ID: 659479
Sample Name: zJ2b57acTF.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:38:37
Date: 08/07/2022
Version: 35.0.0 Citrine

Table of Contents

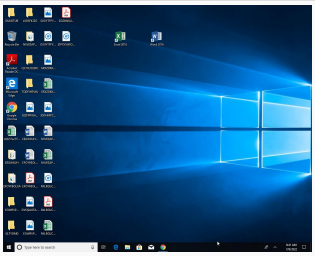
Windows Analysis Report

zJ2b57acTF.xlsx

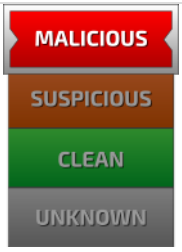
Overview

General Information

Sample Name:	zJ2b57acTF.xlsx
Analysis ID:	659479
MD5:	b8a6fb2af1f2221..
SHA1:	bc2d6b81ef00a5..
SHA256:	6d4e5e60b4f6cb..
Tags:	CVE-2022-30190 Follina xlsx
Infos:	



Detection



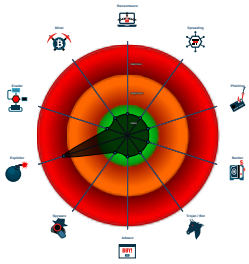
Follina CVE-2022-30190

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Microsoft Office Expl…
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 2300 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
.rels	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x1ae4:$a: PCWDiagnostic • 0x1ad8:$sa3: ms-msdt • 0x1b57:$sb3: IT_BrowseForFile=
.rels	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1ac7:$re1: location.href = "ms-msdt:
.rels	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

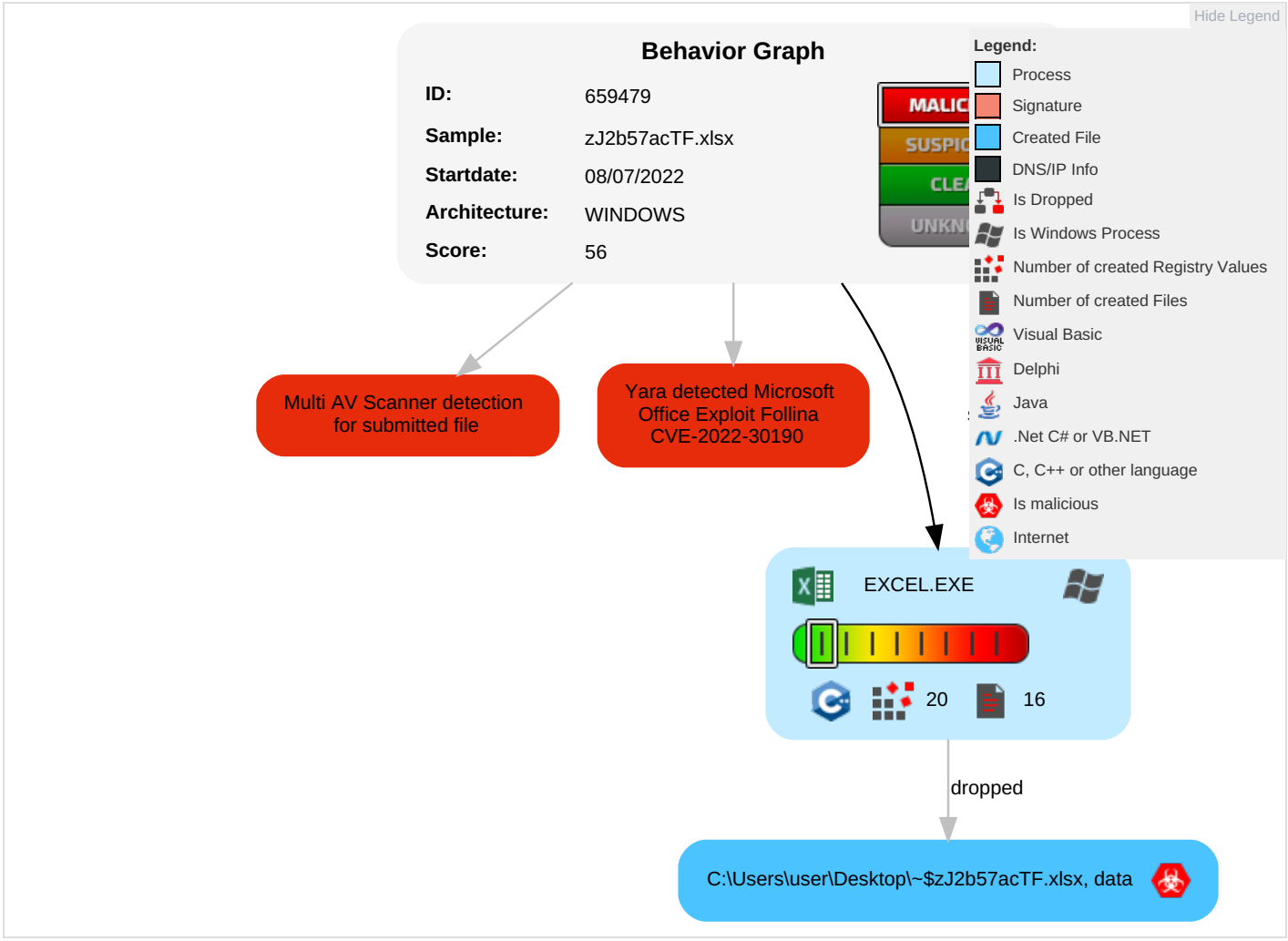
Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

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	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

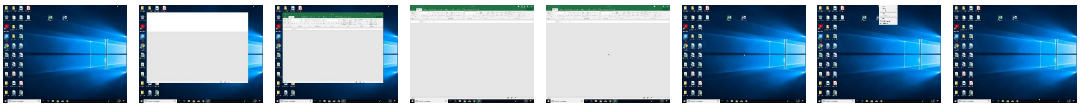
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
zJ2b57acTF.xlsx	23%	Metadefender		Browse
zJ2b57acTF.xlsx	41%	ReversingLabs	Script-JS.Exploit.CVE-2022-30190	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	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://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	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://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.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://ncus.contentsync.	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://asgsmsproxyapi.azurewebsites.net/	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	

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	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://login.microsoftonline.com/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://shell.suite.office.com:1443	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://autodiscover-s.outlook.com/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://roaming.edog.	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://cdn.entity.	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://powerlift.acompli.net	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://cortana.ai	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://api.aadrm.com/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://api.microsoftstream.com/api/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://cr.office.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://graph.ppe.windows.net	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://store.office.cn/addinstemplate	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://messaging.engagement.office.com/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://web.microsoftstream.com/video/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://dataservice.o365filtering.com/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://ncus.contentsync.	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://weather.service.msn.com/data.aspx	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://apis.live.net/v5.0/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://messaging.lifecycle.office.com/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://management.azure.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://outlook.office365.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://wus2.contentsync.	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://api.office.net	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://entitlement.diagnostics.office.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://outlook.office.com/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://outlook.office365.com/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://webshell.suite.office.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://management.azure.com/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://devnull.onenote.com	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://messaging.action.office.com/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://ncus.pagecontentsync.	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://messaging.office.com/	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high
http://https://augloop.office.com/v2	804B232B-F5B7-40B7-9B79-A747BDD996CB.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	659479
Start date and time: 08/07/202208:38:37	2022-07-08 08:38:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zJ2b57acTF.xlsx
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:	28
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:	mal56.expl.winXLSX@1/2@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xlsx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.109.76.141, 52.109.88.40, 52.109.88.39
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, arc.msn.com, ris.api.iris.microsoft.com, go.microsoft.com, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: zJ2b57acTF.xlsx

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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\804B232B-F5B7-40B7-9B79-A747BDD996CB

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):	149155
Entropy (8bit):	5.356541410467761
Encrypted:	false
SSDEEP:	1536:JcQW/gxgB5BQguw5/Q9DQC+zQWk4F77nXmvid3Xx5ETLKz6e:QJQ9DQC+zPXwI
MD5:	35706A3B22BEB1BC66FAC0E768F1D886
SHA1:	19E3DDBD78EC43E94F1FA2D45FD5155869A65699
SHA-256:	5E34998B9025FE6D4A1823AED6E957FB2F238048A54F1EEBF6B19F77652B6872
SHA-512:	EAD4360A43943E946BA8F2128E597A8C0CAE36B0C869622FB68472898E0D40EBFE1E5EAECBF55EADE629A9233DDC7711BAF8CDC12EFEF24D70C34AAF3E533342
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="2022-07-08T06:39:45">.. Build: 16.0.15505.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\Desktop\~$zJ2b57acTF.xlsx

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362C7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft OOXML
Entropy (8bit):	7.2242451103796474
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	zJ2b57acTF.xlsx
File size:	13955
MD5:	b8a6fb2af1f22213fc469b3fc7d65382
SHA1:	bc2d6b81ef00a56dc2fd13fc9a4c90a08d1a5068
SHA256:	6d4e5e60b4f6cbc8a6e14343b59c406fe5c7f948aded16d23a0f6ed6984907c2
SHA512:	3830c5a98c28dae095bd2f44bfa29e27a856f92d3fb5d71bc2170f9d2995d9eb011cea50f84c6487e63f574ae872dd49d6ef0d8b13200c08029b5604393d4c04
SSDEEP:	192:44wboitZCnzIb3UuwVemtGa4cV2s7SlUcwNClk0UNaO8Ibwiu4W8+j4sjt/siAe:44p3zI38jV2s7SluQoPKGW8q4sjFsiAe
TLSH:	39528E1AC127A03DF273807AC20929E6DD9D22079135A40FB0A0B6CD68D2BDB579F75F
File Content Preview:	PK.....e..T..7HL...5....._rels/.rels..._k.0.....}..6...n.....Z....."..Zd.H7K..w.....OC.....'.h...^...8..qE..F../.E.NK...|.....wx.V"..KSGF..s^"..BDUB%c.kp.3...H.P.Z..,@...~..%...0...y..}.F..6a...(8.jV..5G.X 8..W.z?..Hx....k.nh9.Y....X.

File Icon

Icon Hash:	74ecd0d2d6d6d0dc

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: EXCEL.EXE PID: **2300**, Parent PID: **756**

General

Target ID:	0
Start time:	08:39:42
Start date:	08/07/2022
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:	0xab0000
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 Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$zJ2b57acTF.xlsx	0	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	pratesh	success or wait	1	C151E4	WriteFile
C:\Users\user\Desktop\~$zJ2b57acTF.xlsx	55	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	pratesh	success or wait	1	C15241	WriteFile
C:\Users\user\Desktop\~$zJ2b57acTF.xlsx	0	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	pratesh	success or wait	1	C151E4	WriteFile
C:\Users\user\Desktop\~$zJ2b57acTF.xlsx	55	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	pratesh	success or wait	1	C15241	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

No disassembly