ID: 562531
Sample Name: KZ429 FEB17 BSRec_InvNet.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 01:10:37
Date: 29/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

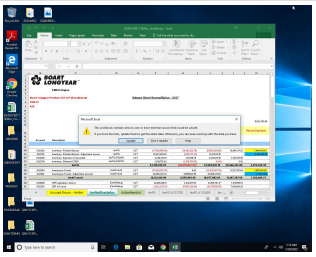
Windows Analysis Report

KZ429 FEB17 BSRec_InvNet.xlsx

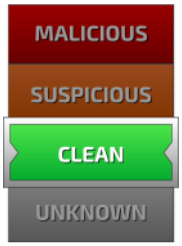
Overview

General Information

Sample Name:	KZ429 FEB17 BSRec_InvNet.xlsx
Analysis ID:	562531
MD5:	31b67f4aa8dccb…
SHA1:	ed39326058a73a.
SHA256:	4137a3675db120.
Infos:	



Detection

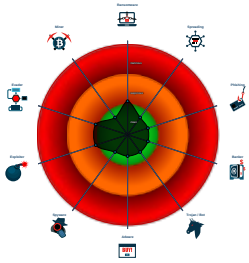


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- EXCEL.EXE (PID: 5148 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - splwow64.exe (PID: 5396 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

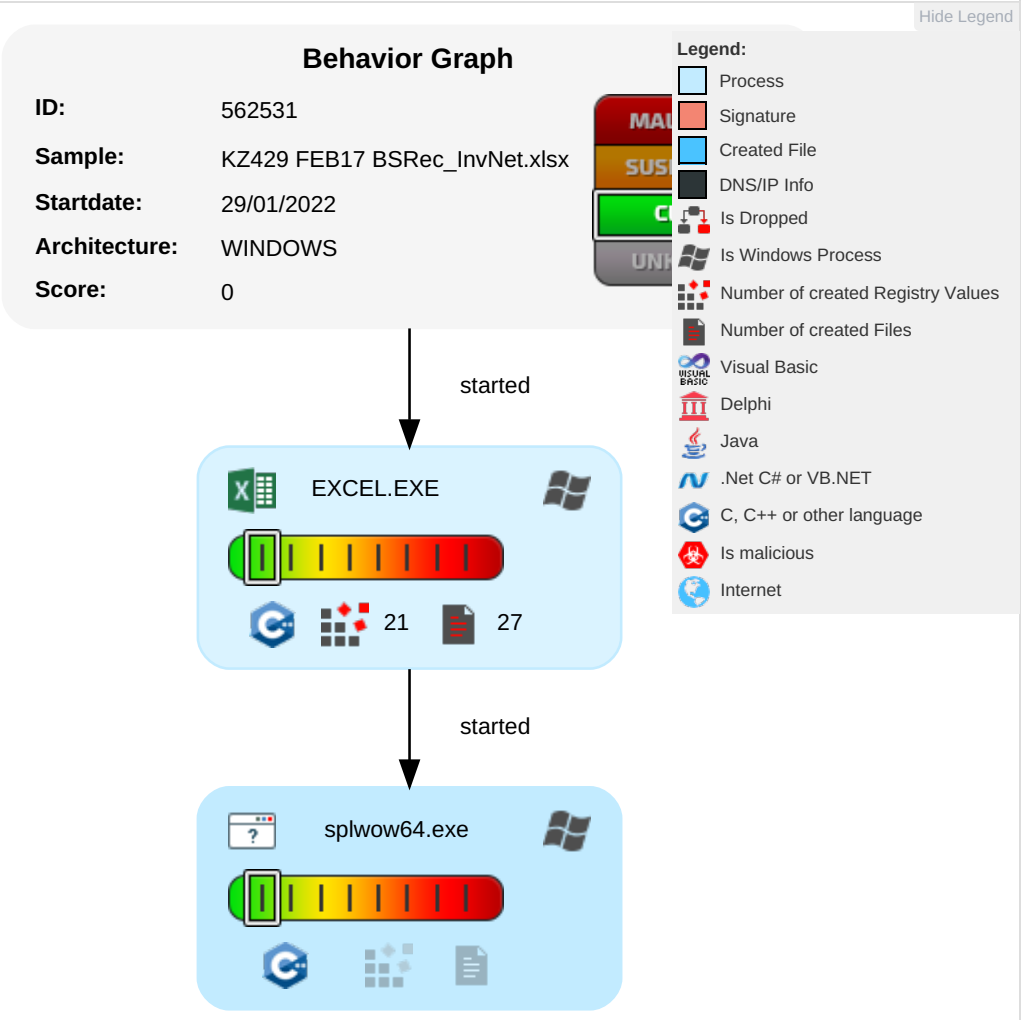
Jbx Signature Overview

There are no malicious signatures, click here to show all signatures.

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	1 Process Injection	1 Masquerading	OS Credential Dumping	1 Virtualization/Sandbox Evasion	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	1 Extra Window Memory Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	1 File and Directory 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Extra Window Memory Injection	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

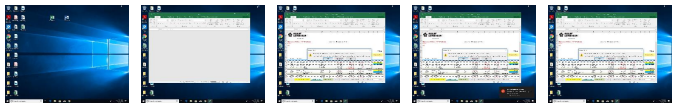
Behavior Graph

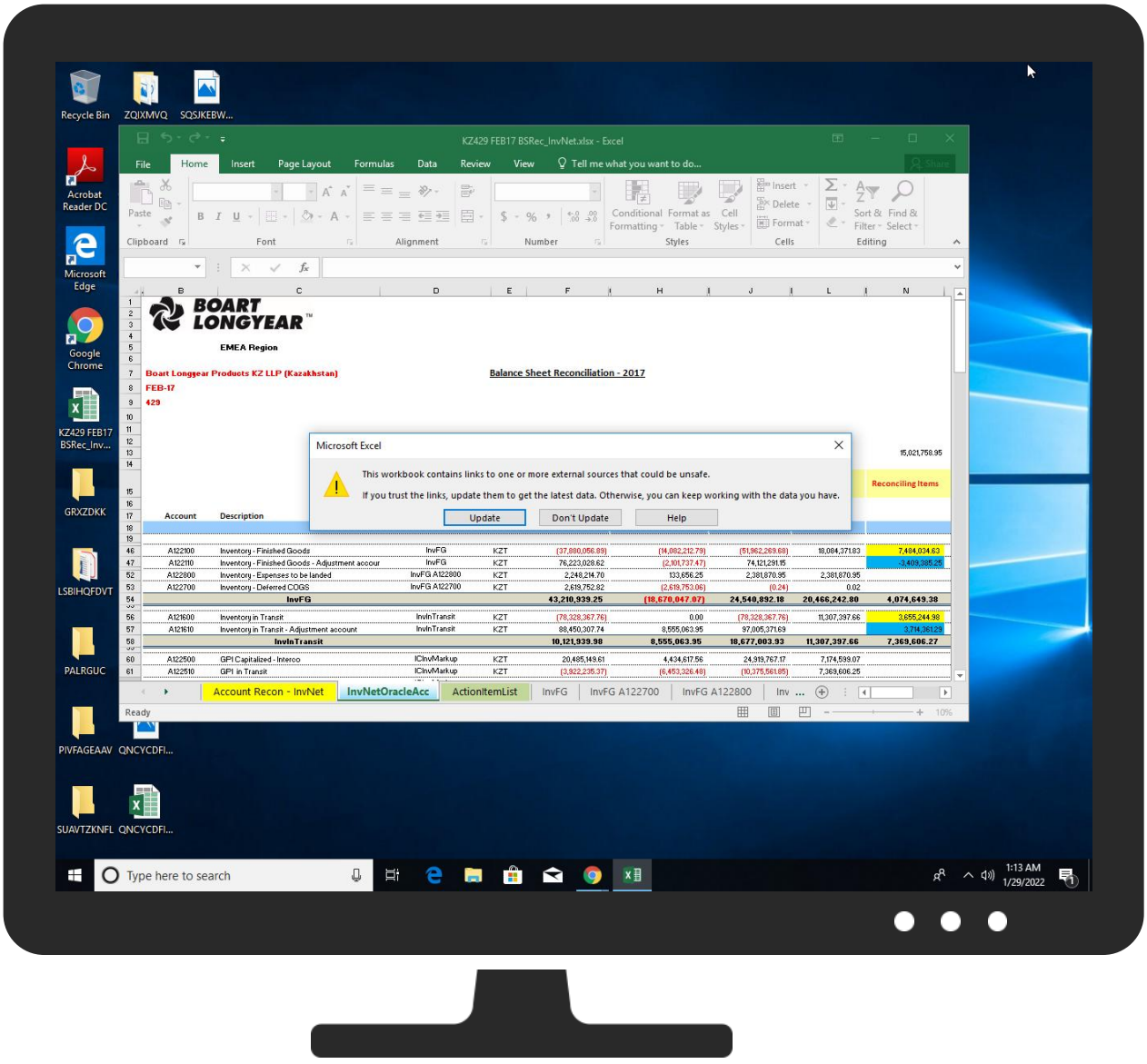


Screenshots

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://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	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.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	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://login.microsoftonline.com/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://shell.suite.office.com:1443	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://autodiscover-s.outlook.com/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://roaming.edog.	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://cdn.entity.	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://powerlift.acompli.net	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://cortana.ai	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://api.aadrm.com/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://api.microsoftstream.com/api/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://cr.office.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://graph.ppe.windows.net	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://officeci.azurewebsites.net/api/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://store.office.cn/addinstemplate	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://globaldisco.crm.dynamics.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://dev0-api.acompli.net/autodetect	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://web.microsoftstream.com/video/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://dataservice.o365filtering.com/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/autodiscover/autodiscover.json	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://ncus.contentsync.	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://weather.service.msn.com/data.aspx	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://apis.live.net/v5.0/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://management.azure.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://outlook.office365.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://wus2.contentsync.	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://api.office.net	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://incidents.diagnosticssdf.office.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://entitlement.diagnostics.office.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://substrate.office.com/search/api/v2/init	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://outlook.office.com/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://outlook.office365.com/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://webshell.suite.office.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://management.azure.com/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://devnull.onenote.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://ncus.pagecontentsync.	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://messaging.office.com/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://augloop.office.com/v2	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://skyapi.live.net/Activity/	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high
http://https://dataservice.o365filtering.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://api.cortana.ai	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com	6A9BB3D1-196A-47AF-A298-A01CBE8FC190.1.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562531
Start date:	29.01.2022
Start time:	01:10:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KZ429 FEB17 BSRec_InvNet.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:	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:	CLEAN
Classification:	clean0.winXLSX@3/8@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:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx

Warnings

- Max analysis timeout: 600s exceeded, the analysis took too long
- Exclude process from analysis (whitelisted): MpCmdRun.exe, taskhostw.exe, RuntimeBroker.exe, Microsoft.Photos.exe, backgroundTaskHost.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, MusNotifyIcon.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe

- Excluded IPs from analysis (whitelisted): 2.20.157.220, 2.20.156.69, 52.109.76.68, 52.109.8.22, 52.109.76.35
- Excluded domains from analysis (whitelisted): fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, settings-win.data.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, config.officeapps.live.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
01:11:34	API Interceptor	1x Sleep call for process: splwow64.exe modified

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\6A9BB3D1-196A-47AF-A298-A01CBE8FC190

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):	142098
Entropy (8bit):	5.354736234223517
Encrypted:	false
SSDEEP:	1536:0cQIfgxrBdA3guwQ/Q9DQW+zUk4F77nXmvidZXQE5LWmE9:48Q9DQW+zwXFU
MD5:	9FAE1B3D0F2DFFA1FC5C95CF634BF20C
SHA1:	04C5D6D0854BFC6151F519735C6232DA5D1D34AB
SHA-256:	AF5686D5BCF33D83BC238CB40B749559A2FF9D07B8FE758DFB18DC49B50FC8C9
SHA-512:	14738ED1EB913BCBD797892D0BCA382427CC433B5B7B3EFDFF55729A5257CFED6C6488C2CACDFCFBA9D4B569573019C61D71E590A8598AB987274F91974D4A16
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="2022-01-29T00:11:33">.. Build: 16.0.14923.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4C29F330.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 736 x 684, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	39836
Entropy (8bit):	7.878450113177619
Encrypted:	false
SSDEEP:	768:kR74Xfv6IM98GeWrL2PBB/HZTv4PC2zWVJVshLAw0Y7Sx:kRcXfv6HqGeA+BfmP2gL7Sx
MD5:	2E2CD6F2A3F8A14E0E8CA21FA1BB4B4B
SHA1:	198375E14FF80A94D82DC0CA20F4105DA7109344
SHA-256:	63245936D251A15D85F9CDABE06E3BB1CFEB16E9A7F02C7B72E72EB7D75B6C5A
SHA-512:	340638281E60773A893BC2508031506F3D460D846D95228096E0EADC7E18FF943C906AC1675FC15F7717CC13FD35C5C9ED955C6E26ADE8BCFBF45F338593979
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....D.....sRGB.....gAMA.....a.....pHYs.....o.d...1IDATx^.1..>....'.|b.._....H...^fw....w.9.....{P ...U$..".....".T.. .k^...7.....0..8.....@.....A..... .....0..8.....@.....x.....+s.....1.g..A...@...c .....XO.@.....]....<.....`=..y....8..t.z:...0?.p....t...`~.....3.. .....1.g..A...@...c .....XO.@.....]....<.....`=..y... .8..t.z:...0?.p....t...`~~].....>.q.ZK..y...??.....}.....?r.....-...b.~....j...o.:.vd..S...E0..{.pU.~..C...'..k.k..#..N.....T.....>#;.Q...&:.p..U.\...pO..>..%.{.^.y....>...\....I..V..N....}.....I...H.. .....a..g.....l]..U.d.wtn(._.._T....G.mx=..`~.....l!(BMD.~.d...f..V...p....}..p"Z..Y..x.K.....uZ./.....r_..!.....5....r...<.S....PVa.=}V.^...\..x.e.P...}l.mt|..6.k.p].~..C...'..k.+.."Z.0{[..... ....+..D.>3...~...I.'...q8..{.^.y....>...X.....p....c".Y..z.q..k.....^.....K.M..5m~.....<..Ot...W,.....".?..B...."`w}8.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\73004B2B.emf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	5004
Entropy (8bit):	4.880532580784114
Encrypted:	false
SSDEEP:	48:ANKfvG+H2cxp2K8R5mPK1PhfP5vVkFuGOa3GEze93tl7ykhA/XbvY+98woStReDk:gKHLYKG5mPKDRv4Og6tO/XP8lEE8
MD5:	4195D6D8FBCE413B298166FFDAB9F5C1
SHA1:	3B0AA8B2E29511492ADD852F0BE1EB48AE669EFB
SHA-256:	904460518FC5ED57981E4DABCB417DC5DBC7F155C0B76EA20D5F8DC8540F4872
SHA-512:	2874C90877A6BFB2C9EEAE01D7F628E1E8180103AB9779AB5392CB771776F20DC345C7DD811DDD84B37637B602F37DBC79461624FD502369BEBB41C28368F46
Malicious:	false
Reputation:	low
Preview:	....l.....U.../.....9...q... EMF.....8.....}.....U..H....._...5...R...p.....S.e.g.o.e. .U.l..... .....u8)..1.5.\.R.o.o.t.\.O.f.f.i.c.e.....l./..mko.....D..V.....u.>.v.....;vD./.../...../.....w.>.v8.....\...\..;v../.....Q.....@...../...w;>.v....\.\...\.h.b...../.....}\.p./...../.cnko. ...../.....8)..../..}.u.....dv.....%.....r..... .....?..... ....?.....?.....l...4..... ... ...(... ... .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\9D04752.jpeg

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 660x137, frames 3
Category:	dropped
Size (bytes):	25938
Entropy (8bit):	7.833218523254594
Encrypted:	false
SSDEEP:	768:RPdG3S2uAu5LAbvlGVzYO00pQlDSmM57dx7SiWIKLvW1:RP88Ap+cZ02kpCiWDg
MD5:	B5BB6A7EF0B322467A20AB38ABC07B97
SHA1:	47B724835E4C7B3DDB0FA32BE2D00CBFD43BADBC
SHA-256:	9CB8D86A1195C6A0C7E2B3FAE92C988BFFB85E24CD245872C543BB3B8295DCBE
SHA-512:	C90C1FF27F5179A9C3CC55C0C72E9B95377902B1F91CE216729BA9BEE899A07671506F4533D759DF3C5351B4263FCCEEA66AECE86E72E15093E361624BC4F0F A
Malicious:	false
Reputation:	low

Preview:	......JFIF.....C.....C.....".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....+3@..(..s...k....A..>.....(..M.\|- .O..M+..#B.G.7....2M.~!.....[.....O....o...9..5.....{...g.3...H.....5.c.+.....f....."k!....\|...8_.....M~..5...K$.....ZP.>X.Fd.....+@&.+.Z...&..C..W...'..._..|6+....<K.yg*t.R{}...a\....W...- ..Q.Bh.G.....X5y.T....z..?....R.....),...n...8#..N...E....F2.._..B?.....#..v.m.....5.i..7.KY..M._.v.fc.9R

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C6957DA4.emf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	5356
Entropy (8bit):	2.3433223432482677
Encrypted:	false
SSDEEP:	48:S83IHpHK2n4x//3G7+wJj7IaK0JohkN+DuuHmt:SVHpHKzx//3+xB7IaK0bNIXGt
MD5:	99A4EF14AF0ED7CC47AED67CDF9C1B6F
SHA1:	76CCECCAA04689B49FEFC31E285287A79E3C8114
SHA-256:	E8504FF99C633ADA90BC68E60C438D6A725B9EE7DDA5CA867E6D11BD47EB6412
SHA-512:	FB08FA565E155963B2A779226E58A4446C544C851616EDC402C6086D403C5BAFE958E5FF9DBC0DDEE03185F728FD6BFA38402283C3076E19F5349CE411045449
Malicious:	false
Reputation:	low
Preview:	....l.....C#..... EMF.....8.....}.....U..H.....K.....'.....%.....L...d.....!..... .....?.....?.....%.....(.....'.....%.....L...d.....!.....?.....?.....%.....(.....'..... .....%.....L...d.....!.....?.....?.....%.....(.....'.....%.....L...d.....!.....?.....?.. .....%.....(.....'.....%.....L...d.....!.....?.....?.....%.....(.....'.....%.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\DCD9B66F.emf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	5348
Entropy (8bit):	2.344745671221623
Encrypted:	false
SSDEEP:	48:SE3IHpHK2n4x//3G7+wJj7IaK0VNCedxp41:SNHpHKzx//3+xB7IaK0VUopw
MD5:	4ACCB58B65F8BF9DB41724A8DFADFD6C
SHA1:	60B13D43FE7B6A371ABCAD15764142685851AED8
SHA-256:	C43A9B6A567B16EC1A9EA2A2D2F9A451BB279422CA00D52F4A1F191499036E8F
SHA-512:	8A08A70DABB7BB49F1D3E23D0DDC79CC14869258A1371992596A9CE707334BCD921C243AAFB44BD7A1D41370C61471204072603ACA7E26B12DFB4B83446CC7A
Malicious:	false
Reputation:	low
Preview:	....l.....C#..... EMF.....8.....}.....U..H.....K.....'.....%.....L...d.....!..... .....?.....?.....%.....(.....'.....%.....L...d.....!.....?.....?.....%.....(.....'..... .....%.....L...d.....!.....?.....?.....%.....(.....'.....%.....L...d.....!.....?.....?.. .....%.....(.....'.....%.....L...d.....!.....?.....?.....%.....(.....'.....%.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EAAAB955.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 539 x 117, 1-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	1813
Entropy (8bit):	7.760708246194418
Encrypted:	false
SSDEEP:	24:/LprG0vhs2thEn3DXJamqANnRiTbPYyg5EUZEaJ5mCpL3kUGNKZK0vQYrYhWuVrB:l1KTXJaDKnRiTbP7UxHj5FxYEadD9ey
MD5:	B7CD4B4DB1368FFC7BED8E8945EA26DA
SHA1:	D2A9B1759322AA7FD625982F9BA546F8B4912515
SHA-256:	1233CE40FB6D8E7D2128FEB5B274E5369037C6CE4F05E08420EC8979FA9BE4BD
SHA-512:	04A9C57CBADF8DA660BA8F83399BAE02DCF30C7A4FAEEFBC024583DABADF7992EB87E52B3B4E6CA1978396D1A196D123D99C5AEB2C5D54C570BF5CAB4180DEAD
Malicious:	false
Reputation:	low

Preview:	.PNG.....IHDR.....u.....sRGB.....gAMA.....a.... cHRM..z&.....u0..`..:....p..Q<....PLTE.....U..~....pHYs..!...!.....IIDATh...Mn.6..p.Zp.....(G..z.....,r..]tY.YD... 3..~..}..ta.....(j8.h.....9.."3!...9.)...b...O.Y`.{f...G.. |.....8 .....F.b.3..&.>\D..H..v.v...H....~.q..]S.|....+.....xD..j. r...=w...I..+.x..... .9Ev....C...#2..Td...n!8~= ...p.A...."..4....j..".."D... \..t..N..s.G>0b.#.+./}....R.....7..m.wO.+b..p...r.-q..yC..1F]....."}j....#..D./w.6w.>pH..(<....)F|.. .!+].....pP$g.H...y.i.[.H...rI..[H.. ."_Xt..zbD... ..x@(:"....+..F.4F."....;KK.%..... 3...cC.M.2.#+b8..."{E.y...g.....6.....u....}A.....E. .....*.."b+...I.....Xo ...rzZ.^..&Bc..$.9.w7...P.-..8.Ft<EfM...;.z&ct..!{M.<.....:.~sr..M..G..9.n#.~.zD.$..!..tW.}.tC.9E..n..C..?ej...<.$).]..~.<..2..z&.H.....1K..B>A..D8.xx....vd.J~z=bx.r.....6,....s.r.m..H.!...B.%MXe..=._m.BO8~.0)..-.y.IF\.O.e.:.f-d<.2./.>.|..X....Q2.t..I..bY.4.d$.U.&#..D)...@.6.. ..)..TN. .

C:\Users\user\Desktop\~$KZ429 FEB17 BSRec_InvNet.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:	false
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.974035344901012
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	KZ429 FEB17 BSRec_InvNet.xlsx
File size:	1358015
MD5:	31b67f4aa8dccb4ed683563dbc104bd0
SHA1:	ed39326058a73ab569efa22534f79ac9ee9953e7
SHA256:	4137a3675db12038c970e56f94ce7bee7a0d920e2514eabefd9a2b28348fc9eb
SHA512:	5803da5436340626230bb4b84a862a99bb2eb4fbd71d58fccc61514c3a8d9bf395b3eea80bbbd0d5e6d8ea8eda701ced4bb0103ae148c5c72775ba7b439c6a63
SSDEEP:	24576:PU+VurG3iP/t5kHbSqE8TE6eB3PHjfQ3JGMuLH3nS0IbrEXD6Px9Z:PZgrGyn4i8G3PHjfiJgLH3n74rEmB
File Content Preview:	PK.....!..3y.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	74ecd0d2d6d6d0dc

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/562531/sample/KZ429 FEB17 BSRec_InvNet.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
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:	False

Summary	
Author:	Gut, Mateusz
Last Saved By:	Bernas, Justyna
Create Time:	2012-08-13T15:44:29Z
Last Saved Time:	2017-03-29T09:51:35Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Thumbnail Scaling Desired:	false
Company:	Boart Longyear
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	15.0300

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 76

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	76
Entropy:	3.09344952647
Base64 Encoded:	False
Data ASCII:	. . . . . F . . . . O L E P a c k a g e . . . . . P a c k a g e . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 0c 00 03 00 00 00 00 00 c0 00 00 00 00 00 00 46 0c 00 00 00 4f 4c 45 20 50 61 63 6b 61 67 65 00 00 00 00 00 08 00 00 00 50 61 63 6b 61 67 65 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x10le10Native, File Type: data, Stream Size: 91167

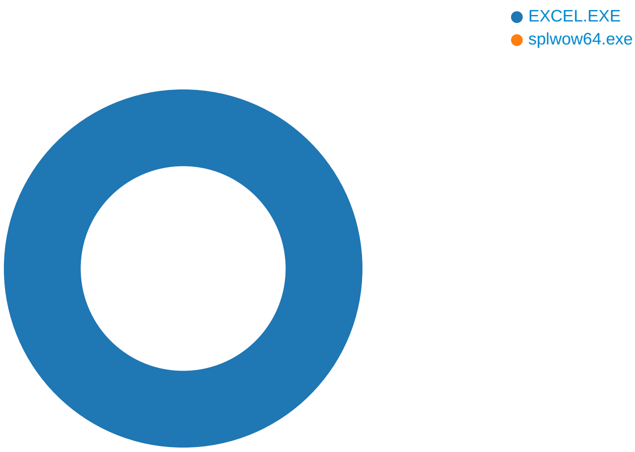
General	
Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	91167
Entropy:	4.5146051143
Base64 Encoded:	True
Data ASCII:	. d . . . . 6 0 7 9 1 F C E . m s g . C : \ \ U s e r s \ \ j u s t y n a . b e r n a s \ \ A p p D a t a \ \ L o c a l \ \ M i c r o s o f t \ \ W i n d o w s \ \ T e m p o r a r y I n t e r n e t F i l e s \ \ C o n t e n t . M S O \ \ 6 0 7 9 1 F C E . m s g . . . . . 6 . . . C : \ \ U s e r s \ \ J U S T Y N ~ 1 . B E R \ \ A p p D a t a \ \ L o c a l \ \ T e m p \ \ 6 0 7 9 1 F C E . m s g . . b . . . . . > . . . . .
Data Raw:	1b 64 01 00 02 00 36 30 37 39 31 46 43 45 2e 6d 73 67 00 43 3a 5c 55 73 65 72 73 5c 6a 75 73 74 79 6e 61 2e 62 65 72 6e 61 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 54 65 6d 70 6f 72 61 72 79 20 49 6e 74 65 72 6e 65 74 20 46 69 6c 65 73 5c 43 6f 6e 74 65 6e 74 2e 4d 53 4f 5c 36 30 37 39 31 46 43 45 2e 6d 73 67 00 00 00 03

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **5148**, Parent PID: **744**

General

Target ID:	1
Start time:	01:11:31
Start date:	29/01/2022
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:	0x1180000
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\~$KZ429 FEB17 BSRec_InvNet.xlsx	0	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	pratesh	success or wait	1	12E51E4	WriteFile
C:\Users\user\Desktop\~$KZ429 FEB17 BSRec_InvNet.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	12E5241	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

Analysis Process: splwow64.exe PID: **5396**, Parent PID: **5148**

General

Target ID:	5
Start time:	01:11:33
Start date:	29/01/2022
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff707d40000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly