Classifications: Spyware | Exploit | Downloader

Threat Names: Lokibot | Mal/HTMLGen-A | Trojan.GenericKDZ.77897 | Trojan.GenericKDZ.77711 | Exploit.CVE-2018-0802.Gen | Generic.Andromeda.C7915F86 | Gen:Variant.Razy.762033

Verdict Reason: -

Sample Type	**Excel Document**
File Name	**09d2b8f86f136cb14832e9a4de582c239c698044adcc8d12d6195f5eff78ccab.xlsx**
ID	#968536
MD5	27eb25e6fbbbd37115055ecc4b557c53
SHA1	4c986607a941900d9d8804aa351dcab0cc4de224
SHA256	09d2b8f86f136cb14832e9a4de582c239c698044adcc8d12d6195f5eff78ccab
File Size	410.62 KB
Report Created	2021-09-28 09:23 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (26 rules, 65 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	2	Spyware
	• Rule "Lokibot" from ruleset "Malware" has matched on a memory dump for (process #3) vbc.exe. • Rule "Lokibot" from ruleset "Malware" has matched on the function strings for (process #3) vbc.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: SecureFX, NCH Fling, Total Commander, QtWeb Internet Browser, Internet Explorer / Edge, IncrediMa... ...vise SSH Client, Trojita, NCH Classic FTP, Microsoft Outlook, PuTTY, Pidgin, Internet Explorer, FAR Manager, Opera Mail, WinChips.			
4/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
4/5	Antivirus	Malicious content was detected by heuristic scan	5	-
	• Built-in AV detected a embedded file as "Trojan.GenericKDZ.77711". • Built-in AV detected a embedded file as "Exploit.CVE-2018-0802.Gen". • Built-in AV detected the sample itself as "Trojan.GenericKDZ.77897". • Built-in AV detected a memory dump of (process #3) vbc.exe as "Generic.Andromeda.C7915F86". • Built-in AV detected a memory dump of (process #3) vbc.exe as "Gen:Variant.Razy.762033".			
4/5	Execution	Document tries to create process	1	-
	• Document creates (process #3) vbc.exe.			
4/5	Reputation	Known malicious file	2	-
	• The sample itself is a known malicious file. • Embedded file "" is a known malicious file.			
4/5	Reputation	Contacts known malicious URL	1	-
	• Reputation analysis labels the URL "http://checkvim.com/ga14/fre.php" which was contacted by (process #3) vbc.exe as "Mal/HTMLGen-A".			
4/5	Reputation	Resolves known malicious domain	1	-
	• Reputation analysis labels the resolved domain "checkvim.com" as "Mal/HTMLGen-A".			
4/5	Defense Evasion	Document is encrypted with default password	1	-
	• 09d2b8f86f136cb14832e9a4de582c239c698044adcc8d12d6195f5eff78ccab.xlsx is encrypted with the default "VelvetSweatshop" password.			
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 #3) vbc.exe resolves host name "checkvim.com" to IP "5.188.89.50". • (Process #3) vbc.exe resolves host name "[illegible]" to IP "-".			
4/5	Network Connection	Connects to remote host	1	-

Score	Category	Operation	Count	Classification
	• (Process #3) vbc.exe opens an outgoing TCP connection to host "5.188.89.50:80".			
4/5	Network Connection	Downloads file	1	Downloader
	• (Process #3) vbc.exe downloads file via http from http://checkvim.com/ga14/fre.php.			
4/5	Network Connection	Downloads executable	1	Downloader
	• Downloads executable via http from http://103.155.83.184/wdc/vbc.exe.			
4/5	Network Connection	Attempts to connect through HTTP	1	-
	• (Process #3) vbc.exe failed to connect to "http://checkvim.com/ga14/fre.php".			
3/5	Discovery	Reads system data	1	-
	• (Process #3) vbc.exe reads the cryptographic machine GUID from registry.			
3/5	Anti Analysis	Delays execution	1	-
	• (Process #3) vbc.exe has a thread which sleeps more than 5 minutes.			
2/5	Discovery	Possibly does reconnaissance	14	-
	• (Process #3) vbc.exe tries to gather information about application "Mozilla Firefox" by registry. • (Process #3) vbc.exe tries to gather information about application "Comodo IceDragon" by registry. • (Process #3) vbc.exe tries to gather information about application "Safari" by registry. • (Process #3) vbc.exe tries to gather information about application "K-Meleon" by registry. • (Process #3) vbc.exe tries to gather information about application "Mozilla SeaMonkey" by registry. • (Process #3) vbc.exe tries to gather information about application "Mozilla Flock" by registry. • (Process #3) vbc.exe tries to gather information about application "Cyberfox" by registry. • (Process #3) vbc.exe tries to gather information about application "Total Commander" by registry. • (Process #3) vbc.exe tries to gather information about application "NetScape" by registry. • (Process #3) vbc.exe tries to gather information about application "Default Programs" by registry. • (Process #3) vbc.exe tries to gather information about application "Bitvise SSH Client" by registry. • (Process #3) vbc.exe tries to gather information about application "SecureFX" by registry. • (Process #3) vbc.exe tries to gather information about application "Postbox" by registry. • (Process #3) vbc.exe tries to gather information about application "Trojita" by registry.			
2/5	Data Collection	Reads sensitive browser data	3	-
	• (Process #3) vbc.exe tries to read sensitive data of web browser "QtWeb Internet Browser" by registry. • (Process #3) vbc.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault. • (Process #3) vbc.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by registry.			
2/5	Data Collection	Reads sensitive application data	5	-
	• (Process #3) vbc.exe tries to read sensitive data of application "Pidgin" by file. • (Process #3) vbc.exe tries to read sensitive data of application "Bitvise SSH Client" by registry. • (Process #3) vbc.exe tries to read sensitive data of application "KiTTY" by registry. • (Process #3) vbc.exe tries to read sensitive data of application "PuTTY" by registry. • (Process #3) vbc.exe tries to read sensitive data of application "WinChips" by registry.			
2/5	Data Collection	Reads sensitive ftp data	10	-

Score	Category	Operation	Count	Classification
		• (Process #3) vbc.exe tries to read sensitive data of ftp application "LinasFTP" by registry. • (Process #3) vbc.exe tries to read sensitive data of ftp application "FileZilla" by file. • (Process #3) vbc.exe tries to read sensitive data of ftp application "BlazeFTP" by file. • (Process #3) vbc.exe tries to read sensitive data of ftp application "BlazeFTP" by registry. • (Process #3) vbc.exe tries to read sensitive data of ftp application "Total Commander" by registry. • (Process #3) vbc.exe tries to read sensitive data of ftp application "FAR Manager" by registry. • (Process #3) vbc.exe tries to read sensitive data of ftp application "SecureFX" by registry. • (Process #3) vbc.exe tries to read sensitive data of ftp application "NCH Fling" by registry. • (Process #3) vbc.exe tries to read sensitive data of ftp application "NCH Classic FTP" by registry. • (Process #3) vbc.exe tries to read sensitive data of ftp application "FTP Navigator" by file.		
2/5	Data Collection	Reads sensitive mail data	5	-
		• (Process #3) vbc.exe tries to read sensitive data of mail application "Pocomail" by file. • (Process #3) vbc.exe tries to read sensitive data of mail application "IncrediMail" by registry. • (Process #3) vbc.exe tries to read sensitive data of mail application "Opera Mail" by file. • (Process #3) vbc.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry. • (Process #3) vbc.exe tries to read sensitive data of mail application "Trojita" by registry.		
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}).		
1/5	Mutex	Creates mutex	1	-
		• (Process #3) vbc.exe creates mutex with name "B7274519EDDE9BDC8AE51348".		
1/5	Obfuscation	Overwrites code	1	-
		• (Process #3) vbc.exe overwrites code to possibly hide behavior.		
1/5	Heuristics	Contains suspicious meta data	1	-
		• Office document contains below average content data.		
-	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

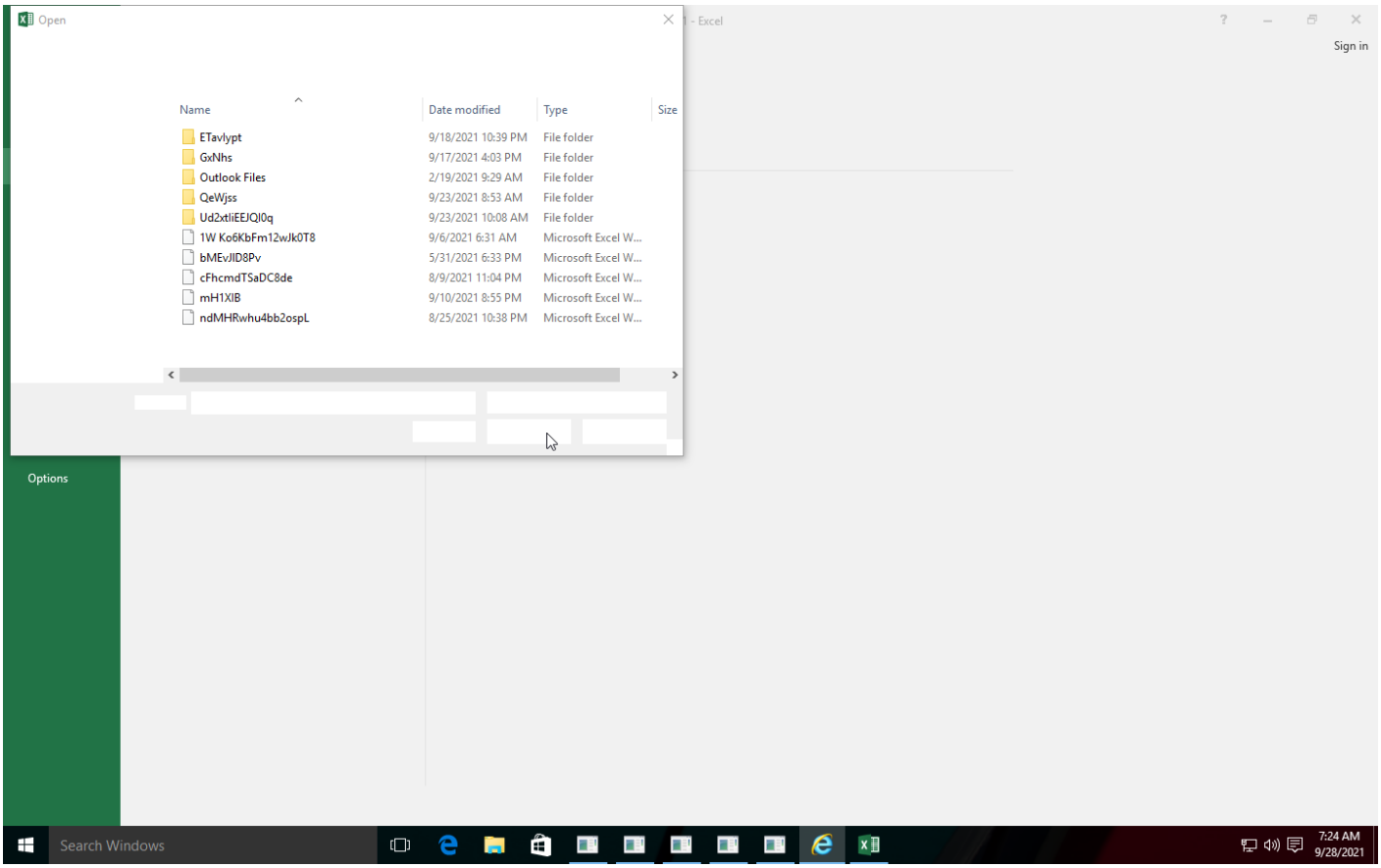
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1203 Exploitation for Client Execution			#T1027 Obfuscated Files or Information	#T1214 Credentials in Registry	#T1082 System Information Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol		
				#T1045 Software Packing	#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					

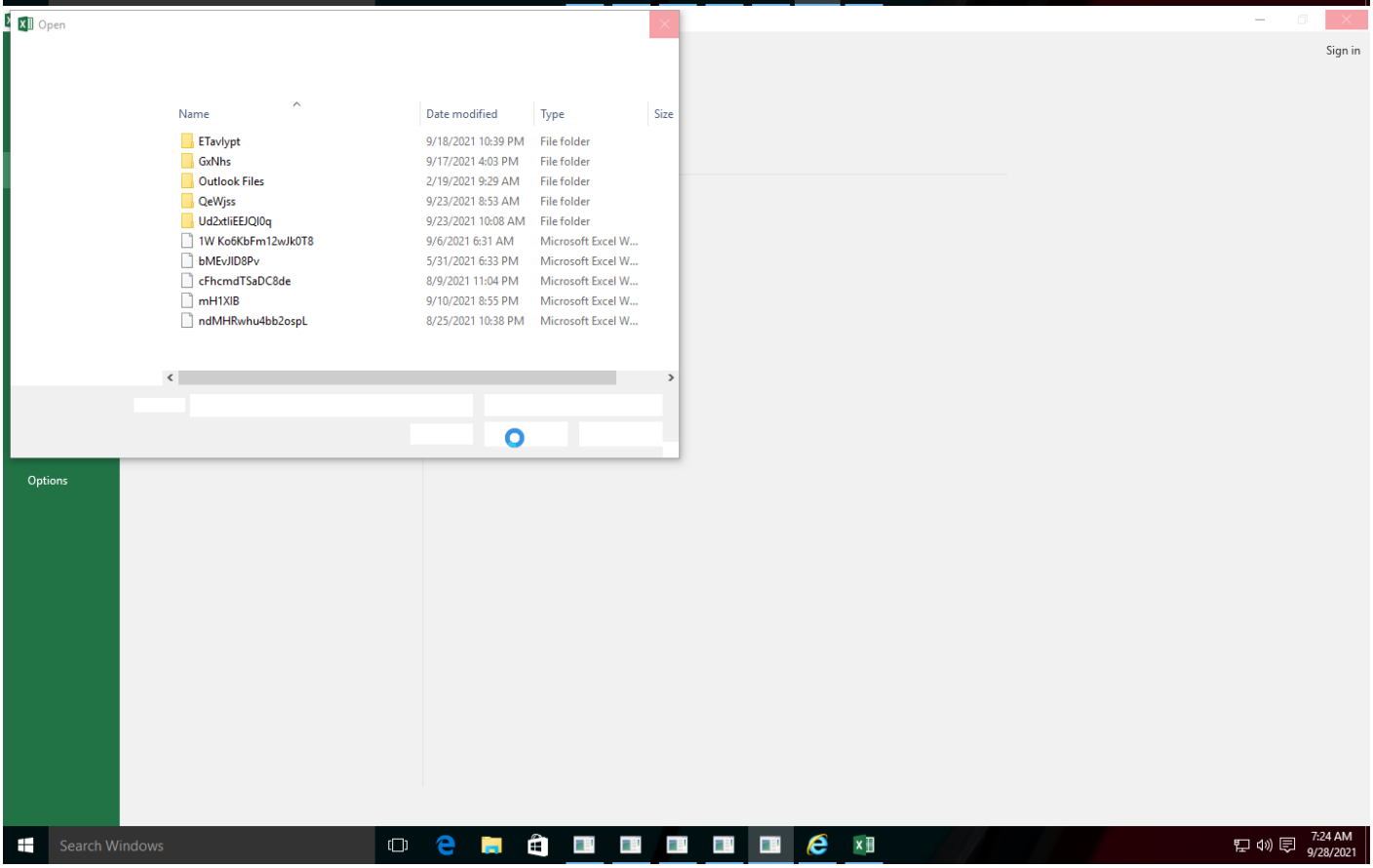
Sample Information

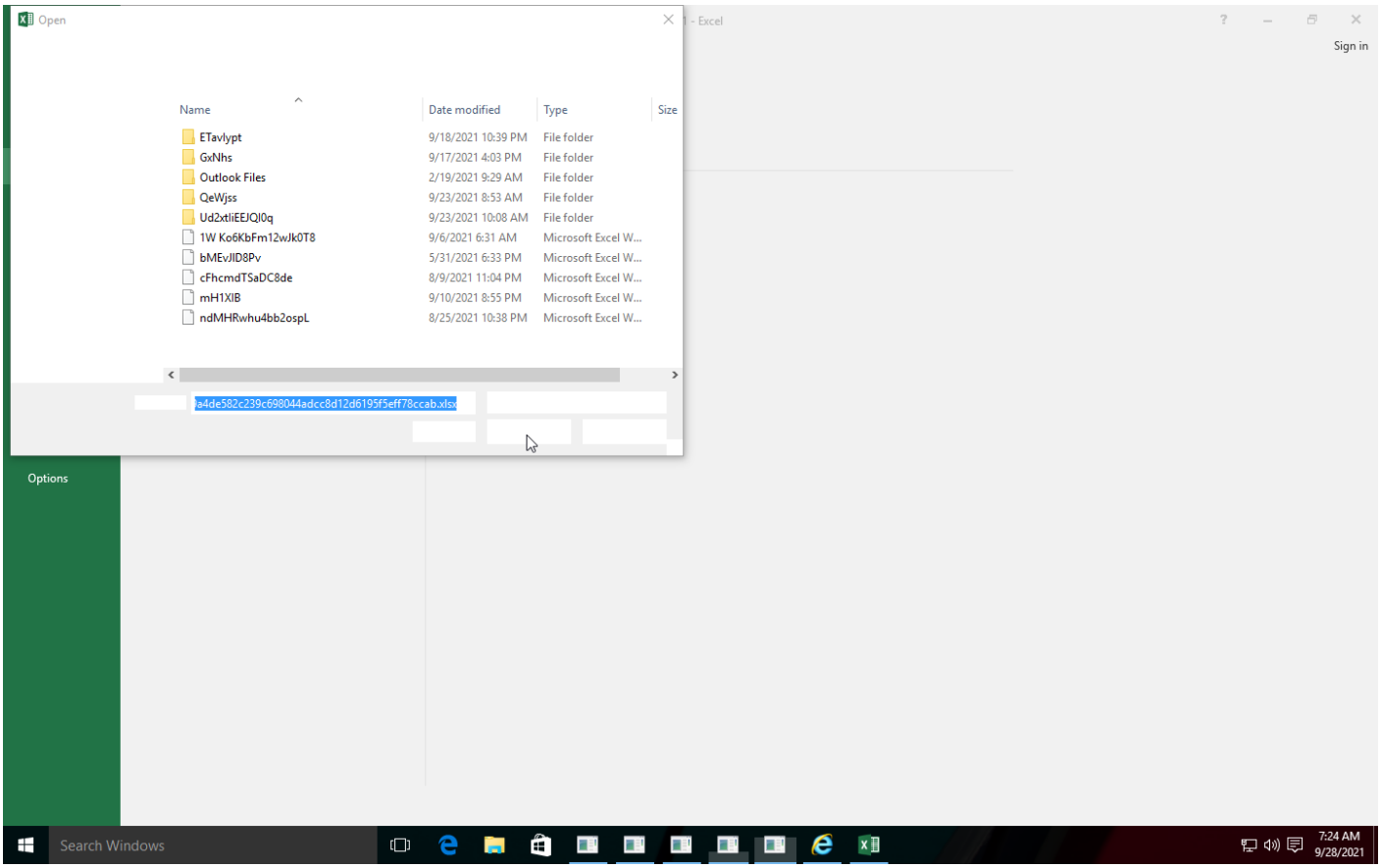
ID	#968536
MD5	27eb25e6fbbbd37115055ecc4b557c53
SHA1	4c986607a941900d9d8804aa351dcab0cc4de224
SHA256	09d2b8f86f136cb14832e9a4de582c239c698044adcc8d12d6195f5eff78ccab
SSDeep	6144:fQOdpdVnGAWCDj4TvvuX2sNNtN+Por6ouj38cawe5kA0t8+yWENL/XfOmPKI:4O7cvCbNtUzP3jmiA06+l6Xf5
File Name	09d2b8f86f136cb14832e9a4de582c239c698044adcc8d12d6195f5eff78ccab.xlsx
File Size	410.62 KB
Sample Type	Excel Document
Has Macros	✓

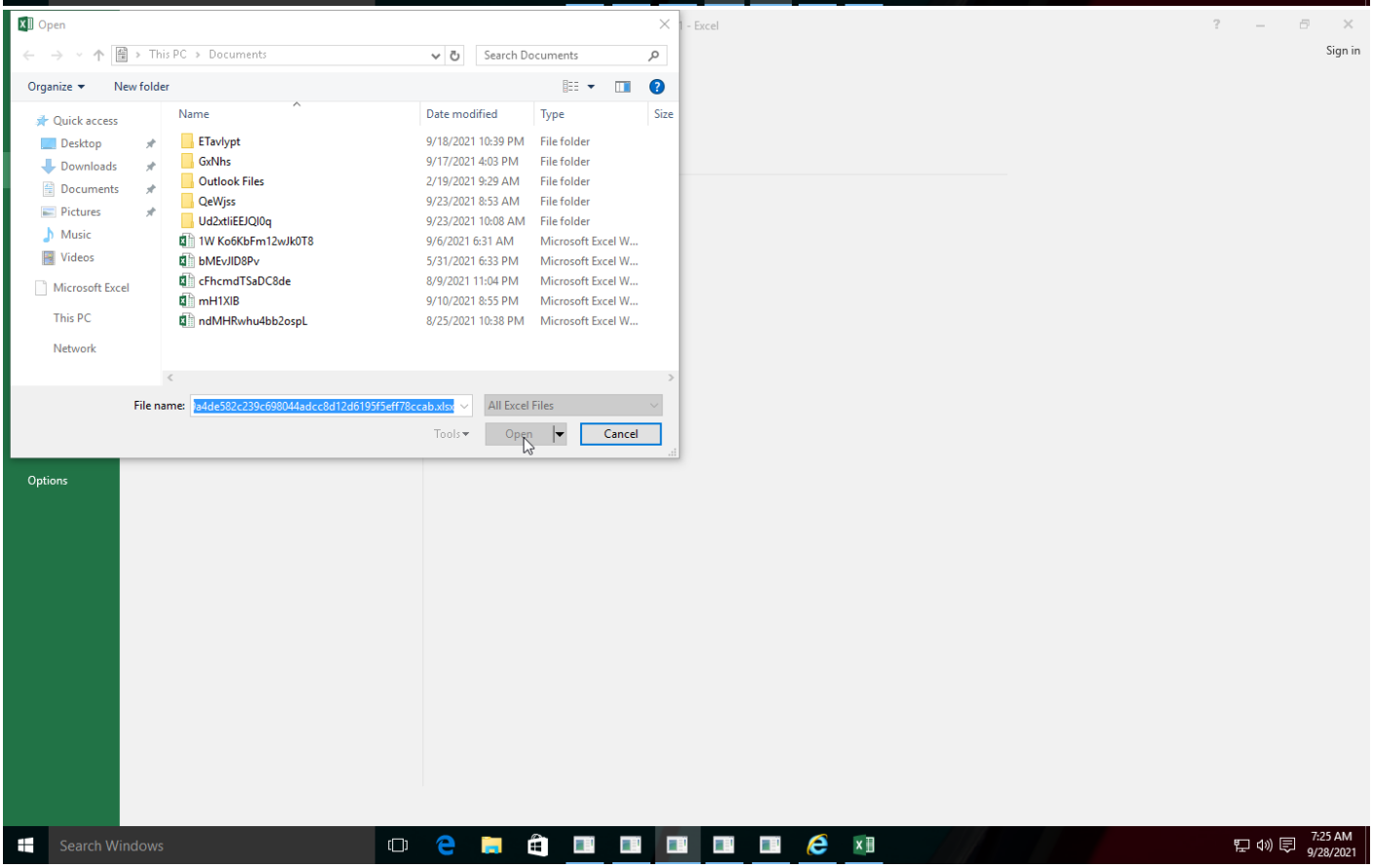
Analysis Information

Creation Time	2021-09-28 09:23 (UTC+2)
Analysis Duration	00:04:08
Termination Reason	Timeout
Number of Monitored Processes	3
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	28
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	26


Open
Name
Date modified
Type
Size
ETavlypt 9/18/2021 10:39 PM File folder
GxNhs 9/17/2021 4:03 PM File folder
Outlook Files 2/19/2021 9:29 AM File folder
QeWjss 9/23/2021 8:53 AM File folder
Ud2xtliEEJQI0q 9/23/2021 10:08 AM File folder
1W Ko6KbFm12wJk0T8 9/6/2021 6:31 AM Microsoft Excel W...
bMEvJID8Pv 5/31/2021 6:33 PM Microsoft Excel W...
cFhcmdTSaDC8de 8/9/2021 11:04 PM Microsoft Excel W...
mH1XIB 9/10/2021 8:55 PM Microsoft Excel W...
ndMHRwhu4bb2ospL 8/25/2021 10:38 PM Microsoft Excel W...
Sign in
Options
Search Windows
7:24 AM
9/28/2021


Open
Name
Date modified
Type
Size
ETavlypt 9/18/2021 10:39 PM File folder
GxNhs 9/17/2021 4:03 PM File folder
Outlook Files 2/19/2021 9:29 AM File folder
QeWjss 9/23/2021 8:53 AM File folder
Ud2xtliEEJQI0q 9/23/2021 10:08 AM File folder
1W Ko6KbFm12wJk0T8 9/6/2021 6:31 AM Microsoft Excel W...
bMEvJID8Pv 5/31/2021 6:33 PM Microsoft Excel W...
cFhcmdTSaDC8de 8/9/2021 11:04 PM Microsoft Excel W...
mH1XIB 9/10/2021 8:55 PM Microsoft Excel W...
ndMHRwhu4bb2ospL 8/25/2021 10:38 PM Microsoft Excel W...
Sign in
Options
Search Windows
7:24 AM
9/28/2021





Screenshots truncated

NETWORK

General

120.07 KB total sent

296.87 KB total received

1 ports 80

3 contacted IP addresses

0 URLs extracted

5 files downloaded

0 malicious hosts detected

DNS

424 DNS requests for 2 domains

1 nameservers contacted

211 total requests returned errors

HTTP/S

2 URLs contacted, 2 servers

214 sessions, 119.64 KB sent, 296.62 KB received

HTTP Requests

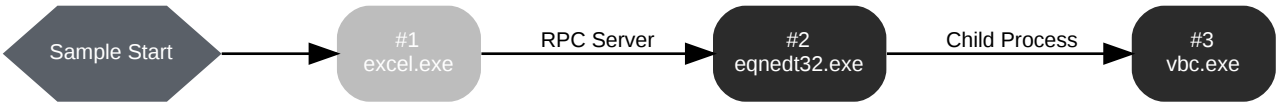
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://103.155.83.184/wdc/vbc.exe	-	-		0 bytes	NA
POST	http://checkvim.com/ga14/fre.php	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	checkvim.com	NoError	5.188.89.50		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: 84690, Reason: Analysis Target
Unmonitor End Time	End Time: 333899, Reason: Terminated by Timeout
Monitor duration	249.21s
Return Code	Unknown
PID	3396
Parent PID	1636
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: 136811, Reason: RPC Server
Unmonitor End Time	End Time: 157036, Reason: Terminated
Monitor duration	20.23s
Return Code	0
PID	3152
Parent PID	628
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
File	1
Process	1

Process #3: vbc.exe

ID	3
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: 154469, Reason: Child Process
Unmonitor End Time	End Time: 333899, Reason: Terminated by Timeout
Monitor duration	179.43s
Return Code	Unknown
PID	4332
Parent PID	3152
Bitness	32 Bit

Dropped Files (5)

File Name	File Size	SHA256	YARA Match
-	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	✗
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.exe	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
-	53 bytes	353fd628b7f6e7d426e5d6a27d1bc3ac22fa7f812e7594cf2ec5ca1175785b50	✗

Host Behavior

Type	Count
System	244
Module	6578
File	307
Environment	1
Registry	181
Mutex	1
User	9

Network Behavior

Type	Count
HTTP	213
DNS	424
TCP	214

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
09d2b8f86f136cb14832e9a4de582c239c698044adcc8d12d6195f5eff78ccab	C:\Users\RDhJ0CNFevzX\Desktop\09d2b8f86f136cb14832e9a4de582c239c698044adcc8d12d6195f5eff78ccab.xlsx	Sample File	410.62 KB	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	-	MALICIOUS
f7e996e828efa2b523a90c99418b95925429ecfd364adc06c7a74250417e8049	Microsoft_Office_Word_Macro-Enabled_Document1.docm	Embedded File	119.64 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	-	MALICIOUS
712f31161e652892b476b13e5671a4fb895d1c37c7d8651429c4efeb62f7639d	image1.png	Embedded File	109.05 KB	image/png	-	MALICIOUS
8bc788fe8527f2818c0d2a2c583d6b06d9a991eb0eee26661631b10eeff2ccde	oleObject1.bin	Embedded File	4.00 KB	application/CDFV2	-	MALICIOUS
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	Write, Create, Delete, Access	CLEAN
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b	C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.lck	Dropped File	1 bytes	application/octet-stream	Write, Create, Delete, 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
e4c1c0121487f83b014b8c81bbaf03db0b7f49584a268a5e67ca64ba6e64676f	-	Downloaded File	205.50 KB	application/vnd.microsoft.portable-executable	-	CLEAN
80aad0ae2fec7897caf8648c99b16b6da20871feb05958cdd324b9f9c6c88b44	-	Downloaded File	288 bytes	application/octet-stream	-	CLEAN
4ba75cecc974b157ac6734d2f6a925a30ac61760d60f326441bac30c95aceef4	-	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
0ac261a3dd7e4e01964f219403d88223318e7b3fa6ccbb196bf2cd9da56151f7	-	Embedded File	1.64 KB	application/octet-stream	-	CLEAN
6c0757667f548698b721e4d723768447046b509c1777d6f1474bde45649d92b0	image1.png	Embedded File	63.53 KB	image/png	-	CLEAN
7bb11564f3c6c559b3ac8ade3e5fca1d51f5451aff5c522d70c3bacec0bbb5d0	image2.jpeg	Embedded File	13.87 KB	image/jpeg	-	CLEAN
a76d01a33a00e98acd33bee9fbe342479ebda9438c922fe264dc0f1847134294	image3.png	Embedded File	33.00 KB	image/png	-	CLEAN
409f06fc20f252c724072a88626cb29f299167eae6655d81df8e9084e62d6cf6	image4.jpeg	Embedded File	8.61 KB	image/jpeg	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\Public\vbc.exe	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.hdb	Dropped File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.lck	Dropped File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.exe	Accessed File	Write, Create, Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://checkvim.com/ga14/fre.php	-	5.188.89.50	-	POST	MALICIOUS
http://103.155.83.184/wdc/vbc.exe	-	103.155.83.184	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
checkvim.com	5.188.89.50	-	DNS, HTTP	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
5.188.89.50	checkvim.com	Russia	DNS, HTTP, TCP	MALICIOUS
192.168.0.1	-	-	UDP, DNS	CLEAN
103.155.83.184	-	Vietnam	HTTP, TCP	CLEAN

Mutex

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

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\CurrentVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\ComodoGroup\IceDragon\Setup\SetupPath	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Apple Computer, Inc.\Safari\InstallDir	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\K-Meleon\CurrentVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\mozilla.org\SeaMonkey\CurrentVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\SeaMonkey\CurrentVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Flock\CurrentVersion	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\QtWeb.NET\QtWeb Internet Browser\AutoComplete	access	vbc.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\8pecxstudios\Cyberfox86\RootDir	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\8pecxstudios\Cyberfox\Path	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Pale Moon\CurrentVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Waterfox\CurrentVersion	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\LinasFTP\Site Manager	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\FlashPeak\BlazeFtp\Settings\LastPassword	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Ghisler\Total Commander\FtpIniName	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\AppDataLow	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\IM Providers	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Netscape	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\ODBC	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\RegisteredApplications	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Wow6432Node	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Classes	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Far\Plugins\FTP\Hosts	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Far2\Plugins\FTP\Hosts	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Bitvise\BvSshClient\LastUsedProfile	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\VanDyke\SecureFX\Config Path	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\NCH Software\Fling\Accounts	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\NCH Software\Fling\Accounts	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\NCH Software\ClassicFTP\FTPAccounts	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\NCH Software\ClassicFTP\FTPAccounts	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\9bis.com\KiTTY\Sessions	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\SimonTatham\PuTTY\Sessions	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\9bis.com\KiTTY\Sessions	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Thunderbird\CurrentVersion	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\IncrediMail\Identities	access	vbc.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Martin Prikryl	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Martin Prikryl	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Postbox\Postbox\CurrentVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\FossaMail\CurrentVersion	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\WinChips\UserAccounts	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\85030200000000000c000000000000046	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\85030200000000000c000000000000046\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	vbc.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Email Address	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User Name	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Server	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User Name	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Email Address	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP User Name	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Server	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Server	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User Name	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP User	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Server URL	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail User Name	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Server	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Port	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Port	read, access	vbc.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Port	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password2	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password2	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password2	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Password2	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password2	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001	access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\Email	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\flaska.net\trojita\imap.auth.pass	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\flaska.net\trojita\msa.smtp.auth.pass	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\������M������k��И���Й��я��\9EDDE9	write, access	vbc.exe	CLEAN

Process

Process Name	Commandline	Verdict
vbc.exe	"C:\Users\Public\vbc.exe"	MALICIOUS
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 (26)

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	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Function Strings	function_strings_process_3.txt	Spyware	5/5

Antivirus (28)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.77897	C:\Users\RDhJ0CNFevzX\Desktop\09d2b8f86f136cb14832e9a4de582c239c698044adcc8d12d6195f5eff78ccab.xlsx	MALICIOUS
Embedded File	Trojan.GenericKDZ.77711	Microsoft_Office_Word_Macro-Enabled_Document1.docm	MALICIOUS
Embedded File	Exploit.CVE-2018-0802.Gen	oleObject1.bin	MALICIOUS
Memory Dump	Generic.Andromeda.C7915F86	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS

File Type	Threat Name	File Name	Verdict
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.762033	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

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

Platform Information

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

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-28 01:56:46+00:00
Built-in AV Database Records	10476967

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