MALICIOUS

Classifications: -

Threat Names: VB:Trojan.Valyria.5339

Verdict Reason: -

Sample Type	**Excel Document**
File Name	**2013496fe5524988c28357245d684cdca787b47c0b3b16cae20b3222977d769b.xlsx.xls**
ID	#2776995
MD5	34ee9111f987b903bce643f660d2d7ce
SHA1	a7b9d6fa34914921826fc7913e0d3ccd145ebaf2
SHA256	2013496fe5524988c28357245d684cdca787b47c0b3b16cae20b3222977d769b
File Size	203.00 KB
Report Created	2021-09-25 14:35 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (10 rules, 17 matches)

Score	Category	Operation	Count	Classification
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected the sample itself as "VB:Trojan.Valyria.5339".			
4/5	Heuristics	Document tries to trick users into running macros	1	-
	• Extracted text from an image embedded in C:\Users\RDhJ0CNFevzX\Desktop\2013496fe5524988c28357245d684cdca787b47c0b3b16cae20b3222977d769b.xlsx.xls suggests enabling macros.			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
4/5	Execution	Document tries to create process	3	-
	• Document creates (process #3) regsvr32.exe. • Document creates (process #4) regsvr32.exe. • Document creates (process #5) regsvr32.exe.			
3/5	Obfuscation	Contains obfuscated URL	3	-
	• C:\Users\RDhJ0CNFevzX\Desktop\2013496fe5524988c28357245d684cdca787b47c0b3b16cae20b3222977d769b.xlsx.xls contains an obfuscated URL "http://103.155.92.211/". • C:\Users\RDhJ0CNFevzX\Desktop\2013496fe5524988c28357245d684cdca787b47c0b3b16cae20b3222977d769b.xlsx.xls contains an obfuscated URL "http://193.38.54.149/". • C:\Users\RDhJ0CNFevzX\Desktop\2013496fe5524988c28357245d684cdca787b47c0b3b16cae20b3222977d769b.xlsx.xls contains an obfuscated URL "http://94.140.114.44/".			
2/5	Execution	Office macro uses an execute function	1	-
	• Office macro uses the run function.			
2/5	Execution	Office macro uses a file I/O function	1	-
	• Office macro uses the close function.			
2/5	Execution	Executes macro on specific event	4	-
	• Executes macro automatically on target "document" and event "open". • Executes macro automatically on target "workbook" and event "open". • Executes macro on target "document" and event "close". • Executes macro on target "workbook" and event "activate".			
1/5	Discovery	Queries Office version	1	-
	• Queries office version via application COM object.			
1/5	Execution	Contains suspicious Office macro	1	-
	• Office document contains a suspicious VBA macro.			
-	Trusted	Known clean file	2	-
	• File "c:\users\rdhj0cnfevzx\appdata\local\temp\~dfcf87438905ed2d8b.tmp" is a known clean file. • File "c:\users\rdhj0cnfevzx\appdata\local\temp\~df47fd94e12aafce74.tmp" is a known clean file.			

Mitre ATT&CK Matrix

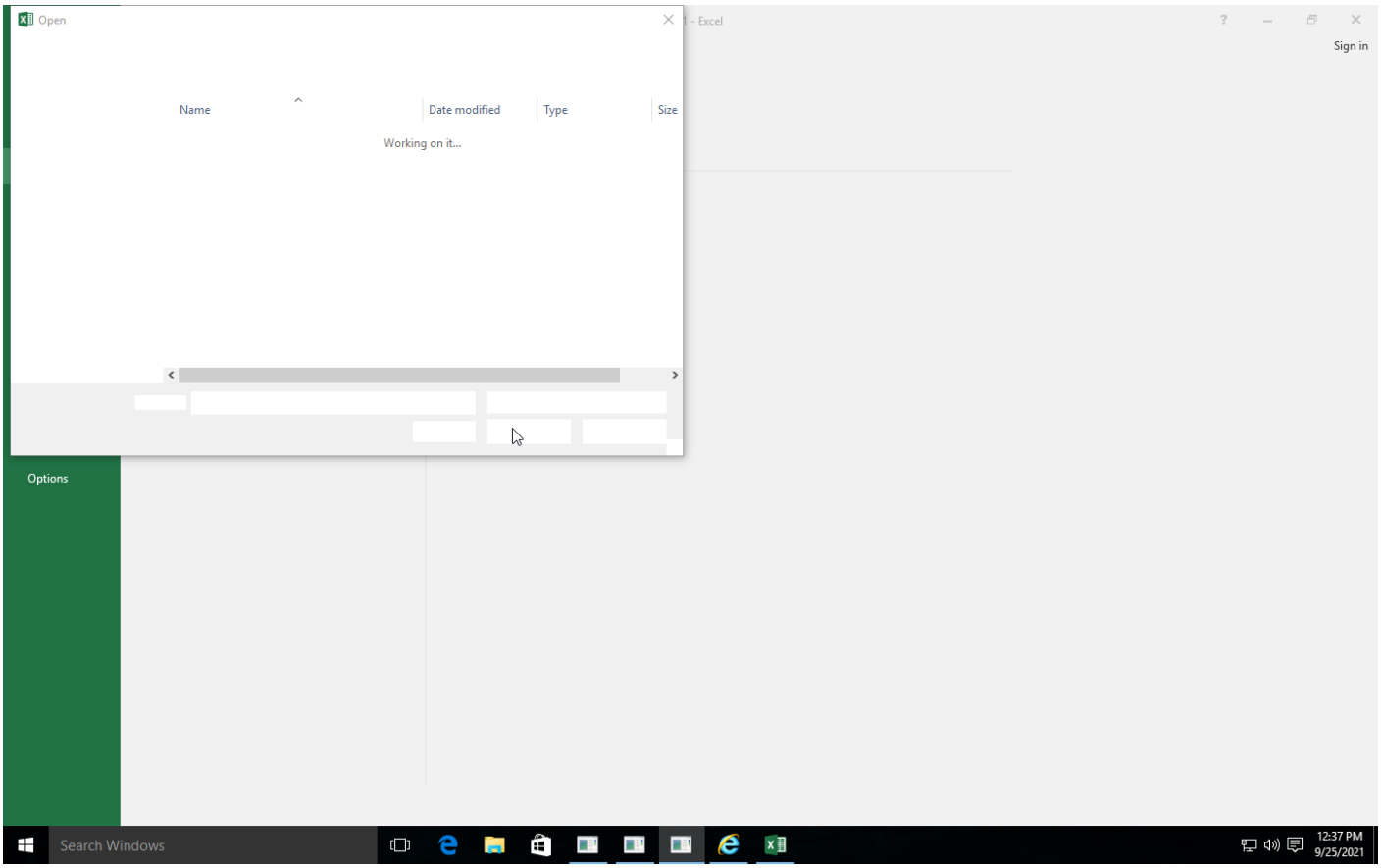
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1064 Scripting			#T1064 Scripting		#T1082 System Information Discovery					
				#T1027 Obfuscated Files or Information							

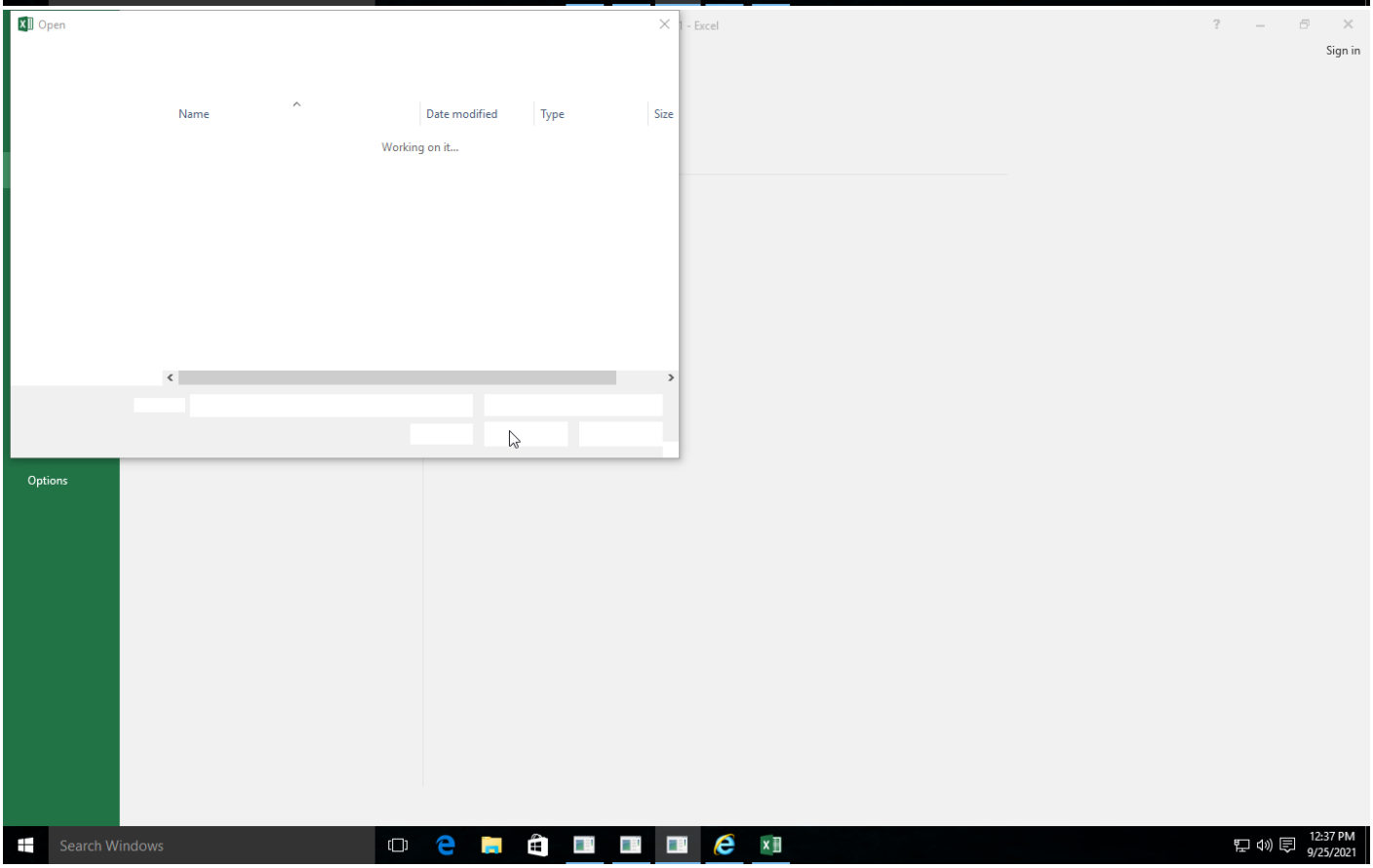
Sample Information

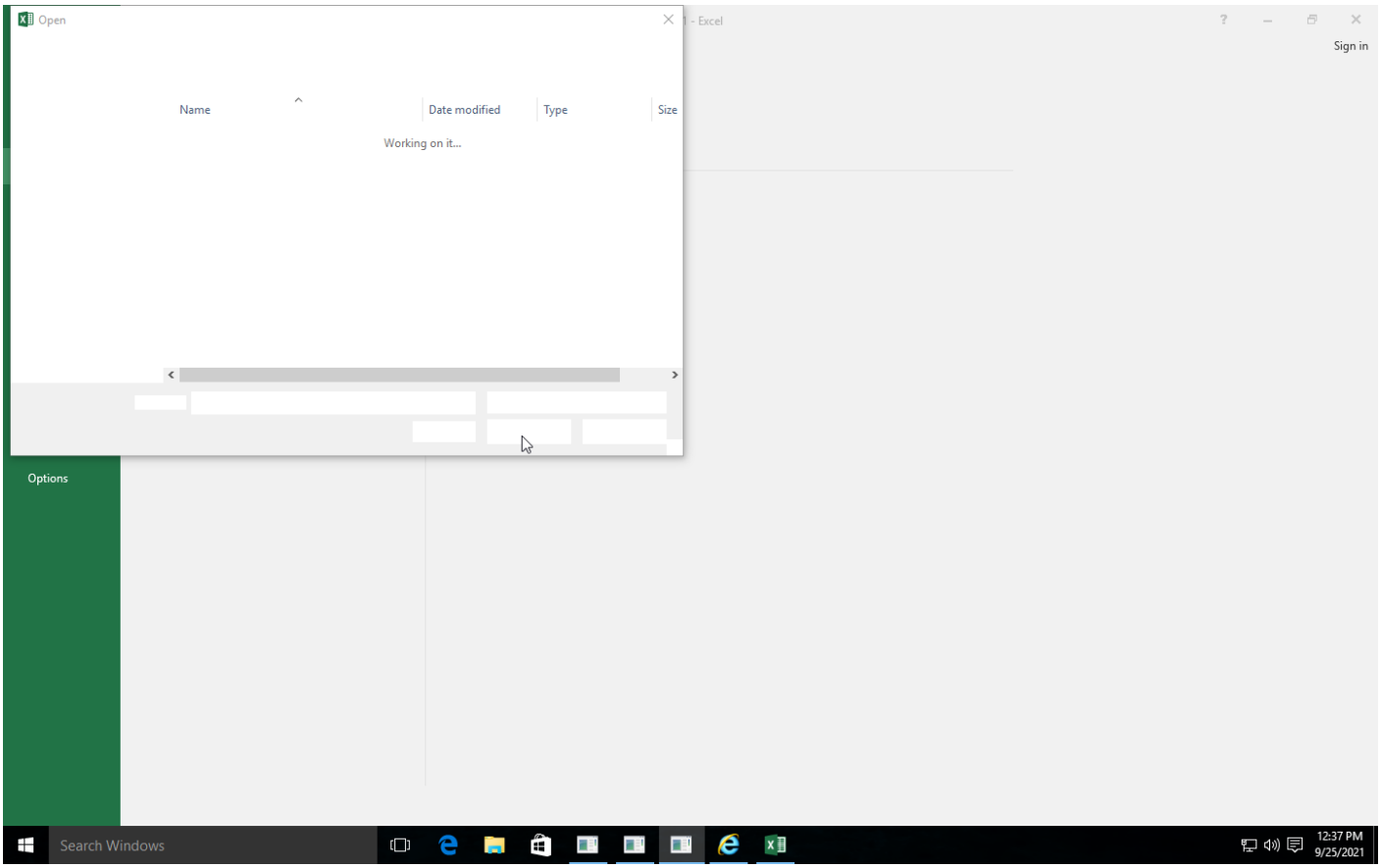
ID	#2776995
MD5	34ee9111f987b903bce643f660d2d7ce
SHA1	a7b9d6fa34914921826fc7913e0d3ccd145ebaf2
SHA256	2013496fe5524988c28357245d684cdca787b47c0b3b16cae20b3222977d769b
SSDeep	6144:oKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgCSPofSHI8oD5j:ERq55j
File Name	2013496fe5524988c28357245d684cdca787b47c0b3b16cae20b3222977d769b.xlsx.xls
File Size	203.00 KB
Sample Type	Excel Document
Has Macros	✓

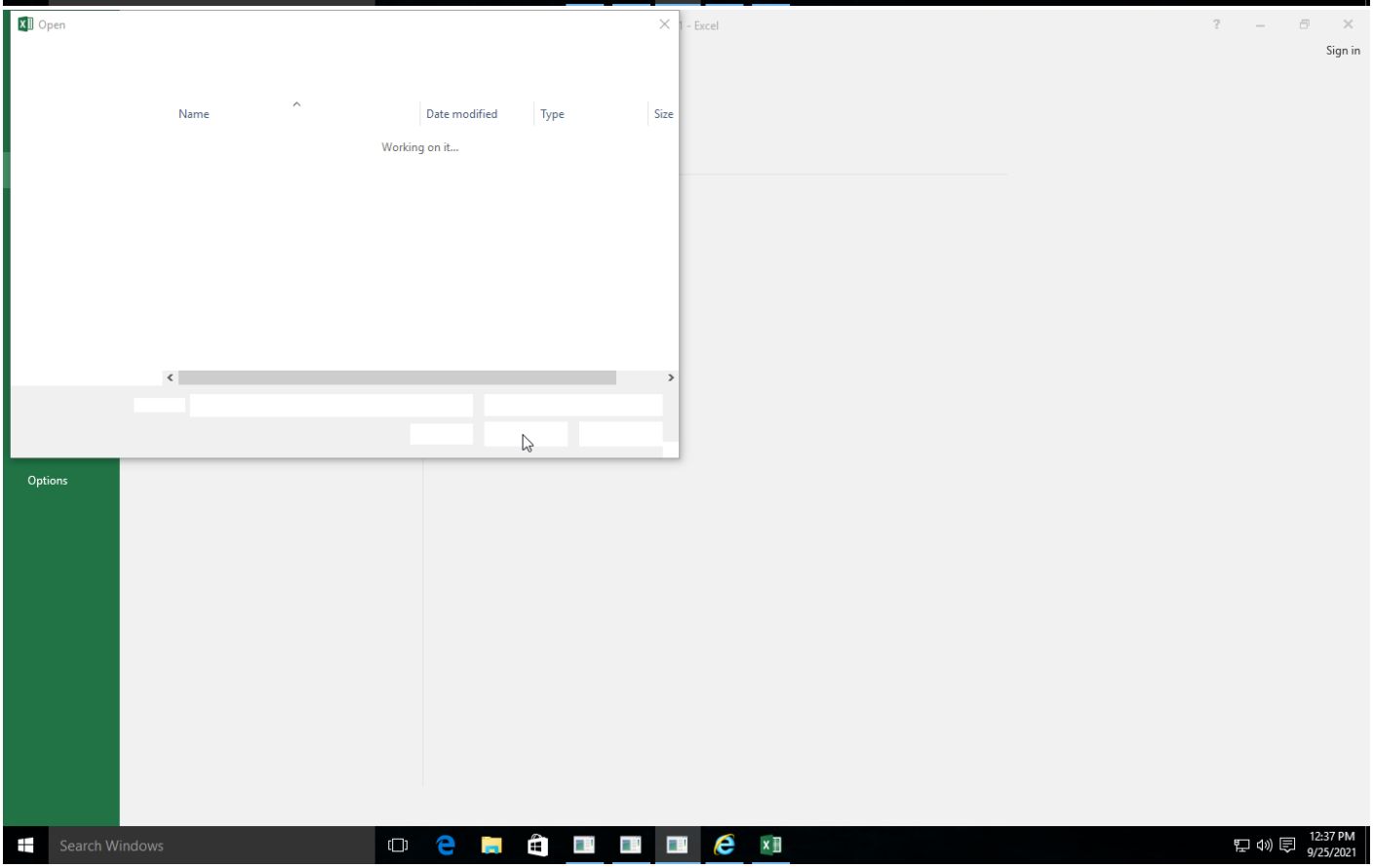
Analysis Information

Creation Time	2021-09-25 14:35 (UTC+2)
Analysis Duration	00:03:44
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✓
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	1
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Open
Name
Date modified
Type
Size
Working on it...
- Excel
Sign in
Options
Search Windows
12:37 PM
9/25/2021


Open
Name
Date modified
Type
Size
Working on it...
- Excel
Sign in
Options
Search Windows
12:37 PM
9/25/2021





Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

1 ports 80

3 contacted IP addresses

3 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

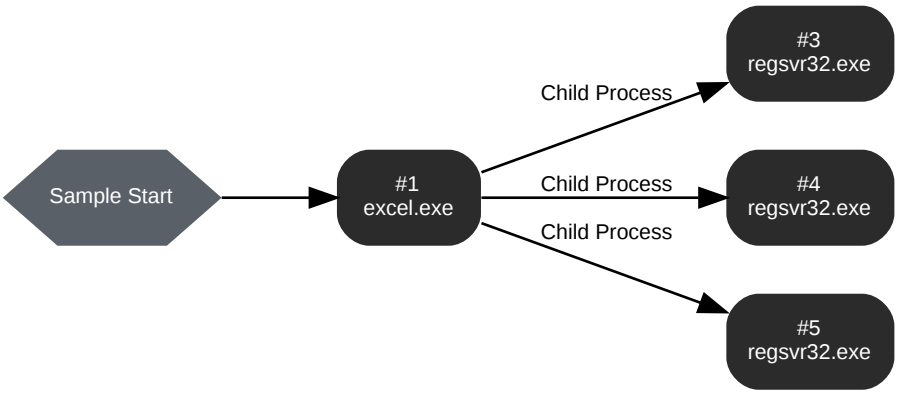
0 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://103.155.92.211/	-	-		0 bytes	NA
GET	http://193.38.54.149/	-	-		0 bytes	NA
GET	http://94.140.114.44/	-	-		0 bytes	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: 97802, Reason: Analysis Target
Unmonitor End Time	End Time: 318730, Reason: Terminated
Monitor duration	220.93s
Return Code	0
PID	5088
Parent PID	1600
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
-	1.50 KB	1dc0c8d7304c177ad0e74d3d2f1002eb773f4b180685a7df6bbe75ccc24b0164	✗
-	512 bytes	076a27c79e5ace2a3d47f9dd2e83e4ff6ea8872b3c2218f66c92b89b55f36560	✗

Host Behavior

Type	Count
Module	14
Registry	45
Window	37
Keyboard	8
COM	1

Process #3: regsvr32.exe

ID	3
File Name	c:\windows\syswow64\regsvr32.exe
Command Line	regsvr32 -silent ..\Xertis.dll
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 198399, Reason: Child Process
Unmonitor End Time	End Time: 202331, Reason: Terminated
Monitor duration	3.93s
Return Code	3
PID	4720
Parent PID	5088
Bitness	32 Bit

Host Behavior

Type	Count
Module	2
Registry	4

Process #4: regsvr32.exe

ID	4
File Name	c:\windows\syswow64\regsvr32.exe
Command Line	regsvr32 -silent ..\Xertis1.dll
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 200897, Reason: Child Process
Unmonitor End Time	End Time: 202488, Reason: Terminated
Monitor duration	1.59s
Return Code	3
PID	4744
Parent PID	5088
Bitness	32 Bit

Host Behavior

Type	Count
Module	2
Registry	4

Process #5: regsvr32.exe

ID	5
File Name	c:\windows\syswow64\regsvr32.exe
Command Line	regsvr32 -silent ..\Xertis2.dll
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 201317, Reason: Child Process
Unmonitor End Time	End Time: 203235, Reason: Terminated
Monitor duration	1.92s
Return Code	3
PID	4008
Parent PID	5088
Bitness	32 Bit

Host Behavior

Type	Count
Module	2
Registry	4

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2013496fe5524988c28357245d684cdca787b47c0b3b16cae20b3222977d769b	C:\Users\RDhJ0CNFevzX\Desktop\2013496fe5524988c28357245d684cdca787b47c0b3b16cae20b3222977d769b.xlsx.xls	Sample File	203.00 KB	application/vnd.ms-excel	-	MALICIOUS
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN
1dc0c8d7304c177ad0e74d3d2f1002eb773f4b180685a7df6bbe75ccc24b0164	c:\users\rdhj0cnfevzx\appdata\local\temp\~dfcf87438905ed2d8b.tmp	Dropped File	1.50 KB	application/CDFV2	-	CLEAN
076a27c79e5ace2a3d47f9dd2e83e4ff6ea8872b3c2218f66c92b89b55f36560	c:\users\rdhj0cnfevzx\appdata\local\temp\~df47fd94e12aafce74.tmp	Dropped File	512 bytes	application/octet-stream	-	CLEAN
d36f4c20dc961f9647f933d75e97cb62ef094a2cb7ee61dd4196c60b66bdf0d2	0.JPG	Embedded File	160.17 KB	image/jpeg	-	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://103.155.92.211	-	-	-	GET	CLEAN
http://193.38.54.149	-	-	-	GET	CLEAN
http://94.140.114.44	-	-	-	GET	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
94.140.114.44	-	Latvia	TCP	CLEAN
103.155.92.211	-	Malaysia	TCP	CLEAN
193.38.54.149	-	Netherlands	TCP	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\MdiMaximized	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\GridWidth	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\GridHeight	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\ShowGrid	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\AlignToGrid	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\SaveBeforeRun	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\ShowToolTips	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\CollapseWindows	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\UpgradeVBX	read, access	excel.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\ReadOnlyMode	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\BackgroundProjectLoad	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\FolderView	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\Tool	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\PropertiesWindow	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\UI	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\Dock	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\VBE\6.0\Addins	access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\Designers	access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\ToolboxControls	access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\CtlsShowSelected	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\DsnShowSelected	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\MainWindow	read, access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\Clsid\{C62A69F0-16DC-11CE-9E98-00AA00574A4F}\Instance CLSID	read, access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\.dll	read, access	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\dllfile	access	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\dllfile\AutoRegister	access	regsvr32.exe	CLEAN

Process

Process Name	Commandline	Verdict
excel.exe	"C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE"	CLEAN
regsvr32.exe	regsvr32 -silent ..\Xertis.dll	CLEAN
regsvr32.exe	regsvr32 -silent ..\Xertis1.dll	CLEAN
regsvr32.exe	regsvr32 -silent ..\Xertis2.dll	CLEAN

YARA / AV

Antivirus (1)

File Type	Threat Name	File Name	Verdict
Sample File	VB:Trojan.Valyria.5339	C:\Users\RDhJ0CNFevzX\Desktop\2013496fe5524988c28357245d684cdca787b47c0b3b16cae20b3222977d769b.xlsx.xls	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	2021-09-25 08:22:24+00:00
Built-in AV Database Records	10456970

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