ID: 382553
Sample Name: 12345.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 09:47:08
Date: 06/04/2021
Version: 31.0.0 Emerald

Table of Contents

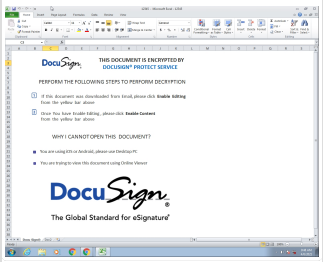
Analysis Report 12345.xlsm

Overview

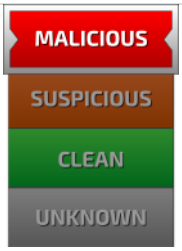
General Information

Sample Name:	12345.xlsm
Analysis ID:	382553
MD5:	5851c6423d6cffd..
SHA1:	8992a00647a35e..
SHA256:	a7893081be92e7..
Tags:	GG Gozi ISFB Ursnif xlsm
Infos:	

Most interesting Screenshot:



Detection



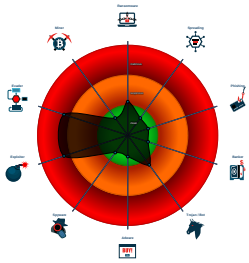
Hidden Macro 4.0

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

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Allocates a big amount of memory (p…
- Excel documents contains an embe…
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Registers a DLL
- Uses a known web browser user age…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2308 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 1476 cmdline: regsvr32.exe -s ..\nvcoerf.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1820 cmdline: regsvr32.exe -s ..\nvcoerf1.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2560 cmdline: regsvr32.exe -s ..\nvcoerf2.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2608 cmdline: regsvr32.exe -s ..\nvcoerf3.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2592 cmdline: regsvr32.exe -s ..\nvcoerf4.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

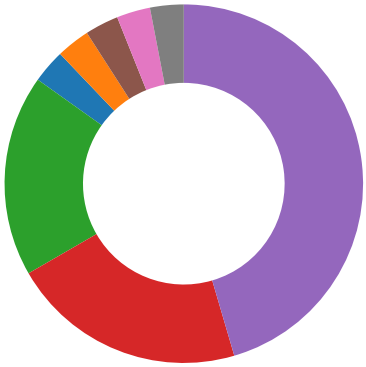
Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

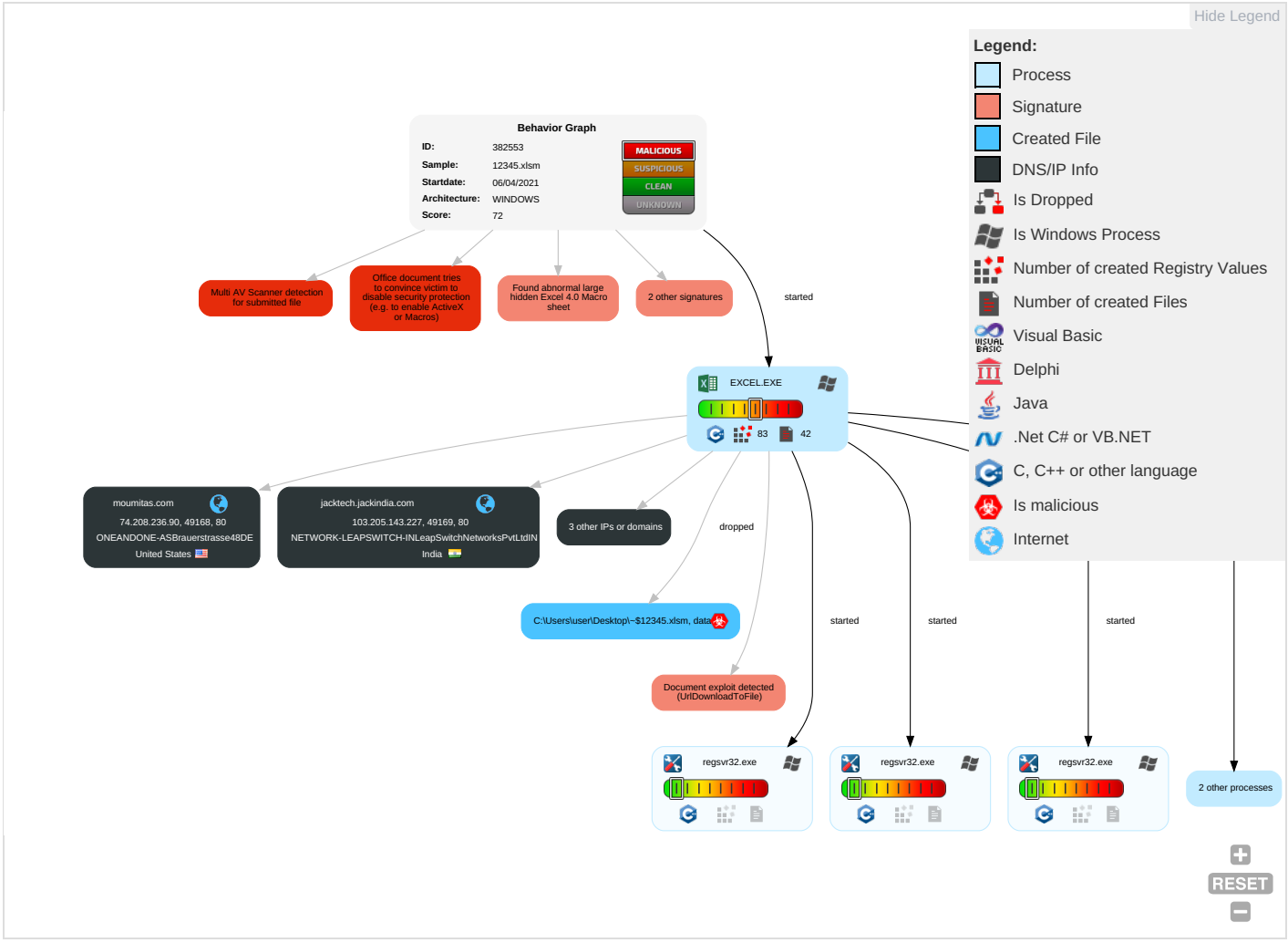
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

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
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Regsvr32 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 3	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Masquerading 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

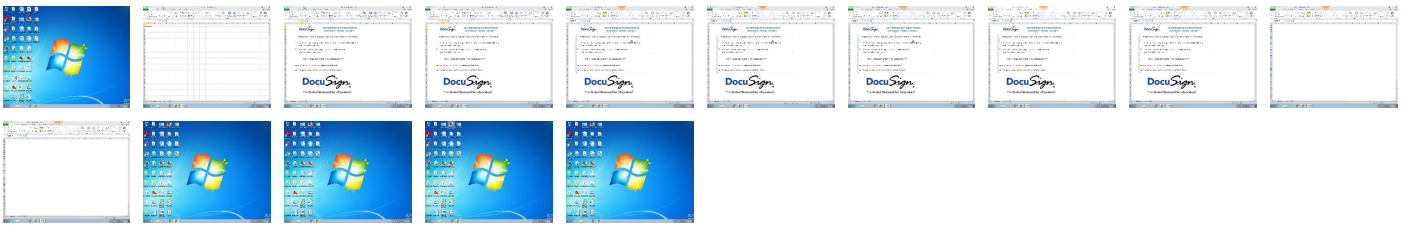
Behavior Graph

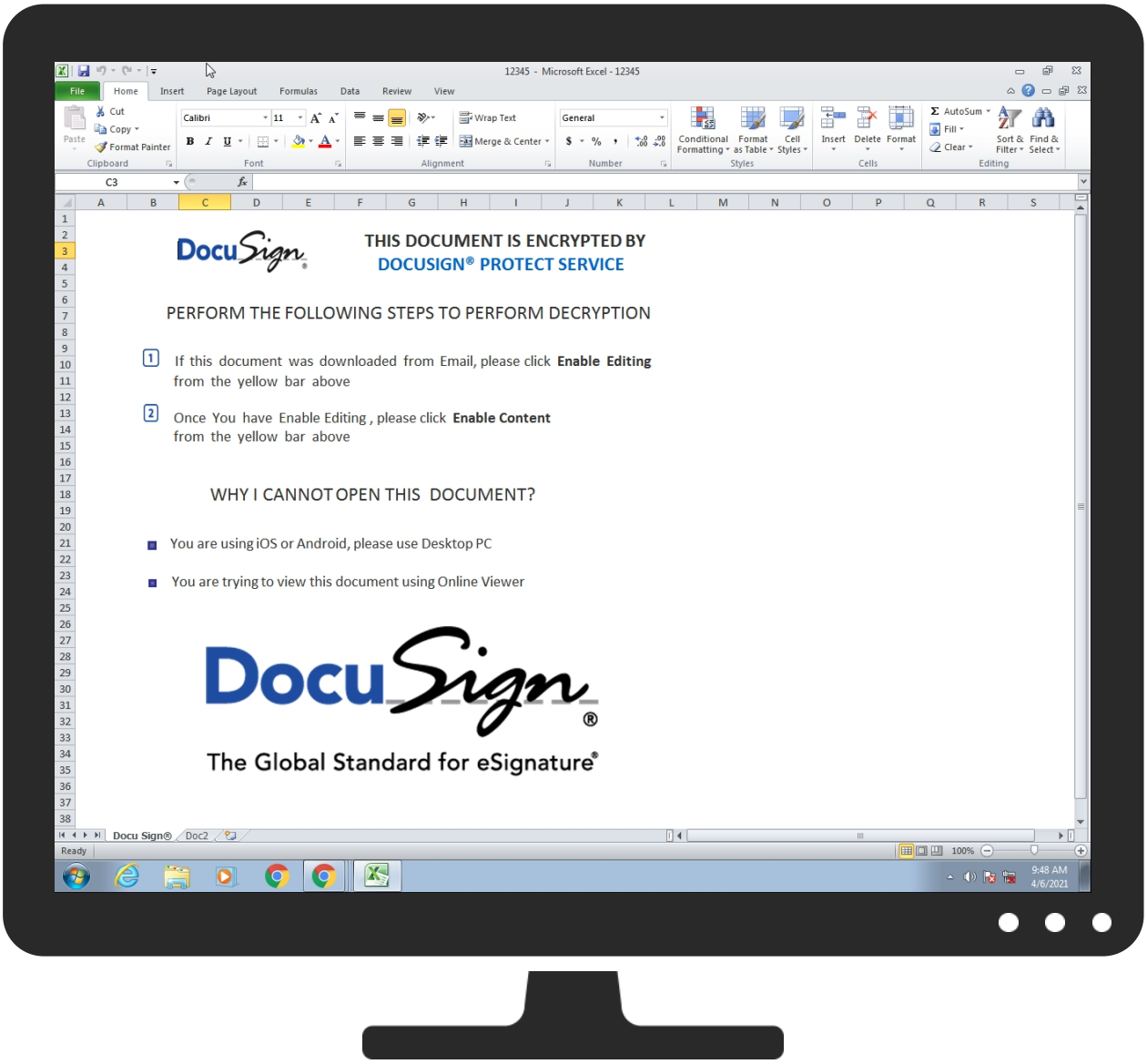


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
12345.xlsm	17%	ReversingLabs	Document-Excel.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://velma-harber30ku.com/gg.gif	0%	Avira URL Cloud	safe	
http://mills-skyla30ec.com/gg.gif	0%	Avira URL Cloud	safe	
http://jacktech.jackindia.com/ds/0204.gif	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://moumitas.com/ds/0204.gif	0%	Avira URL Cloud	safe	
http://laura9630fr.com/gg.gif	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
laura9630fr.com	8.211.4.209	true	false		unknown
mills-skyla30ec.com	8.211.4.209	true	false		unknown
jacktech.jackindia.com	103.205.143.227	true	false		unknown
velma-harber30ku.com	8.211.4.209	true	false		unknown
moumitas.com	74.208.236.90	true	false		unknown

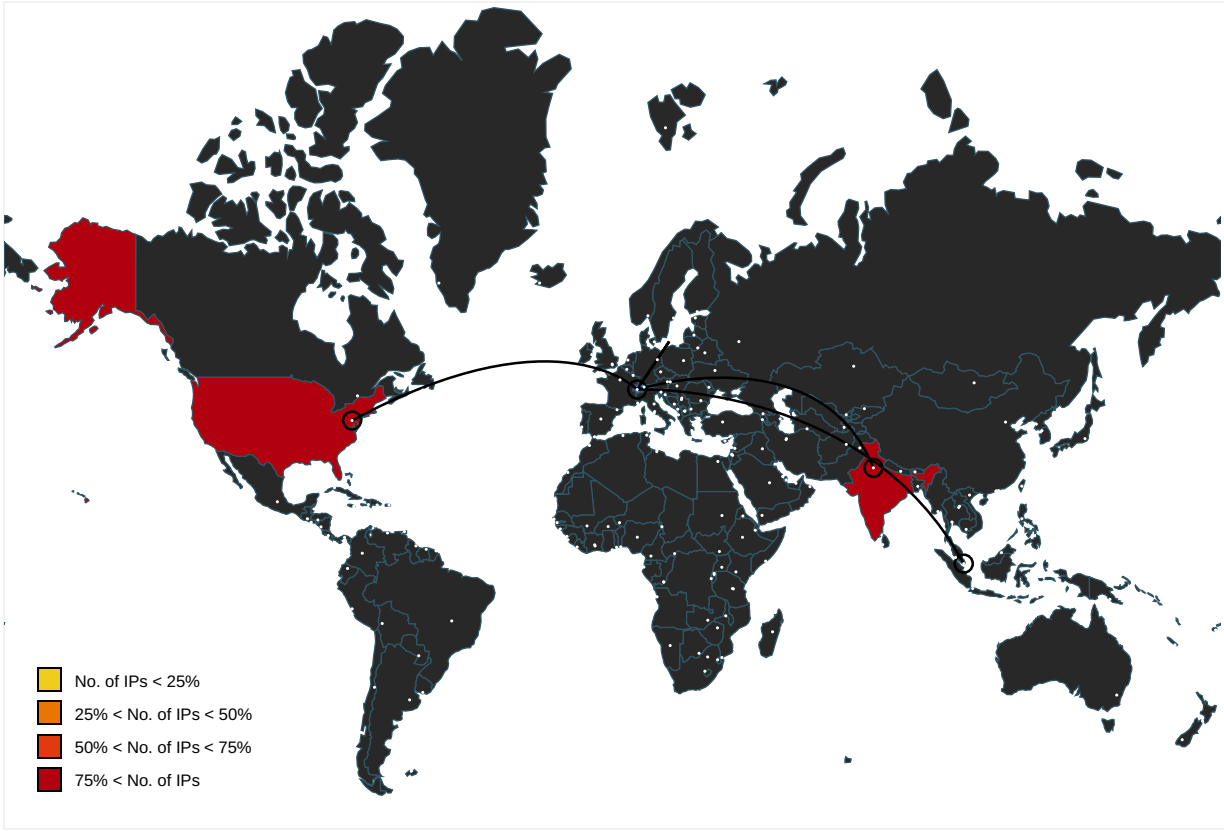
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://velma-harber30ku.com/gg.gif	false	• Avira URL Cloud: safe	unknown
http://mills-skyla30ec.com/gg.gif	false	• Avira URL Cloud: safe	unknown
http://jacktech.jackindia.com/ds/0204.gif	false	• Avira URL Cloud: safe	unknown
http://moumitas.com/ds/0204.gif	false	• Avira URL Cloud: safe	unknown
http://laura9630fr.com/gg.gif	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://servername/isapibackend.dll	regsvr32.exe, 00000003.0000000 2.2093312611.0000000001CE0000. 00000002.00000001.sdmp, regsvr 32.exe, 00000004.00000002.2093 803930.0000000001C90000.000000 02.00000001.sdmp, regsvr32.exe, 00000005.00000002.2094400807 .0000000001D80000.00000002.000 00001.sdmp, regsvr32.exe, 0000 0006.00000002.2094974245.00000 00001C80000.00000002.00000001. sdmp, regsvr32.exe, 00000007.0 0000002.2096134178.0000000001C 30000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.205.143.227	jacktech.jackindia.com	India		132335	NETWORK-LEAPSWITCH-INLeapSwitchNetworksPvtLtdIN	false
8.211.4.209	laura9630fr.com	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
74.208.236.90	moumitas.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382553
Start date:	06.04.2021
Start time:	09:47:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	12345.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:	9
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:	mal72.expl.evad.winXLSM@11/10@5/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 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 • VT rate limit hit for: /opt/package/joesandbox/database/analysis/382553/sample/12345.xlsm

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.205.143.227	documents-748443571.xlsm	Get hash	malicious	Browse	• jacktech.jackindia.com/ds/0204.gif
	documents-1887159634.xlsm	Get hash	malicious	Browse	• jacktech.jackindia.com/ds/0204.gif
	documents-683917632.xlsm	Get hash	malicious	Browse	• jacktech.jackindia.com/ds/0204.gif
	documents-683917632.xlsm	Get hash	malicious	Browse	• jacktech.jackindia.com/ds/0204.gif
	documents-1760163871.xlsm	Get hash	malicious	Browse	• jacktech.jackindia.com/ds/0204.gif
	documents-1760163871.xlsm	Get hash	malicious	Browse	• jacktech.jackindia.com/ds/0204.gif
8.211.4.209	documents-1887159634.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif
	documents-748443571.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	documents-1887159634.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif
	documents-683917632.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif
	documents-683917632.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif
	documents-1760163871.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif
	documents-1760163871.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif
74.208.236.90	documents-1887159634.xlsm	Get hash	malicious	Browse	• moumitas.com/ds/0204.gif
	documents-748443571.xlsm	Get hash	malicious	Browse	• moumitas.com/ds/0204.gif
	documents-1887159634.xlsm	Get hash	malicious	Browse	• moumitas.com/ds/0204.gif
	documents-683917632.xlsm	Get hash	malicious	Browse	• moumitas.com/ds/0204.gif
	documents-683917632.xlsm	Get hash	malicious	Browse	• moumitas.com/ds/0204.gif
	documents-1760163871.xlsm	Get hash	malicious	Browse	• moumitas.com/ds/0204.gif
	documents-1760163871.xlsm	Get hash	malicious	Browse	• moumitas.com/ds/0204.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
laura9630fr.com	documents-748443571.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1887159634.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-683917632.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-683917632.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 8.211.4.209
moumitas.com	documents-748443571.xlsm	Get hash	malicious	Browse	• 74.208.236.90
	documents-1887159634.xlsm	Get hash	malicious	Browse	• 74.208.236.90
	documents-683917632.xlsm	Get hash	malicious	Browse	• 74.208.236.90
	documents-683917632.xlsm	Get hash	malicious	Browse	• 74.208.236.90
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 74.208.236.90
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 74.208.236.90
jacktech.jackindia.com	documents-748443571.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-1887159634.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-683917632.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-683917632.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 103.205.143.227
velma-harber30ku.com	documents-748443571.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1887159634.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-683917632.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-683917632.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 8.211.4.209
mills-skyla30ec.com	documents-748443571.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1887159634.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-683917632.xlsm	Get hash	malicious	Browse	• 8.211.4.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	documents-683917632.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 8.211.4.209

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	documents-1887159634.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-748443571.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1887159634.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	L87N50MbDG.exe	Get hash	malicious	Browse	• 8.209.67.151
	documents-683917632.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-683917632.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	Proforma invoice.doc	Get hash	malicious	Browse	• 47.244.190.114
	yPkfbflyoh.exe	Get hash	malicious	Browse	• 8.208.95.18
	4CwmE1pYh5.exe	Get hash	malicious	Browse	• 47.91.72.80
	com.multicamera.coolwending.translator.apk	Get hash	malicious	Browse	• 47.253.30.230
	JYDy1dAHdW.exe	Get hash	malicious	Browse	• 8.208.95.18
	EppTbowa74.exe	Get hash	malicious	Browse	• 8.208.95.18
	tcNbszVulx.exe	Get hash	malicious	Browse	• 8.208.95.18
	USHrlfZEJC.exe	Get hash	malicious	Browse	• 8.208.95.18
	Order Drawing.exe	Get hash	malicious	Browse	• 47.241.107.134
	msals.pumpl.dll	Get hash	malicious	Browse	• 8.208.95.92
	RMwfvA9kZy.exe	Get hash	malicious	Browse	• 8.210.22.196
	5zc9vbGBo3.exe	Get hash	malicious	Browse	• 8.208.95.18
NETWORK-LEAPSWITCH-INLeapSwitchNetworksPvtLtdIN	documents-1887159634.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-748443571.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-1887159634.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-683917632.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-683917632.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	ogknJKPa1C.apk	Get hash	malicious	Browse	• 43.228.237.131
	ogknJKPa1C.apk	Get hash	malicious	Browse	• 43.228.237.131
	#Ud83d#Udd04bvoneida- empirix.com iPhone 8 104 OKeep.htm	Get hash	malicious	Browse	• 103.83.192.66
	PI.exe	Get hash	malicious	Browse	• 103.250.186.101
	#Uc138#Uae08 #Uacc4#Uc0b0#Uc11c.exe	Get hash	malicious	Browse	• 103.205.143.111
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 103.250.186.248
	4vnTrjsACd.rtf	Get hash	malicious	Browse	• 103.250.186.248
	955037-012021-98_98795947.doc	Get hash	malicious	Browse	• 103.250.185.39
	FEB_2021.EXE	Get hash	malicious	Browse	• 103.250.186.248
	2S6VUd960E.exe	Get hash	malicious	Browse	• 103.250.186.248
	ZjPOfkD2zH.exe	Get hash	malicious	Browse	• 103.250.186.248
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 45.64.104.167
	NEW AGREEMENT 2021.xlsx	Get hash	malicious	Browse	• 103.250.186.248

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\699323C9.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:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBAC F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..l.S.2...Q.'C.....h}x..... .....\..N...z...._.|.....III.666...~~~..6l.Q.J...\.. m..g.h.SRR.\.p....'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]..;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GII|..2. m,,,.-[.....sr.V1..g...on.....dl.'..."[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#""h.K..K.....g.....^..w.!.$.&...7n.].F.\\\.A....6lxjj.K/.....g.....3g... ...f....:t..s..5.C4..+W.y...88..?.,Y. .^...8{.@VN.6....Kbch.=zt...7+T....v.z....P.....VVV..."t.N.....$..Jag.v.U...P[(_.I?.9.4i.G.$U..D.....W.r.....!>|..#G...3..x.b.....P....H!.Vj .....u.2..*;..Z..c..._Ga....&L.....`.1.[.n].7..W_m..#8k...)U..L.....G..q.F.e>..s.....q....J....(.N.V...k..>m....=.).

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\761041BF.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:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.IR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. l@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7B5BE736.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:	12:6v/7aLMZ5l9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7B5BE736.png	
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.]..........O..m7.r0|..."......?A.....w..;.N1u....._[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P."......y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4AC70B4.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 364 x 139, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	8854
Entropy (8bit):	7.949751503848125
Encrypted:	false
SSDEEP:	192:VS+uZNogNC+NXtYvselFpeBnmMYCft0gVaSgZTaG+3uWYvVZmSGQ9pFT+x5ylxvr:03CbJ+mMYCmgUrNaB3uzvPm1UpFimlxj
MD5:	780FD0ABF9055E2D8FA1BAB6D4B9163E
SHA1:	CFCD5C73C9C517161DEC8D4B01ABFCA4B272AEBE
SHA-256:	6A3CDBFDB8911742673C2882E912369BC525A7BD41C9B6EFC5C9A84DAFF6C3B2
SHA-512:	8359AF512FA5771EB542B1A854F15E74555C7E1F956924520AC6CEBBAE1322D27AC8FBDD390275C5A31223613986B0CBF5871A406CA2DDBB996B9EB7A94E871A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...l.....E..7....pHYs.....tEXtSoftware.Adobe ImageReadyq.e<.."#IDATx..]M.$.u.Y...V.Z!$.....C.H2>.....JBR....c.2..k....'.f.....qg..7O.W..0.'.bO6x.. .l..#!W...`h.~.....Y...*+..._.x."....#.....[.....C.ISj..i..i.peOD..BT.N....IoD..qS..M{.I.D...!...[."A....GM.....I.M.....'T#D....&Q.H..''...Cqn"l....&.G.Mo....MI.....u&.~.#k.....R...<Q7 %o~}.$d..L..j.<l..<...N.K.M"l.aU...G,N...v....LE..Y@.l....;n.?.Z%.&.V.....,d".K^bM..B. ....B.l"l.a.....<...q...."K.....{,...j.&...F.@xU.....i.q..R.`u#<.....mR...j+ ..^.x...1TR..qw"l ....&.a.W...}v.....S.zT..a...J.0....5... E..i"l.a%..<.....lSM.a...N.....hl....."D...R.u....."Q.K.#.gM)}.L...*..b..D.y9{.kR7aA....:_..LL#.....M...).{.l..O..lv...IP0l+....Y.Y.5.....j@$.C.h !qy/.D..%...g.c...D.....X..M$O.v%Z..S.%w..1"l....B'.O.I..B..}.....iL...X..3..`[.g...j..J.'...Y...rr..@m....@.uC.#.....e!.4...M.a.y.....&h.o...Y.Q...@....N]6..."H.

C:\Users\user\AppData\Local\Temp\91DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	95644
Entropy (8bit):	7.876847080944676
Encrypted:	false
SSDEEP:	1536:m/JbW9FdM374yC2hawvTJIVseTSV7SaTe8NDUYl+LrHtlmuzx2rfg8:GJbW9FdM37OMvhnSaTDDFysE2rr
MD5:	050A914F070781F5D082643D109AC64B
SHA1:	19454C889848ACEE4AB57B46D558D9F7559057C6
SHA-256:	8F3F5D498B2A305BFC71CF3B9C36575AA534FB2B4385033DF802E0951F087B73
SHA-512:	6813F90051781DCDEE696054FC2777D5921DAE1819C67D7A25E6AC4521B81F56E6B736902416D9727F793AE5F6BB9403D552F4B6D2F1D9560539B998438A5285
Malicious:	false
Preview:	.U.N.0..#.?D....#4j.b.....mb./..h..k7.....>....."j.Zv.LX.Nz.]..wW.9.0.....Z..d...'.u....e}J.7.({.....G+.....B.E..l2..w.\.S.`._X.{....].8.k.?...T.D.FK..(.pjG.....D.`. ....&DM...R.`..^... Mm..|}?".....%..:.O*.B^9...G.....F.t-,..W.?...{.l...2-..`..Xc.....Z..=;<.T.....;$.>$../').#>.....y..m..za.....b.}S.D..x..|.f$8.....1.^DP...t...^s..PQ<f.|.....c.4.n..H.4.....=.]."..4l....U...q.. ..y.+P{.yy.....PK.....!...`.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\12345.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 14:08:15 2020, mtime=Tue Apr 6 15:47:39 2021, atime=Tue Apr 6 15:47:39 2021, length=95644, window=hide
Category:	dropped
Size (bytes):	1984
Entropy (8bit):	4.515851448728121
Encrypted:	false
SSDEEP:	48:8ufc/XT0jFt1QBaQh2ufc/XT0jFt1QBaQ/:8r/XojFtuBaQh2r/XojFtuBaQ/
MD5:	A42E1B2F2EB49399030FF949E1FD9AA7
SHA1:	E549D5FDAB738F24C17AEC23D61D65C03095C78D
SHA-256:	B9565B4E5D4619DA0F545F7B203C1E02D4C42DDAE508CC6E7CF4C9BF04C95921
SHA-512:	253ED6013AD30706BC834C52325F2DA74316EDF5AE423CD32796A43DE039D97F70138F9A5AA85E97CBE4658EBDBE617E600833EF9998DB421C68B30DF618938
Malicious:	false
Preview:	L.....F.... ...jK.{.....+.....+...u.....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..u...R. .12345~1.XLS.B.....Q.y.Q.y*...8.....1.2.3.4.5...x.l.s.m.....t.....-...8...[.....?J.....C:\Users\..#.....\\830021\Users.user\Desktop\12345.xlsm.!.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.1.2.3.4.5...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.....830021.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L.....

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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Tue Apr 6 15:47:39 2021, atime=Tue Apr 6 15:47:39 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.477827899747489
Encrypted:	false
SSDEEP:	12:85QpCfsfsCLgXg/XAlCPCHaXtB8XzB/6MExX+Wnicvb3bDtZ3YilMMEpxRljKg1x:85akU/XTd6jcxYefDv3qXqrNru/
MD5:	17C5ED0D3A4A2A9F20A997F68242EE84
SHA1:	82196D6FC7570C3DE1D7614294EB4F3B70330846
SHA-256:	44E7F9FEBF8656BFE856E002228F3D57C23D2CE704C1235D25F4FA3C8ECA0A5D
SHA-512:	B3FEF15814C7CAEC05C27AE9358CD1780E8241F26B51C4DACECED0963C7893C626C60F9BBDD1DC1EA3C5E9AA03347577A361090F80CFD801408E8411A7A110 6
Malicious:	false
Preview:	L.....F.....7G.....+.....+...0.....i....P.O. .:i....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....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\..#.....\\830021\Users.user\Desktop.....\....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....830021.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	70
Entropy (8bit):	4.450013373778756
Encrypted:	false
SSDEEP:	3:oyBVomxW/LprXC3QLprXCmxW/LprXCv:djALBIQLB+LBs
MD5:	8D90BE2693870D9F8B85B2F981628B31
SHA1:	F1EA8A5440EFA7E99E91415481FC9DD89EF0D2E7
SHA-256:	AD0BDAAB996D0966EF9B85AED4713407724A2889AB06755E43E76103570E7AC9
SHA-512:	7BE5A626FC0670A5A6BD1B3A50359072D9806736816FFFF0FF25CA244BC931AA5EF4D3B751081202FEAA863AC4A2C6551CF528965DFD7152125C8CABE01609B4
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..12345.LNK=0..12345.LNK=0..[misc]..12345.LNK=0..

C:\Users\user\Desktop\A2DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	95644
Entropy (8bit):	7.876847080944676
Encrypted:	false
SSDEEP:	1536:m/JbW9FdM374yC2hawvTJIVseTSV7SaTe8NDUYl+LrHtlmuzx2rfg8:GJbW9FdM37OMvhnSaTDDFysE2rr
MD5:	050A914F070781F5D082643D109AC64B
SHA1:	19454C889848ACEE4AB57B46D558D9F7559057C6
SHA-256:	8F3F5D498B2A305BFC71CF3B9C36575AA534FB2B4385033DF802E0951F087B73
SHA-512:	6813F90051781DCDEE696054FC2777D5921DAE1819C67D7A25E6AC4521B81F56E6B736902416D9727F793AE5F6BB9403D552F4B6D2F1D9560539B998438A5285
Malicious:	false
Preview:	.U.N.0..#.?D....#4j.b.....mb./..h..k7.....>....."j.Zv.LX.Nz.]..wW.9.0.....Z..d...'.u....e}J.7.({.....G+.....B.E..l2..w.\.S.`.._X.{....].8.k.?...T.D.FK..(.pjG.....D.`. ....&DM...R.`..^...Mm..]}?"....%..:.O*.B^9...G.....F.t-,..W.?...{.l...2-..`..Xc.....Z..=;<.T.....;$.>$../').#>.....y..m..za.....b.}S.D..x..|.f$8.....1.^DP...t...^s..PQ<f.|.....c.4.n..H.4.....=.].".4l....U...q..y.+P{.yy.....PK.....!...`.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$12345.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\~$12345.xlsm	
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.884862176121338
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	12345.xlsm
File size:	95672
MD5:	5851c6423d6cffdbfdd9ce4276592acb
SHA1:	8992a00647a35e67a887127b5aa7269cc9c597c6
SHA256:	a7893081be92e7c0c1672482df252f282abca98ff09ff559f246bcc5244d74c3
SHA512:	8a9510adb6020f887e4fa134fe8dc9df394bf055a7c596057ca92e582f72508da624c8072ad73488d8112b402360fcc4d1e4c381ecd247c06b450c17fcd737f3
SSDEEP:	1536:Qb/ndoJz+kgpei9EM5fybX8dz+HAITWPtsmLMWzMNFOfhOJYS6xybsD9fe2hawZ+:QbpJ5fybX8dz+HzT0s+MWzYoUJixzWMo
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 "12345.xlsm"

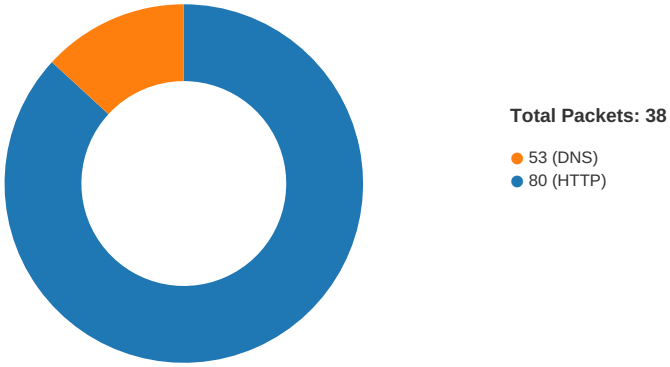
Indicators

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:48:01.163120031 CEST	49165	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:01.201642990 CEST	80	49165	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:01.201731920 CEST	49165	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:01.202414036 CEST	49165	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:01.283674955 CEST	80	49165	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:01.613493919 CEST	80	49165	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:01.613579035 CEST	80	49165	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:01.613660097 CEST	49165	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:01.613713026 CEST	49165	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:01.613914967 CEST	49165	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:01.652276993 CEST	80	49165	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:01.682090998 CEST	49166	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:01.720725060 CEST	80	49166	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:01.720828056 CEST	49166	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:01.721354961 CEST	49166	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:01.803678989 CEST	80	49166	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:02.127644062 CEST	80	49166	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:02.127686024 CEST	80	49166	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:02.127845049 CEST	49166	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:02.128031969 CEST	49166	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:02.166296005 CEST	80	49166	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:02.482728004 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:02.521353960 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:02.521567106 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:02.522023916 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:02.603694916 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:02.928333998 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:02.928371906 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:02.928489923 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:02.928627968 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 6, 2021 09:48:02.967076063 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 6, 2021 09:48:03.003235102 CEST	49168	80	192.168.2.22	74.208.236.90
Apr 6, 2021 09:48:03.161860943 CEST	80	49168	74.208.236.90	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:48:03.161964893 CEST	49168	80	192.168.2.22	74.208.236.90
Apr 6, 2021 09:48:03.162693024 CEST	49168	80	192.168.2.22	74.208.236.90
Apr 6, 2021 09:48:03.321307898 CEST	80	49168	74.208.236.90	192.168.2.22
Apr 6, 2021 09:48:03.409498930 CEST	80	49168	74.208.236.90	192.168.2.22
Apr 6, 2021 09:48:03.409692049 CEST	49168	80	192.168.2.22	74.208.236.90
Apr 6, 2021 09:48:03.410177946 CEST	49168	80	192.168.2.22	74.208.236.90
Apr 6, 2021 09:48:03.415561914 CEST	80	49168	74.208.236.90	192.168.2.22
Apr 6, 2021 09:48:03.415684938 CEST	49168	80	192.168.2.22	74.208.236.90
Apr 6, 2021 09:48:03.569153070 CEST	80	49168	74.208.236.90	192.168.2.22
Apr 6, 2021 09:48:03.569214106 CEST	49168	80	192.168.2.22	74.208.236.90
Apr 6, 2021 09:48:03.841801882 CEST	49169	80	192.168.2.22	103.205.143.227
Apr 6, 2021 09:48:04.034101963 CEST	80	49169	103.205.143.227	192.168.2.22
Apr 6, 2021 09:48:04.034275055 CEST	49169	80	192.168.2.22	103.205.143.227
Apr 6, 2021 09:48:04.034775972 CEST	49169	80	192.168.2.22	103.205.143.227
Apr 6, 2021 09:48:04.226507902 CEST	80	49169	103.205.143.227	192.168.2.22
Apr 6, 2021 09:48:04.761071920 CEST	80	49169	103.205.143.227	192.168.2.22
Apr 6, 2021 09:48:04.761336088 CEST	49169	80	192.168.2.22	103.205.143.227
Apr 6, 2021 09:48:15.172677040 CEST	80	49169	103.205.143.227	192.168.2.22
Apr 6, 2021 09:48:15.172846079 CEST	49169	80	192.168.2.22	103.205.143.227
Apr 6, 2021 09:50:00.743765116 CEST	49169	80	192.168.2.22	103.205.143.227
Apr 6, 2021 09:50:01.241911888 CEST	49169	80	192.168.2.22	103.205.143.227
Apr 6, 2021 09:50:02.209271908 CEST	49169	80	192.168.2.22	103.205.143.227
Apr 6, 2021 09:50:04.143825054 CEST	49169	80	192.168.2.22	103.205.143.227
Apr 6, 2021 09:50:07.997279882 CEST	49169	80	192.168.2.22	103.205.143.227

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:48:00.806061029 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 6, 2021 09:48:01.147500992 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 6, 2021 09:48:01.625456095 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 6, 2021 09:48:01.679797888 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 6, 2021 09:48:02.142688036 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 6, 2021 09:48:02.480325937 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 6, 2021 09:48:02.946787119 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 6, 2021 09:48:03.001132965 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 6, 2021 09:48:03.421154022 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 6, 2021 09:48:03.839102030 CEST	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 6, 2021 09:48:00.806061029 CEST	192.168.2.22	8.8.8.8	0x73f5	Standard query (0)	velma-harber30ku.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:48:01.625456095 CEST	192.168.2.22	8.8.8.8	0x8296	Standard query (0)	laura9630fr.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:48:02.142688036 CEST	192.168.2.22	8.8.8.8	0x15d4	Standard query (0)	mills-skyla30ec.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:48:02.946787119 CEST	192.168.2.22	8.8.8.8	0xccae	Standard query (0)	moumitas.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:48:03.421154022 CEST	192.168.2.22	8.8.8.8	0x887e	Standard query (0)	jacktech.jackindia.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2021 09:48:01.147500992 CEST	8.8.8.8	192.168.2.22	0x73f5	No error (0)	velma-harber30ku.com		8.211.4.209	A (IP address)	IN (0x0001)
Apr 6, 2021 09:48:01.679797888 CEST	8.8.8.8	192.168.2.22	0x8296	No error (0)	laura9630fr.com		8.211.4.209	A (IP address)	IN (0x0001)
Apr 6, 2021 09:48:02.480325937 CEST	8.8.8.8	192.168.2.22	0x15d4	No error (0)	mills-skyla30ec.com		8.211.4.209	A (IP address)	IN (0x0001)
Apr 6, 2021 09:48:03.001132965 CEST	8.8.8.8	192.168.2.22	0xccae	No error (0)	moumitas.com		74.208.236.90	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2021 09:48:03.839102030 CEST	8.8.8.8	192.168.2.22	0x887e	No error (0)	jacktech.jackindia.com		103.205.143.227	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- velma-harber30ku.com
- laura9630fr.com
- mills-skyla30ec.com
- moumitas.com
- jacktech.jackindia.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	8.211.4.209	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 6, 2021 09:48:01.202414036 CEST	0	OUT	GET /gg.gif HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: velma-harber30ku.com Connection: Keep-Alive
Apr 6, 2021 09:48:01.613493919 CEST	1	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 06 Apr 2021 07:48:01 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Length: 74 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 2e 3c 2f 68 31 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 67 67 2e 67 69 66 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e Data Ascii: Not Found. The requested URL /gg.gif was not found on this server.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	8.211.4.209	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 6, 2021 09:48:01.721354961 CEST	2	OUT	GET /gg.gif HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: laura9630fr.com Connection: Keep-Alive
Apr 6, 2021 09:48:02.127644062 CEST	2	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 06 Apr 2021 07:48:01 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Length: 74 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 2e 3c 2f 68 31 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 67 67 2e 67 69 66 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e Data Ascii: Not Found. The requested URL /gg.gif was not found on this server.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	8.211.4.209	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 6, 2021 09:48:02.522023916 CEST	3	OUT	GET /gg.gif HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: mills-skyla30ec.com Connection: Keep-Alive
Apr 6, 2021 09:48:02.928333998 CEST	3	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 06 Apr 2021 07:48:02 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Length: 74 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 2e 3c 2f 68 31 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 67 67 2e 67 69 66 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e Data Ascii: Not Found. The requested URL /gg.gif was not found on this server.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	74.208.236.90	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 6, 2021 09:48:03.162693024 CEST	4	OUT	GET /ds/0204.gif HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: moumitas.com Connection: Keep-Alive
Apr 6, 2021 09:48:03.409498930 CEST	5	IN	HTTP/1.1 503 Service Unavailable Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=15 Date: Tue, 06 Apr 2021 07:48:03 GMT Server: Apache X-Powered-By: PHP/7.3.27 Data Raw: 34 66 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 2e 3c 2f 68 31 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 64 73 2f 30 32 30 34 2e 67 69 66 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 0d 0a Data Ascii: 4f Not Found. The requested URL /ds/0204.gif was not found on this server.

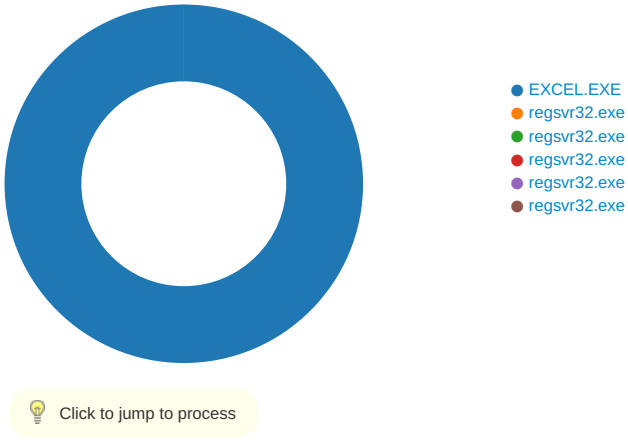
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49169	103.205.143.227	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 6, 2021 09:48:04.034775972 CEST	6	OUT	GET /ds/0204.gif HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: jacktech.jackindia.com Connection: Keep-Alive
Apr 6, 2021 09:48:04.761071920 CEST	6	IN	HTTP/1.1 503 Service Unavailable Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Content-Length: 97 Content-Encoding: gzip Vary: Accept-Encoding Date: Tue, 06 Apr 2021 07:48:03 GMT Server: LiteSpeed Data Raw: 1f 8b 08 00 00 00 00 00 03 b3 c9 30 b4 f3 cb 2f 51 70 cb 2f cd 4b d1 b3 d1 cf 30 b4 0b c9 48 55 28 4a 2d 2c 4d 2d 2e 49 4d 51 08 0d f2 51 d0 4f 29 d6 37 30 32 30 d1 4b cf 4c 53 28 4f 2c 56 c8 cb 2f 51 48 03 e9 50 c8 cf 53 28 c9 c8 2c 56 28 4e 2d 2a 4b 2d d2 03 00 b3 0a 0e ff 4f 00 00 00 Data Ascii: 0/Qp/K0HU(J-,M-.IMQQO)7020KLS(O,V/QHPS(,V(N-*K-O

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2308 Parent PID: 584

General

Start time:	09:47:36
Start date:	06/04/2021
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:	0x13fcf0000
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\D01B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14003EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\91DE0000	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\~$12345.xlsm	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FEEABB9AC0	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A2DE0000	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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140A1828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140A1828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140A1828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140A1828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140A1828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140A1828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140A1828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140A1828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140A1828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\6C0D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14003EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D01B.tmp	success or wait	1	1402AB818	DeleteFileW
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\image013.pn~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEABB9AC0	unknown

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\6C0D.tmp	success or wait	1	1402AB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\91DE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\Desktop\A2DE0000	C:\Users\user\Desktop\12345.xlsm.	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	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.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.png	C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~s~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.png	C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~s~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.png	C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~s~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.png	C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~s~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.png	C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~s~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image018.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image018.pngss	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image019.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image019.pngss	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image020.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image020.pngss	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image021.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image021.pngss	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image022.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image022.pngss	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_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\~$12345.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	13FF3F526	WriteFile
C:\Users\user\Desktop\~$12345.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	13FF3F591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\91DE0000	569	440	c4 55 cb 4e e3 30 14 dd 23 cd 3f 44 de 8e 12 17 16 23 34 6a ca 62 06 96 0c 12 cc 07 b8 f6 6d 62 d5 2f f9 1a 68 ff 9e 6b 37 14 a8 da 06 04 12 9b 3e e2 9c a7 e3 9b e9 c5 ca 9a ea 01 22 6a ef 5a 76 da 4c 58 05 4e 7a a5 5d d7 b2 ff 77 57 f5 39 ab 30 09 a7 84 f1 0e 5a b6 06 64 17 b3 1f 27 d3 bb 75 00 ac 08 ed b0 65 7d 4a e1 37 e7 28 7b b0 02 1b 1f c0 d1 ca c2 47 2b 12 fd 8d 1d 0f 42 2e 45 07 fc 6c 32 f9 c5 a5 77 09 5c aa 53 e6 60 b3 e9 5f 58 88 7b 93 aa cb 15 5d de 38 99 6b c7 aa 3f 9b fb b2 54 cb 44 08 46 4b 91 c8 28 7f 70 6a 47 a4 f6 8b 85 96 a0 bc bc b7 44 dd 60 88 20 14 f6 00 c9 9a 26 44 4d 8a f1 16 52 a2 60 c8 f8 5e cd e0 ba 1d 4d 6d b3 e7 7c 7d 3f 22 82 c1 1d c8 88 cd a1 87 86 90 25 0a f6 3a e0 4f 2a eb 80 42 5e 39 dc c3 80 fb 47 1b 18 b5 82 ea 46 c4 74	.U.N.0..#.?D.....#4j.b........ mb./..h..k7.......>........... "j.Zv.LX.Nz.]...wW.9.0.....Z. .d...'..u.....e}J.7.({........G +.....B.E..l2...w.\.S.`.._X.{. ...].8.k..?...T.D.FK..(.pjG... ......D.`. .....&DM...R.`..^.. ..Mm..|}?"..........%..:.O*..B ^9....G.....F.t	success or wait	34	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\91DE0000	1009	2	03 00	..	success or wait	20	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\91DE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 d0 f2 60 80 ba 01 00 00 8f 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	24	7FEEABB9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\91DE0000	35355	8854	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 6c 00 00 00 8b 08 06 00 00 00 45 a9 a3 37 00 00 00 09 70 48 59 73 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 22 23 49 44 41 54 78 da ec 5d 4d 88 24 c9 75 8e 59 86 d5 0a 56 ee 5a 21 24 c3 9a ed 1a cb 7f e0 43 d7 48 32 3e f8 d0 d9 c8 f6 4a 42 52 d7 80 84 f0 c5 9d 63 0c 32 fe a1 6b 8d 11 06 81 27 fb 66 9f a6 06 db 02 83 71 67 cb 7f 37 4f b6 57 d8 bb e8 30 d9 27 eb 62 4f 36 78 05 fe 9d 6c c9 17 23 21 57 83 85 f6 60 68 e7 ab 7e d1 1d 13 1d ff 19 59 bf ef 83 a0 7f 2a 2b f3 e5 8b 17 5f bc 78 f1 22 e2 d6 c5 c5 05 23 10 08 dd e0 d6 ad 5b bd e6 c7 00 0b fc de c7 a2 43 d5 94 49 53 6a f8 bd 69 9f 15	.PNG........IHDR...l.........E ..7....pHYs.................tE XtSoftware.Adobe ImageReadyq.e <.."#IDATx..]M.$.u.Y...V.Z! $.. .....C.H2>.....JBR......c.2..k ....'.f......qg..7O.W...0.'.bO 6x...l..#!W...`h..~......Y.... .*+...._.x."......#......[..... ....C..ISj..i..	success or wait	4	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Temp\91DE0000	93923	1721	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 d0 f2 60 80 ba 01 00 00 8f 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 00 00 f3 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 eb 32 5d dc 26 01 00 00 d3 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 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 3e e0 bd 9e bd 01 00 00 00 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7f 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..-.........!..2].&....... ....xl/_rels/wor kbook.xml.relsPK..-.........!. >............................ xl/workbook.xml	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\Desktop\~$12345.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	13FF3F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$12345.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	13FF3F591	WriteFile
C:\Users\user\Desktop\A2DE0000	569	440	c4 55 cb 4e e3 30 14 dd 23 cd 3f 44 de 8e 12 17 16 23 34 6a ca 62 06 96 0c 12 cc 07 b8 f6 6d 62 d5 2f f9 1a 68 ff 9e 6b 37 14 a8 da 06 04 12 9b 3e e2 9c a7 e3 9b e9 c5 ca 9a ea 01 22 6a ef 5a 76 da 4c 58 05 4e 7a a5 5d d7 b2 ff 77 57 f5 39 ab 30 09 a7 84 f1 0e 5a b6 06 64 17 b3 1f 27 d3 bb 75 00 ac 08 ed b0 65 7d 4a e1 37 e7 28 7b b0 02 1b 1f c0 d1 ca c2 47 2b 12 fd 8d 1d 0f 42 2e 45 07 fc 6c 32 f9 c5 a5 77 09 5c aa 53 e6 60 b3 e9 5f 58 88 7b 93 aa cb 15 5d de 38 99 6b c7 aa 3f 9b fb b2 54 cb 44 08 46 4b 91 c8 28 7f 70 6a 47 a4 f6 8b 85 96 a0 bc bc b7 44 dd 60 88 20 14 f6 00 c9 9a 26 44 4d 8a f1 16 52 a2 60 c8 f8 5e cd e0 ba 1d 4d 6d b3 e7 7c 7d 3f 22 82 c1 1d c8 88 cd a1 87 86 90 25 0a f6 3a e0 4f 2a eb 80 42 5e 39 dc c3 80 fb 47 1b 18 b5 82 ea 46 c4 74	.U.N.0..#.?D.....#4j.b........ mb./..h..k7.......>........... "j.Zv.LX.Nz.]...wW.9.0.....Z. .d...'..u.....e}J.7.({........G +.....B.E..l2...w.\.S.`.._X.{. ...].8.k..?...T.D.FK..(.pjG... ......D.`. .....&DM...R.`..^.. ..Mm..|}?"..........%..:.O*..B ^9....G.....F.t	success or wait	34	7FEEABB9AC0	unknown
C:\Users\user\Desktop\A2DE0000	1009	2	03 00	..	success or wait	20	7FEEABB9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A2DE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 d0 f2 60 80 ba 01 00 00 8f 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	PK..........!...`............ [Content_Types].xml ... (...................................	success or wait	24	7FEEABB9AC0	unknown
C:\Users\user\Desktop\A2DE0000	35355	8854	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 6c 00 00 00 8b 08 06 00 00 00 45 a9 a3 37 00 00 00 09 70 48 59 73 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 22 23 49 44 41 54 78 da ec 5d 4d 88 24 c9 75 8e 59 86 d5 0a 56 ee 5a 21 24 c3 9a ed 1a cb 7f e0 43 d7 48 32 3e f8 d0 d9 c8 f6 4a 42 52 d7 80 84 f0 c5 9d 63 0c 32 fe a1 6b 8d 11 06 81 27 fb 66 9f a6 06 db 02 83 71 67 cb 7f 37 4f b6 57 d8 bb e8 30 d9 27 eb 62 4f 36 78 05 fe 9d 6c c9 17 23 21 57 83 85 f6 60 68 e7 ab 7e d1 1d 13 1d ff 19 59 bf ef 83 a0 7f 2a 2b f3 e5 8b 17 5f bc 78 f1 22 e2 d6 c5 c5 05 23 10 08 dd e0 d6 ad 5b bd e6 c7 00 0b fc de c7 a2 43 d5 94 49 53 6a f8 bd 69 9f 15	.PNG........IHDR...l.........E ..7....pHYs.................tE XtSoftware.Adobe ImageReadyq.e <.."#IDATx..]M.$.u.Y...V.Z! $.. .....C.H2>.....JBR......c.2..k ....'.f......qg..7O.W...0.'.bO 6x...l..#!W...`h..~......Y.... .*+...._.x."......#......[..... ....C..ISj..i..	success or wait	4	7FEEABB9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A2DE0000	93923	1721	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 d0 f2 60 80 ba 01 00 00 8f 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 00 00 f3 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 eb 32 5d dc 26 01 00 00 d3 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 19 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 3e e0 bd 9e bd 01 00 00 00 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 7f 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..-.....!..2].&..... .....xl/_rels/wor kbook.xml.relsPK..-.....!. >..... 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\E4AC70B4.png	0	8854	success or wait	2	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\761041BF.png	0	848	success or wait	2	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\699323C9.png	0	8301	success or wait	2	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7B5BE736.png	0	557	success or wait	2	7FEEABB9AC0	unknown
C:\Users\user\Desktop\12345.xlsm	unknown	8	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\Desktop\12345.xlsm	0	8	pending	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\699323C9.png	0	8301	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7B5BE736.png	0	557	success or wait	3	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\761041BF.png	0	848	success or wait	2	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4AC70B4.png	0	8854	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\699323C9.png	0	8301	success or wait	1	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7B5BE736.png	0	557	success or wait	3	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\761041BF.png	0	848	success or wait	2	7FEEABB9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4AC70B4.png	0	8854	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	4	7FEEABB9AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED05A	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED25C	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED318	success or wait	1	7FEEABB9AC0	unknown
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\F8102	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	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\F8FA2	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	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.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 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED05A	ED05A	binary	04 00 00 00 04 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 DC C1 91 8D 04 2B D7 01 5A D0 0E 00 5A D0 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	success or wait	1	7FEEABB9AC0	unknown
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	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.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 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.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\Resiliency\DocumentRecovery\ED25C	ED25C	binary	04 00 00 00 04 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 E5 ED DD 8D 04 2B D7 01 5C D2 0E 00 5C D2 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEABB9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED318	ED318	binary	04 00 00 00 04 09 00 00 21 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 31 00 32 00 33 00 34 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 C8 DF FC 8D 04 2B D7 01 18 D3 0E 00 18 D3 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	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	r78	binary	72 37 38 00 04 09 00 00 02 00 00 00 00 00 00 00 2E 00 00 00 01 00 00 00 16 00 00 00 0C 00 00 00 31 00 32 00 33 00 34 00 35 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 31 00 32 00 33 00 34 00 35 00 00 00	success or wait	1	7FEEABB9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F8102	F8102	binary	04 00 00 00 04 09 00 00 2A 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 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 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 0F D5 36 A7 04 2B D7 01 02 81 0F 00 02 81 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	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	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEABB9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEABB9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F8FA2	F8FA2	binary	04 00 00 00 04 09 00 00 2A 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 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 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 0F D5 36 A7 04 2B D7 01 A2 8F 0F 00 A2 8F 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEABB9AC0	unknown

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

Analysis Process: regsvr32.exe PID: 1476 Parent PID: 2308

General

Start time:	09:47:43
Start date:	06/04/2021
Path:	C:\Windows\System32\regsvr32.exe

Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s ..\nvcoerf.dll
Imagebase:	0xff1a0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 1820 Parent PID: 2308

General

Start time:	09:47:43
Start date:	06/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s ..\nvcoerf1.dll
Imagebase:	0xff1a0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2560 Parent PID: 2308

General

Start time:	09:47:44
Start date:	06/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s ..\nvcoerf2.dll
Imagebase:	0xff1a0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2608 Parent PID: 2308

General

Start time:	09:47:44
Start date:	06/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s ..\nvcoerf3.dll
Imagebase:	0xff1a0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2592 Parent PID: 2308

General

Start time:	09:47:44
Start date:	06/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s ..\nvcoerf4.dll
Imagebase:	0xff1a0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis