MALICIOUS

Classifications: -

Threat Names: Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Excel Document**
File Name	**habilitado para macro.xlsm**
ID	#8861740
MD5	3558aa966eb00cfbd3071f868e5afb25
SHA1	64dba1361a188e493205ce894d5494db6d489035
SHA256	acfe38dfd3856d7edda03ab3a3f78e7ad908912b162d6a79507f813d442eaa58
File Size	116.72 KB
Report Created	2023-09-19 15:11 (UTC)
Target Environment	win10_64_th2_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (12 rules, 25 matches)

Score	Category	Operation	Count	Classification
4/5	Network Connection	Attempts to connect through HTTPS	2	-
	• (Process #1) excel.exe connects to hxxps://www[.]dropbox[.]com/s/zhp1b06imehwylq/Synaptics.rar?dl=1. • (Process #1) excel.exe connects to hxxps://docs[.]google[.]com/uc?id=0BxsMXGfPIZfSVzUyaHFYVkQxeFk&export=download.			
4/5	Reputation	Malicious host or URL detected via reputation	2	-
	• Reputation analysis labels the URL "hxxps://www[.]dropbox[.]com/s/zhp1b06imehwylq/Synaptics.rar?dl=1" which was contacted by (process #1) excel.exe as Mal/HTMLGen-A. • (Process #1) excel.exe contacted known malicious URL hxxps://docs[.]google[.]com/uc?id=0BxsMXGfPIZfSVzUyaHFYVkQxeFk&export=download.			
2/5	Network Connection	Office macro uses a network function	2	-
	• Office macro uses the network function open. • Office macro uses the network function send.			
2/5	Heuristics	Office macro uses a suspicious function	1	-
	• Macro uses function regwrite (which writes a registry entry.).			
2/5	Execution	Executes macro on specific event	6	-
	• Executes macro automatically on target "workbook" and event "open". • Executes macro on target "workbook" and event "beforeclose". • Executes macro on target "workbook" and event "beforesave". • Executes macro on target "workbook" and event "newsheet". • Executes macro on target "workbook" and event "sheetactivate". • Executes macro on target "workbook" and event "sheetchange".			
2/5	Execution	Creates suspicious COM object	3	-
	• Office macro creates suspicious WinHttp.WinHttpRequest.5.1 COM object. • Office macro creates suspicious WinHttp.WinHttpRequest.5 COM object. • Office macro creates suspicious WScript.Shell COM object.			
2/5	Execution	Office macro uses an execute function	1	-
	• Office macro uses the shell function.			
2/5	Execution	Office macro uses a file I/O function	4	-
	• Office macro uses the open function. • Office macro uses the write function. • Office macro uses the savetofile function. • Office macro uses the close function.			
2/5	YARA	Suspicious content matched by YARA rules	2	-
	• YARA detected "VBA_Create_File" from ruleset "Generic" in script. • YARA detected "VBA_Download_Commands" from ruleset "Generic" in script.			
1/5	Discovery	Queries Office version	1	-
	• Queries office version via application COM object.			

Score	Category	Operation	Count	Classification
1/5	Execution	Contains suspicious Office macro	1	-

• Office document contains a suspicious VBA macro.

Mitre ATT&CK Matrix

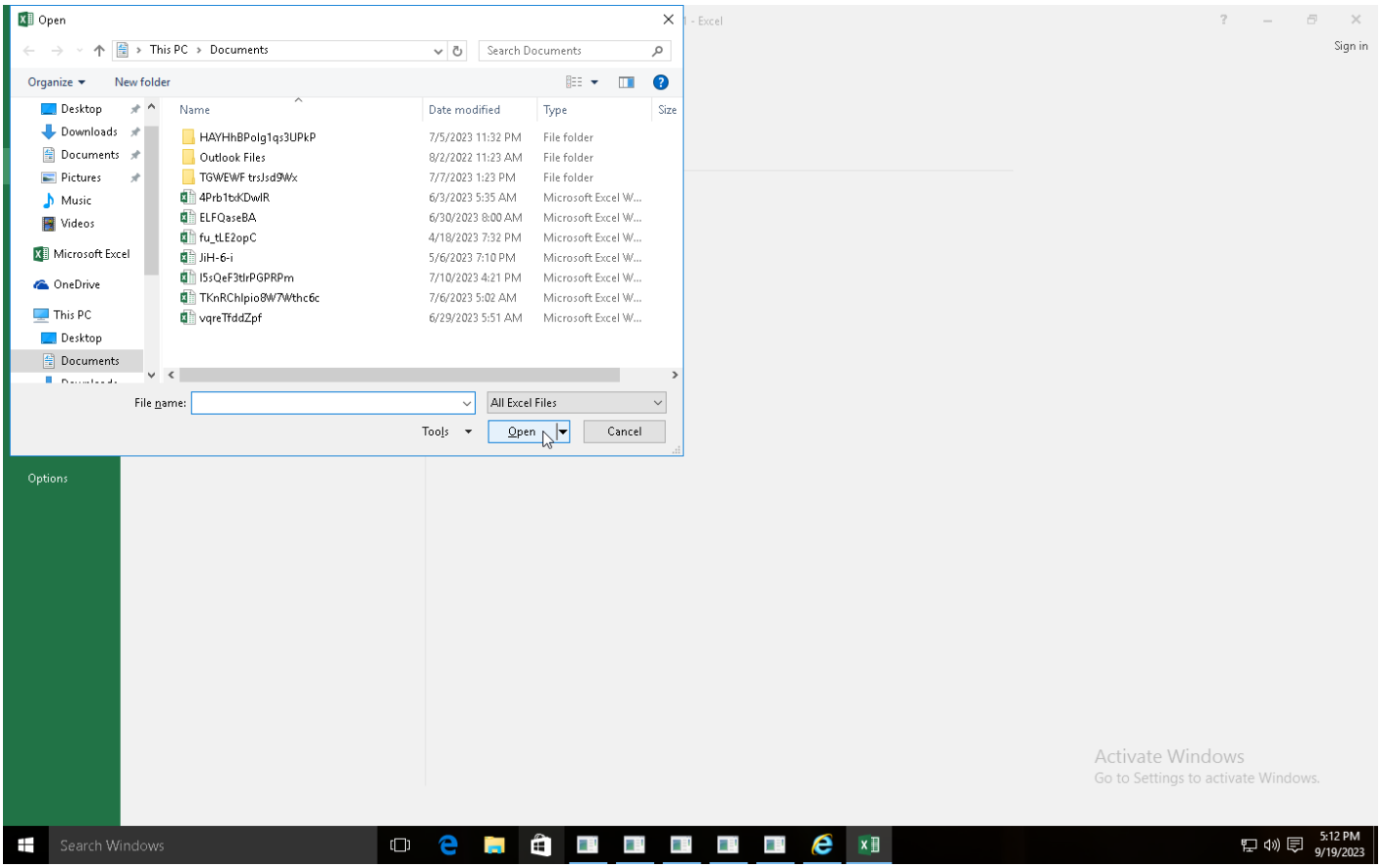
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1064 Scripting			#T1064 Scripting		#T1082 System Information Discovery			#T1071 Standard Application Layer Protocol		
									#T1032 Standard Cryptographic Protocol		

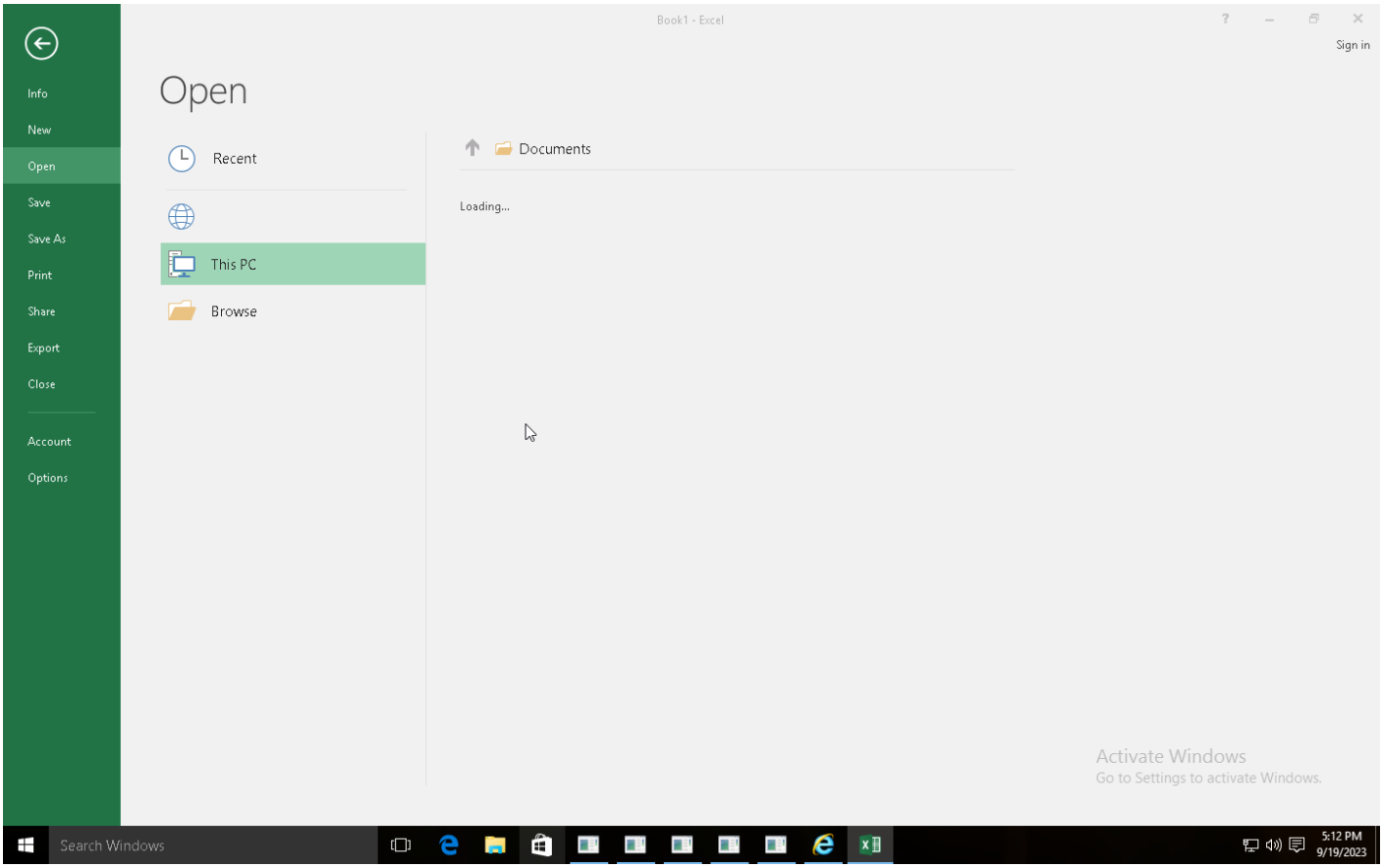
Sample Information

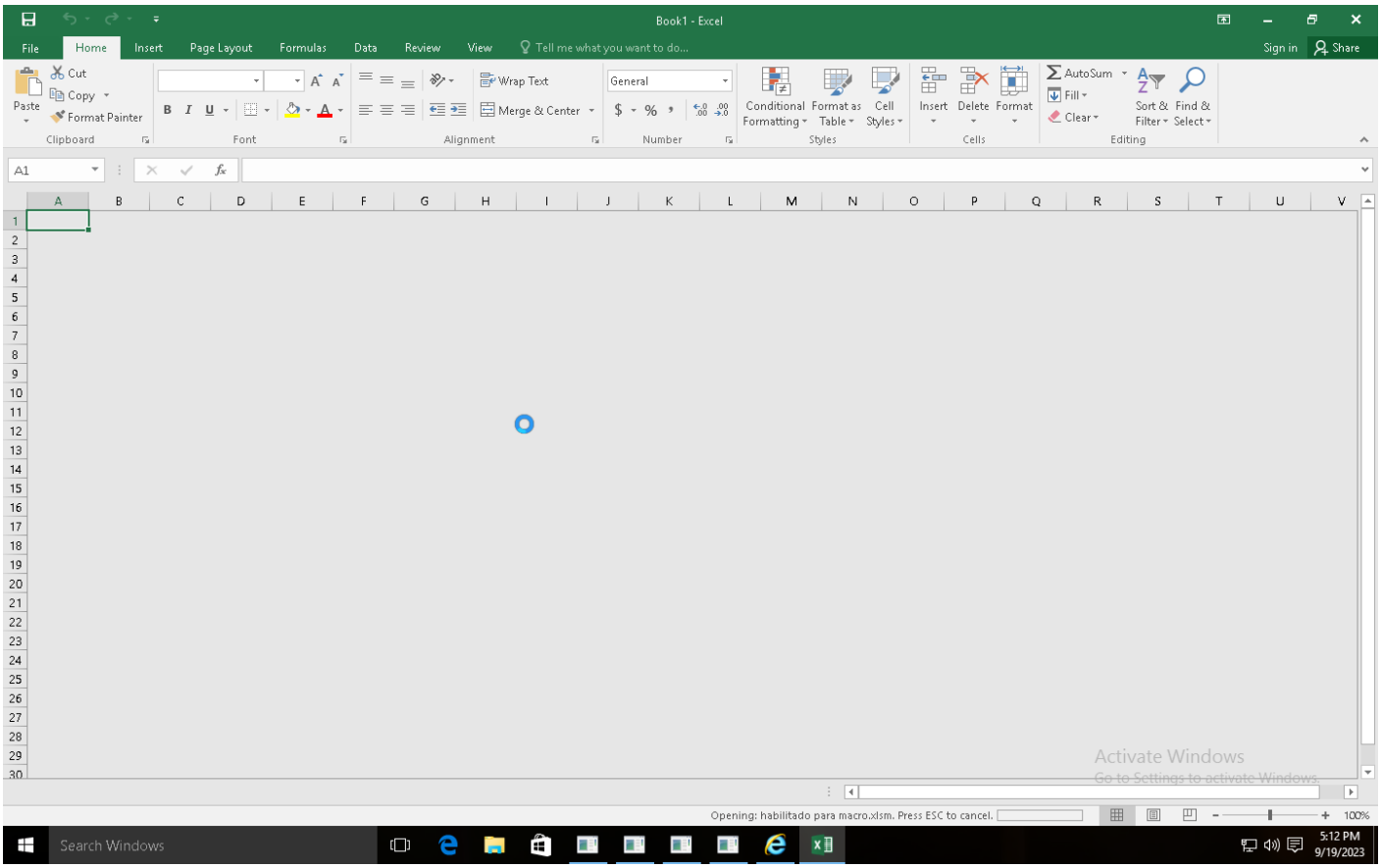
ID	#8861740
MD5	3558aa966eb00cfbd3071f868e5afb25
SHA1	64dba1361a188e493205ce894d5494db6d489035
SHA256	acfe38dfd3856d7edda03ab3a3f78e7ad908912b162d6a79507f813d442eaa58
SSDeep	1536:eLEHorDlOhAYiQRshfkp7Vgk5moAVNL9weeSlQT989dhWB99mhLdSwxOTj4vUYtX:vgpy9shfCh5moAPf8xW1UxO3pYwvWNIu
File Name	habilitado para macro.xlsm
File Size	116.72 KB
Sample Type	Excel Document
Has Macros	✔

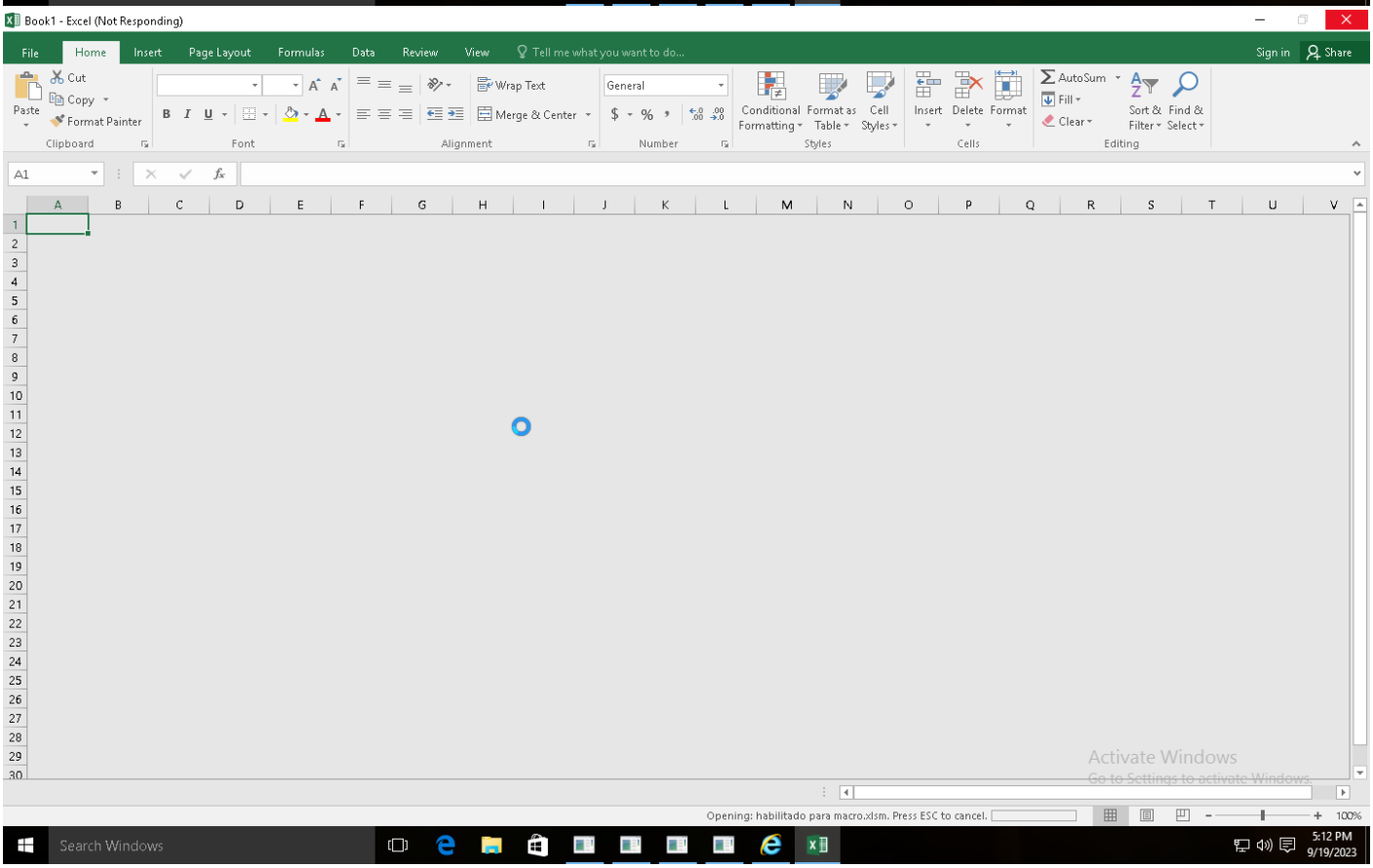
Analysis Information

Creation Time	2023-09-19 15:11 (UTC)
Analysis Duration	00:04:03
Termination Reason	Timeout
Number of Monitored Processes	1
Execution Successful	True
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	2


Open
This PC › Documents
Search Documents
Organize
New folder
Desktop
Downloads
Documents
Pictures
Music
Videos
Microsoft Excel
OneDrive
This PC
Desktop
Documents
Name
Date modified
Type
Size
HAYHhBPolg1qs3UPkP 7/5/2023 11:32 PM File folder
Outlook Files 8/2/2022 11:23 AM File folder
TGWEWF trsJsd9Wx 7/7/2023 1:23 PM File folder
4Prb1txKDwIR 6/3/2023 5:35 AM Microsoft Excel W...
ELFQaseBA 6/30/2023 8:00 AM Microsoft Excel W...
fu_tLE2opC 4/18/2023 7:32 PM Microsoft Excel W...
JiH-6-i 5/6/2023 7:10 PM Microsoft Excel W...
I5sQeF3tlrPGPRPm 7/10/2023 4:21 PM Microsoft Excel W...
TKnRChIpio8W7Wthc6c 7/6/2023 5:02 AM Microsoft Excel W...
vqreTfddZpf 6/29/2023 5:51 AM Microsoft Excel W...
File name:
All Excel Files
Tools
Open
Cancel
Options
Sign in
Activate Windows
Go to Settings to activate Windows.
Search Windows
5:12 PM
9/19/2023


Book1 - Excel
Sign in
Info
New
Open
Save
Save As
Print
Share
Export
Close
Account
Options
Open
Recent
This PC
Browse
Documents
Loading...
Activate Windows
Go to Settings to activate Windows.
Search Windows
5:12 PM
9/19/2023





Screenshots truncated

NETWORK

General

2.27 KB total sent

18.57 KB total received

2 ports 443, 53

3 contacted IP addresses

7 URLs extracted

2 files downloaded

2 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 2 servers

2 sessions, 3.37 KB sent, 26.47 KB received

HTTP Requests

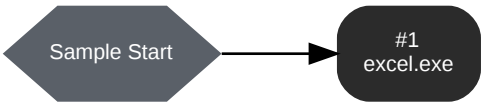
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://www[.]google[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://docs[.]google[.]com/uc?id=0BxsMXGfPIZfSVzUyaHFYVkQxeFk&export=download	-	-	-	0 bytes	MALICIOUS
GET	hxxps://www[.]dropbox[.]com/s/zhp1b06imehwylq/Synaptics.rar?dl=1	-	-	-	0 bytes	MALICIOUS
GET	hxxps://support[.]apple[.]com/HT204416	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]mozilla[.]org/firefox/new/	-	-	-	0 bytes	CLEAN
GET	hxxps://assets[.]dropbox[.]com/www/en-us/illustrations/spot/bowl-empty.svg	-	-	-	0 bytes	CLEAN
GET	hxxps://cfl[.]dropboxstatic[.]com/static/metaserver/static/css/error.css	-	-	-	0 bytes	CLEAN
GET	hxxps://cfl[.]dropboxstatic[.]com/static/images/favicon.ico	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]google[.]com/chrome	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	docs[.]google[.]com	NO_ERROR	172.217.18.110	-	CLEAN
A	www[.]dropbox[.]com, www-env[.]dropbox-dns[.]com	NO_ERROR	162.125.66.18	www-env[.]dropbox-dns[.]com	CLEAN

BEHAVIOR

Process Graph



Process #1: excel.exe

ID	1
File Name	c:\program files\microsoft office\office16\excel.exe
Command Line	"C:\Program Files\Microsoft Office\Office16\EXCEL.EXE"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 64864, Reason: Analysis Target
Unmonitor End Time	End Time: 308051, Reason: Terminated by timeout
Monitor duration	243.19s
Return Code	Unknown
PID	4992
Parent PID	2024
Bitness	64 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
-	5.35 KB	48b090cbfa1300a7a60f6eaafa08ddaccfc96943c8a3e943a4b9d9e45a18b52a	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
COM	12
Registry	44
File	6
System	1
Module	1

Network Behavior

Type	Count
HTTPS	3

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
acfe38dfd3856d7edda03ab3a3f78e7ad908912b162d6a79507f813d442eaa58	C:\Users\RDhJ0CNFevzX\Desktop\habilitado para macro.xlsm	Sample File	116.72 KB	application/vnd.ms-excel.sheet.macroEnabled.12	-	MALICIOUS
21d5b93498b882306a08230096176234c238833061b5954b1ae874e17d8dcbf3	ThisWorkbook	Script	6.33 KB	application/x-vba-macros	-	SUSPICIOUS
a9a292cabe24873cac1e508e576b71f49ddb3a36c1fe27cafffb0e054692f453	-	Downloaded File	1.09 KB	text/html	-	CLEAN
48b090cbfa1300a7a60f6eaafa08ddaccfc96943c8a3e943a4b9d9e45a18b52a	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso4a31.tmp, c:\users\rdhj0cnfevzx\appdata\local\micro... ...t\windows\inetcache\content.mso\mso6f0.tmp, c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso7dd.tmp	Dropped File	5.35 KB	image/png	-	CLEAN
3212aadb6d3a1789c1b9957ce3473863c8ffc425b6706384119568c165d73f34	-	Downloaded File	1.60 KB	text/html	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\habilitado para macro.xlsm	Sample File	-	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso4a31.tmp	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\msoe20.tmp	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\msoe21.tmp	Dropped File	-	CLEAN
C:\Program Files\Common Files\Microsoft Shared\VBA\VBA7.1\VBE7.DLL	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso6f0.tmp	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso7dd.tmp	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso986.tmp	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso549.tmp	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso89a.tmp	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso7dc.tmp	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso89b.tmp	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso6f1.tmp	Dropped File	-	CLEAN

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso4a41.tmp	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso987.tmp	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\mso4ea.tmp	Dropped File, Modified File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\msoc89.tmp	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\msoc88.tmp	Dropped File	-	CLEAN
ThisWorkbook	Miscellaneous File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\msoa63.tmp	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\content.mso\msoa64.tmp	Dropped File	-	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://www[.]dropbox[.]com/s/zhp1b06imehwylq/Synaptics.rar?dl=1	Extracted, Contacted	162.125.66.18	Germany	GET	MALICIOUS
hxxps://docs[.]google[.]com/uc?id=0BxsMXGfPlZfSVzUyaHFYVkQxeFk&export=download	Extracted, Contacted	172.217.18.110	United States	GET	MALICIOUS
hxxps://www[.]google[.]com/chrome	Extracted	-	-	-	CLEAN
hxxps://support[.]apple[.]com/HT204416	Extracted	-	-	-	CLEAN
hxxps://cfl[.]dropboxstatic[.]com/static/metaserver/static/css/error.css	Extracted	-	-	-	CLEAN
hxxps://cfl[.]dropboxstatic[.]com/static/images/favicon.ico	Extracted	-	-	-	CLEAN
hxxps://assets[.]dropbox[.]com/www/en-us/illustrations/spot/bowl-empty.svg	Extracted	-	-	-	CLEAN
hxxp://www[.]google[.]com	Extracted	-	-	-	CLEAN
hxxps://www[.]mozilla[.]org/firefox/new/	Extracted	-	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
www[.]mozilla[.]org	-	-	-	CLEAN
docs[.]google[.]com	172.217.18.110	United States	HTTPS, DNS, TCP	CLEAN
cfl[.]dropboxstatic[.]com	-	-	-	CLEAN
www[.]google[.]com	-	-	-	CLEAN
www[.]dropbox[.]com	162.125.66.18	Germany	HTTPS, DNS, TCP	CLEAN
assets[.]dropbox[.]com	-	-	-	CLEAN
www-env[.]dropbox-dns[.]com	162.125.66.18	Germany	HTTPS, DNS, TCP	CLEAN
support[.]apple[.]com	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
172.217.18.110	docs[.]google[.]com	United States	HTTPS, DNS, TCP	CLEAN
162.125.66.18	www[.]dropbox[.]com, www-env[.]dropbox-dns[.]com	Germany	HTTPS, DNS, TCP	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CLASSES_ROOT\TypeLib\{00020430-0000-0000-C000-000000000046}\2.0\0	access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	access, create	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{00020430-0000-0000-C000-000000000046}\2.0	access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{2DF8D04C-5BFA-101B-BDE5-00AA0044DE52}\2.8\0\win64	read, access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{2DF8D04C-5BFA-101B-BDE5-00AA0044DE52}	access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\BreakOnAllErrors	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\BreakOnServerErrors	read, access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{000204EF-0000-0000-C000-000000000046}	access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{00020813-0000-0000-C000-000000000046}	access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{00020430-0000-0000-C000-000000000046}	access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{00020813-0000-0000-C000-000000000046}\1.9\0\win64	read, access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{00020430-0000-0000-C000-000000000046}\2.0\0\win64	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security\VBAWarnings	access, write	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\BackGroundCompile	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\RequireDeclaration	read, access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib	access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security\VBAWarnings	access, write	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{000204EF-0000-0000-C000-000000000046}\4.2\9\win64	read, access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{2DF8D04C-5BFA-101B-BDE5-00AA0044DE52}\2.8\0	access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\NotifyUserBeforeStateLoss	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\CompileOnDemand	read, access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{000204EF-0000-0000-C000-000000000046}\4.2\9	access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{00020813-0000-0000-C000-000000000046}\1.9\0	access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{000204EF-0000-0000-C000-000000000046}\4.2	access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\TypeLib\{00020813-0000-0000-C000-000000000046}\1.9	access	excel.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CLASSES_ROOT\TypeLib\{2DF8D04C-5BFA-101B-BDE5-00AA0044DE52}\2.8	access	excel.exe	CLEAN

Process

Process Name	Commandline	Verdict
excel.exe	"C:\Program Files\Microsoft Office\Office16\EXCEL.EXE"	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Generic	VBA_Create_File	VBA macro contains file creation commands; possible dropper	-	ThisWorkbook	-	2/5
Generic	VBA_Download_Commands	VBA macro may attempt to download external content; possible dropper	-	ThisWorkbook	-	2/5

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	2023.3.1
Dynamic Engine Version	2023.3.1 / 07/17/2023 04:23
Static Engine Version	2023.3.1.0 / 2023-07-17 03:00:15
AV Exceptions Version	2023.3.1.2 / 2023-07-01 17:20:29
Link Detonation Heuristics Version	2023.3.1.24 / 2023-08-31 16:59:16
Smart Memory Dumping Rules Version	2023.3.1.2 / 2023-07-01 17:20:29
Config Extractors Version	2023.3.1.31 / 2023-09-07 19:33:31
Signature Trust Store Version	2023.3.1.2 / 2023-07-01 17:20:29
VMRay Threat Identifiers Version	2023.3.1.32 / 2023-09-11 09:59:25
YARA Built-in Ruleset Version	2023.3.1.24

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	8.0.1710.11

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