ID: 562532
Sample Name: RU419 FEB17 BSRec_InvNet.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 01:20:50
Date: 29/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

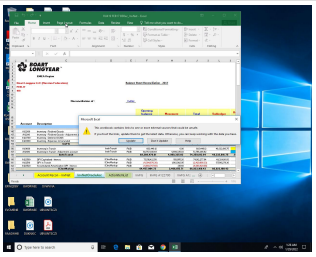
Windows Analysis Report

RU419 FEB17 BSRec_InvNet.xlsx

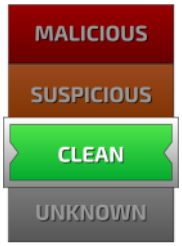
Overview

General Information

Sample Name:	RU419 FEB17 BSRec_InvNet.xlsx
Analysis ID:	562532
MD5:	bb2bdf2659b515..
SHA1:	72405dd23abe1d.
SHA256:	a36ec67f835cb7...
Infos:	



Detection

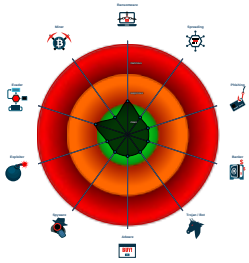


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- EXCEL.EXE (PID: 864 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - splwow64.exe (PID: 5804 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

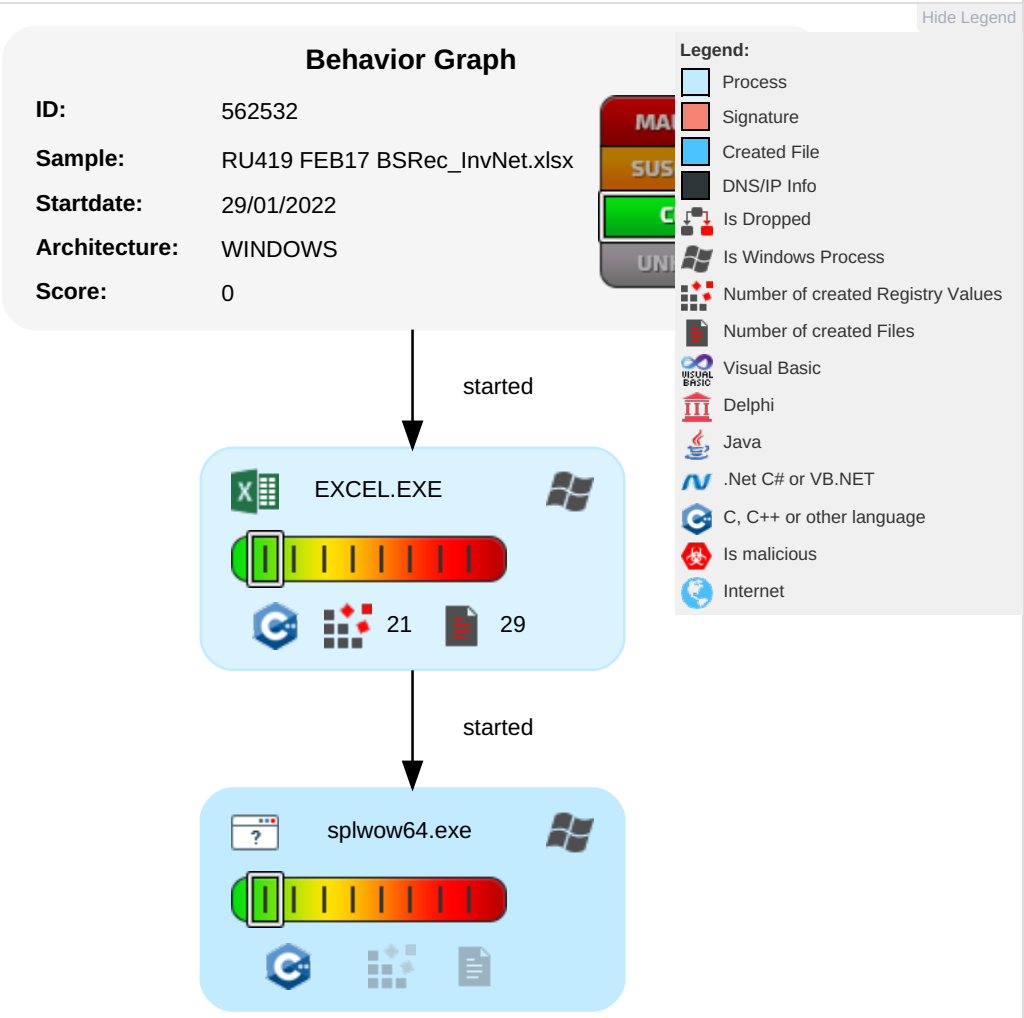
Jbx Signature Overview

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	Boot or Logon Initialization Scripts	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

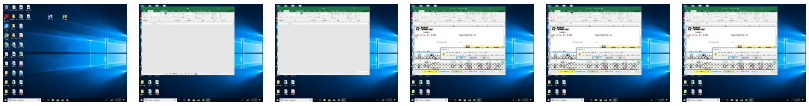
Behavior Graph

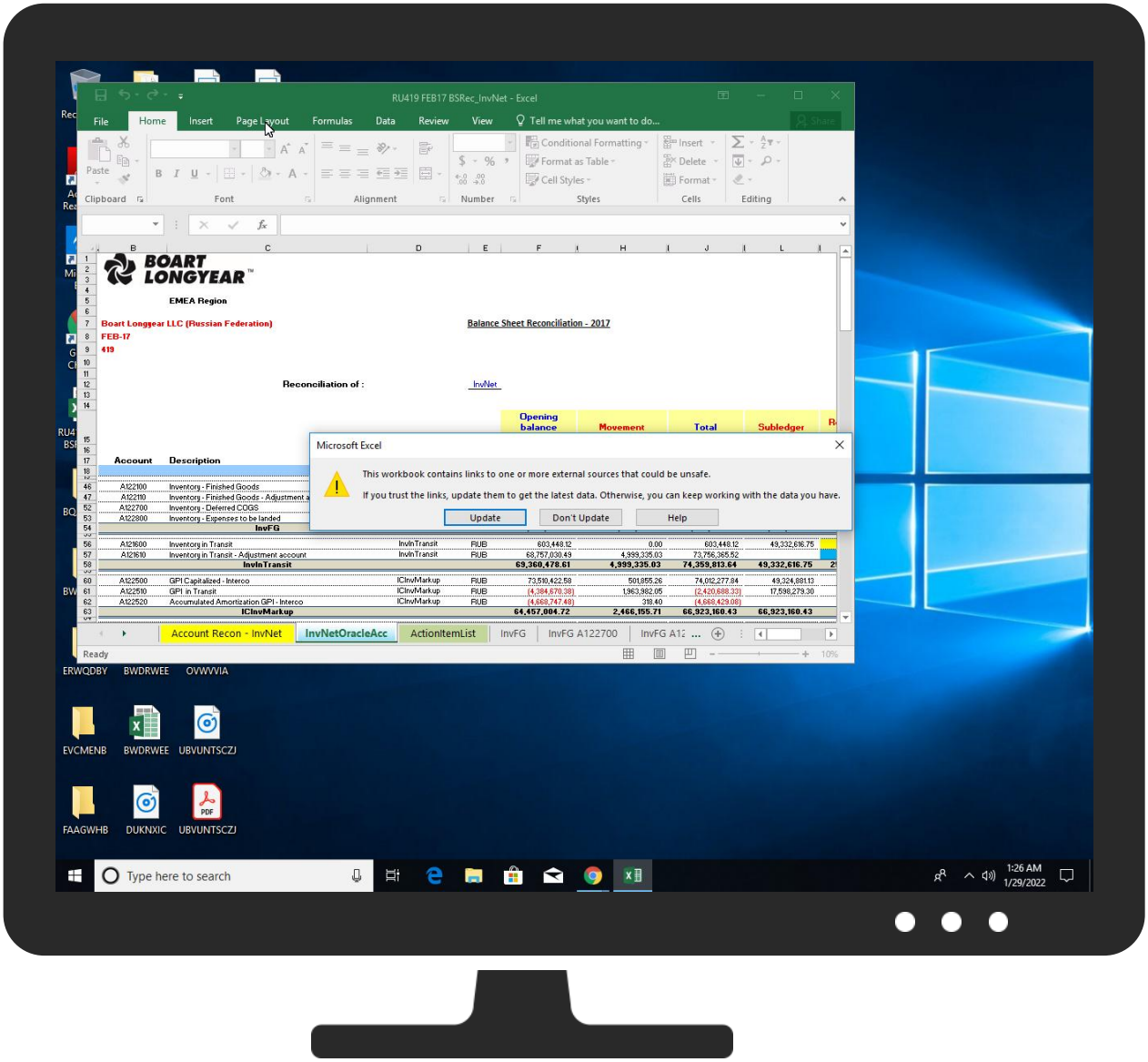


Screenshots

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://schemas.microsoft.c	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://schemas.mic-	0%	Avira URL Cloud	safe	
http://schemas.micro	0%	URL Reputation	safe	
http://www.w3.o	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	

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	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://login.microsoftonline.com/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://shell.suite.office.com:1443	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://autodiscover-s.outlook.com/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://roaming.edog.	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://cdn.entity.	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://powerlift.acompli.net	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://schemas.microsoft.c	splwow64.exe, 00000002.00000003.72715181 7.0000000002F93000.00000004.00000020.000 20000.00000000.sdmp, splwow64.exe, 00000 002.00000003.725796275.0000000002F93000. 00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000002.00000003.727939 883.0000000002F94000.00000004.00000020.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://cortana.ai	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://api.aadrm.com/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://api.microsoftstream.com/api/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://cr.office.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://graph.ppe.windows.net	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://store.office.cn/addinstemplate	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://web.microsoftstream.com/video/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://graph.windows.net	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://dataservice.o365filtering.com/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://ncus.contentsync.	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://weather.service.msn.com/data.aspx	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://apis.live.net/v5.0/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://management.azure.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://outlook.office365.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://wus2.contentsync.	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://api.office.net	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://schemas.mic-	splwow64.exe, 00000002.00000003.72715181 7.0000000002F93000.00000004.00000020.000 20000.00000000.sdmp, splwow64.exe, 00000 002.00000003.725796275.0000000002F93000. 00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000002.00000003.727939 883.0000000002F94000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://entitlement.diagnostics.office.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://schemas.micro	splwow64.exe, 00000002.00000003.75190372 5.0000000003E8D000.00000004.00000020.000 20000.00000000.sdmp, splwow64.exe, 00000 002.00000003.728110028.0000000003D8D000. 00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000002.00000003.752108 390.0000000003E94000.00000004.00000020.0 0020000.00000000.sdmp, splwow64.exe, 000 00002.00000003.728264733.0000000003D9400 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://substrate.office.com/search/api/v2/init	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://outlook.office.com/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://outlook.office365.com/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://webshell.suite.office.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://management.azure.com/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://www.w3.o	splwow64.exe, 00000002.00000003.74969636 8.000000000300C000.00000004.00000020.000 20000.00000000.sdmp, splwow64.exe, 00000 002.00000003.735988966.0000000003E5E000. 00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000002.00000003.735894 422.0000000003E5D000.00000004.00000020.0 0020000.00000000.sdmp, splwow64.exe, 000 00002.00000003.751571773.000000000300C00 0.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000002.00000003.735741916.0000 000003E57000.00000004.00000020.00020000. 00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://devnull.onenote.com	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://ncus.pagecontentsync.	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://messaging.office.com/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://augloop.office.com/v2	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false		high
http://https://skyapi.live.net/Activity/	5FA6FEA0-CB2C-4F8E-9780-03CCC61C3B5C.0.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562532
Start date:	29.01.2022
Start time:	01:20:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RU419 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:	30
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@3/12@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): taskhostw.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, MusNotifyIcon.exe, Microsoft.Photos.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 2.20.157.220, 52.109.88.177, 52.109.12.22, 52.109.8.22
- Excluded domains from analysis (whitelisted): 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, 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, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

Time	Type	Description
01:22:05	API Interceptor	11x 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\5FA6FEA0-CB2C-4F8E-9780-03CC C61C3B5C

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):	5.354734876629519
Encrypted:	false
SSDEEP:	1536:HcQIfgxrBdA3guwQ/Q9DQW+zUk4F77nXmvidZXQE5LWmE9:V8Q9DQW+zwXFU
MD5:	4D2D30320E0FF2EBB190E00ADE9107A9
SHA1:	50761E3502A695D58D1329EFA94A5FC4BD6D78E1
SHA-256:	1649753A06896B3183046837B6ABC949640FA55289B395987056E09BDCAA78BE
SHA-512:	A90327F40016D6BEBFF15A49B522BFED37097D803180F6C1887A2852F99ED813F0C9A5DF088FCCB3DC383A5279E5507AFEEDABDDC33054C7940B35284900639
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="2022-01-29T00:22:03">.. 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\37E97714.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):	5364
Entropy (8bit):	4.856335090472488
Encrypted:	false
SSDEEP:	96:QxgBS1YKG5mPKDRv4Og6tO/XP8lEERc0l+e6HK:QxK5mPaRvO/f8lEERdl+e6HK
MD5:	72FEAFCA807874E6742DFBD011C2B2CD
SHA1:	845FFB7468E2B0932848D356D8127CEE249EB712
SHA-256:	F95F6C5360B90FCECB95608C8364FE5BA2D9372166B7F32766C8A9255AA9CDEE
SHA-512:	1A345CF4D4CCCB263893C4C3C7E353E6DAC44E8EDB880DF19264720C35499035A8154A47B468C422E14C0A93AFA89A80FEFA3DF44CE0101640A02F90D868ADC
Malicious:	false
Reputation:	low
Preview:	....l...0...../.....C..q... EMF.....8.....}.....U..H.....5...R...p.....S.e.g.o.e. .U.l..... .....vp..&1.5.\.R.o.o.t.\.O.f.f.i.c.e.....mEr.....D..Y.....v...v.....t...8.....X.wb.P..... ....6....t.....X.t...w...v...Y..... .....w...v...Y.....cnEr..... .....p..&....}.v.....dv.....%.....r..... ... .?.....?.....l...4..... ... ...(... ... .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\50D0390D.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):	2.3390883230088235
Encrypted:	false
SSDEEP:	48:S83IHpHK2g4x//3G7+wJj7IaK0JohkN+DuuHmt:SVHpHK2x//3+xB7IaK0bNIXGt
MD5:	FA14D04AC7BE94D9470D68B5B05326B9
SHA1:	4C15B8938037773793BC22A9008B83935419D8E0
SHA-256:	CEE5C6209A2D15A2E6EA6DE993B547C375E5716A90D472B55789E4553A212FD1
SHA-512:	419BEFFEE7DA34D924C172A3C8144F160C4306316697123BBF431BD357B3A8AB47540AEEF9855030233C9CFD84BEBD8A429CBFBD10C8D34616EA092D9A6E14EC
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\5237299F.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):	5996
Entropy (8bit):	2.187911659414248
Encrypted:	false
SSDEEP:	24:YOPJZ7pbkyVbYqpBBBBBBBUBBBBBBqBBBBBBBUBBBBBBqBBBBBBBUBBBBBBqBBBc:9vdbkgbUKOwfnV3UqcZZI6Lae
MD5:	914B8A0FCDE8E024E1614BC59CF4CEF0
SHA1:	121F6CF39B1341AA8AF2EDC312DCAA3B58701A80
SHA-256:	FB25589D52AC2015251A56299D5DBF0A164B8CB78086F76BCE990DC717838804
SHA-512:	1B7E4837C949D8509F35C528D4B574CF74C15ED36180F014838723B4ED792316712C4A4EED8740388A43C99EAA406079F02D1FCFB2E27BC62FDAB955CD8CF42
Malicious:	false
Reputation:	low
Preview:	....l.....]...J.....9..... EMF....l.....8.....}.....U..H...F...,.. ...EMF+.@.....`...`...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....!.....%.....'.....%.....K.....M...$... .....?...!.. ....?.....?.. .....l...0..... ... ...(... ..."..... .....?.....3...7...7...?.M..... .....?...!.. ....F.f.....?.....?.....l...4..... ... ...(... ... .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\69015696.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):	5232
Entropy (8bit):	4.879542142933512
Encrypted:	false
SSDEEP:	96:59f2pmYKG5mPKDRv4Og6tO/XP8lEEF6+idRm:5Un5mPaRvO/f8lEE5idRm
MD5:	2A31FF37D8F06AB63C08A874B00F78A5
SHA1:	A216FB97942EE30E82D13F8D308F3D34FB0A3451
SHA-256:	9E941032F88F698814AEC1D444A3541591928A804CCDE5769F535C1590B2907F
SHA-512:	6F51504BFA3FDCF895B04197EA0AA670FEC99BB3A3EE199AF85BC56E5748A1D2B6C113F504431883A7C050C9FF6ADB3D28C50E21B64FDAC4036D5CB6C3D304 66
Malicious:	false
Reputation:	low
Preview:	....l...#.....9.../.....50..q... EMF....p.....8.....}.....U..H.....]...5...R...p.....S.e.g.o.e. .U.l..... .....,ux3S*1.5.\.R.o.o.t.\.O.f.f.i.c.e.....,.E..nQp.....D..^.....,u8..w.....t..E...E.....`.E.....5...E.P.Tu.6....t..E..XTu...w...w...^..U...U..-(.....^.....|t.5.....@.E....w...w...^0.E..... .\.E..oQp.....L.E.....x3S*\.E..},u.....dv.....%.....r..... ... .?.....?.....l...4..... ... ...(... ... .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6A727948.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):	5280
Entropy (8bit):	4.841321930941806
Encrypted:	false
SSDEEP:	96:I0DS0VwurYKG5mPKDRv4Og6tO/XP8lEEHuwL:PDS0G5mPaRvO/f8lEEHuwL
MD5:	E630F750E3440205E6695E75AE1179EB
SHA1:	78DA9D8DF55169C1072618BB97DE5C56517E1329
SHA-256:	E1AAD6F483DEDF11E1156DF09545495BA928CFCF93140B40850420940E6EF11A
SHA-512:	1BE3355C0E87C414D810E0A584BEB0117AB250F1B80F2300E8EB9070D8A17EBE6DB70763CB693948FCCDA4932FEF0C4932DB81CEA9E28E84358146C8515CA9 A4
Malicious:	false
Reputation:	low

Preview:	....l...).....u.../.....k9..t... EMF.....@.....4...>.....<.....5...R...p.....S.e.g.o.e. .U.l..... .....8v..."1.5.\.R.o.o.t.\.O.f.f.i.c.e.....4..nCq.....D..T.....8v...v.....[vd.4...4.....4.....v...v8.....u...u..[v..4.k.....@.....4....v...v....\.u...u..;t.....4.....(zu...4.....4..oCq .....4....."..4..}8v.....dv.....%.....r..... ... .?.....?.....l...4..... ... ...(.. ... .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7D410405.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....>...\....l...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\9658063C.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):	2.333641896616443
Encrypted:	false
SSDEEP:	48:SE3IHpHK2g4x//3G7+wJj7IaK0pNCedxpc1:SNHpHK2x//3+xB7IaK0pUop8
MD5:	10CC58B3B22AD2D5A9BE889181790552
SHA1:	75D40D411B3A3D288E735A4C628DA44C4C39FA3C
SHA-256:	4A2DDC7AE24E1F9277476B6ACD369F53D0250FC329C9BD3B93B6AE64A17B15F5
SHA-512:	F3407353135BC0DD9A1C3861627D1574CA7DC1609514E32BC47892A84D81B133D1AECEF3C85DAE36B32DE0D53560B8CD36EEEA451F382831E2E387AEB7E608A1
Malicious:	false
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\A39313AA.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
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...l..+.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\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D3E7BBA3.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:	C90C1FF27F5179A9C3CC55C0C72E9B95377902B1F91CE216729BA9BEE899A07671506F4533D759DF3C5351B4263FCCEEA66AECE86E72E15093E361624BC4F0FA
Malicious:	false
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\DC2AD8A9.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):	5220
Entropy (8bit):	4.886315397806876
Encrypted:	false
SSDEEP:	96:F04WAPlYKG5mPKDRv4Og6tO/XP8lEEu6KdRE:i4G5mPaRvO/f8lEE+dRE
MD5:	CFC2EB922357AFC2E08B818DF59D2DB4
SHA1:	8123513647762ABFC4460CEFB958BD4A64ECF759
SHA-256:	CCE3BE7E4559A991BA398CBC436519D5B25B07AC458A454D62288A3C31BD35A0
SHA-512:	FA046F388ADD71D6A0819422C1232D44B9F126DEA55FD4761DB00B52299301CADFE744E06CF4DF8B14A5D10EA7BF10C305AE95594165E0ED232EDED3C07D9DF4
Malicious:	false
Preview:	....l..".....0.../.....t... EMF....d.....@.....4...>.....<.....S...5...R...p.....S.e.g.o.e. .U.l..... .....t..].1.5.\.R.o.o.t.\.O.f.f.i.c.e.....n.q.....D..P.....t..w.....4v.....H...EX;w.....6...4v.....X.v..6w...w...P.....\.....(.....6w...w...P.....D....o.q.. .....4.....].D....}.t.....dv.....%.....r..... ... .?.....?.....l...4..... ... ...(.. ... .

C:\Users\user\Desktop\~$RU419 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
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.9948250784848955
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	RU419 FEB17 BSRec_InvNet.xlsx
File size:	4768919
MD5:	bb2bdf2659b515eee1f56c0382847fd7
SHA1:	72405dd23abe1d3f97b75e3eb50bcecbf51669f8
SHA256:	a36ec67f835cb7968270d43f151df7b0b3cbd501b5eeb4688b8676758deadb0e
SHA512:	9c19fc7b871fbdbb46b7af3c50dc29436ffbd28f94d9ed91dbfcb8e1830210be7b66115012dbd67564afa1132107186e22f8d1c839681ed439d487aa49bc5b00
SSDEEP:	98304:zV40bHJu4znpW5DYAY+5HA0MefCaeCtu2qc60yHkOriCbm2:54A04TpADFYUMfvCtH7f0iCD
File Content Preview:	PK.....!...5#....^.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0d2d6d6d0dc

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	7

OLE File "/opt/package/joesandbox/database/analysis/562532/sample/RU419 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:	2017-03-29T09:51:12Z
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

General	
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: 91443	
General	
Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	91443
Entropy:	5.35403120266
Base64 Encoded:	True
Data ASCII:	/ e . . . . R E E M E A G o o d s I n T r a n s i t o l d e r t h a n 9 0 d a y s R U . m s g . C : \ \ U s e r s \ \ j u s t y n a . b e r n a s \ \ D e s k t o p \ \ R e c o n M A R - 2 0 1 6 \ \ m o j e \ \ S E P - 1 6 \ \ r a p o r t y \ \ R E E M E A G o o d s I n T r a n s i t o l d e r t h a n 9 0 d a y s R U . m s g . . . . . ` . . . 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 \ \ R E E M E A G o o d s I n T r a n s i t o l d e r t
Data Raw:	2f 65 01 00 02 00 52 45 20 45 4d 45 41 20 47 6f 6f 64 73 20 49 6e 20 54 72 61 6e 73 69 74 20 6f 6c 64 65 72 20 74 68 61 6e 20 39 30 20 64 61 79 73 20 52 55 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 44 65 73 6b 74 6f 70 5c 52 65 63 6f 6e 20 4d 41 52 2d 32 30 31 36 5c 6d 6f 6a 65 5c 53 45 50 2d 31 36 5c 72 61 70 6f 72 74 79 5c 52 45 20 45

OLE File "/opt/package/joesandbox/database/analysis/562532/sample/RU419 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:	2017-03-29T09:51:12Z
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: \x1Ole10Native, File Type: data, Stream Size: 91443	
General	
Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	91443
Entropy:	5.35403120266
Base64 Encoded:	True
Data ASCII:	/e....RE EMEA Goods In Transit older than 90 days RU.msg.C:\\Users\\justyna.bernas\\Desktop\\Recon MAR-2016\\moje\\SEP-16\\raporty\\RE EMEA Goods In Transit older than 90 days RU.msg.....`...C:\\Users\\JUSTYN~1.BER\\AppData\\Local\\Temp\\RE EMEA Goods In Transit older t
Data Raw:	2f 65 01 00 02 00 52 45 20 45 4d 45 41 20 47 6f 6f 64 73 20 49 6e 20 54 72 61 6e 73 69 74 20 6f 6c 64 65 72 20 74 68 61 6e 20 39 30 20 64 61 79 73 20 52 55 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 44 65 73 6b 74 6f 70 5c 52 65 63 6f 6e 20 4d 41 52 2d 32 30 31 36 5c 6d 6f 6a 65 5c 53 45 50 2d 31 36 5c 72 61 70 6f 72 74 79 5c 52 45 20 45

OLE File "/opt/package/joesandbox/database/analysis/562532/sample/RU419 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:	2017-03-29T09:51:12Z
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....OLE Package.....Package..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: \x1Ole10Native, File Type: data, Stream Size: 91443	
General	
Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	91443
Entropy:	5.35403120266
Base64 Encoded:	True

General	
Data ASCII:	/e....RE EMEA Goods In Transit older than 90 days RU.msg.C:\\Users\\justyna.bernas\\Desktop\\Recon MAR-2016\\moje\\SEP-16\\raporty\\RE EMEA Goods In Transit older than 90 days RU.msg.....`...C:\\Users\\JUSTYN~1.BER\\AppData\\Local\\Temp\\RE EMEA Goods In Transit older t
Data Raw:	2f 65 01 00 02 00 52 45 20 45 4d 45 41 20 47 6f 6f 64 73 20 49 6e 20 54 72 61 6e 73 69 74 20 6f 6c 64 65 72 20 74 68 61 6e 20 39 30 20 64 61 79 73 20 52 55 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 44 65 73 6b 74 6f 70 5c 52 65 63 6f 6e 20 4d 41 52 2d 32 30 31 36 5c 6d 6f 6a 65 5c 53 45 50 2d 31 36 5c 72 61 70 6f 72 74 79 5c 52 45 20 45

OLE File "/opt/package/joesandbox/database/analysis/562532/sample/RU419 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:	2017-03-29T09:51:12Z
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....OLE Package.....Package..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: \x1Ole10Native, File Type: data, Stream Size: 121286

General	
Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	121286
Entropy:	5.36470100495
Base64 Encoded:	True
Data ASCII:	......RE Account 122800 reconciliation (Inventory - Expenses to be landed).msg.C:\\Users\\justyna.bernas\\Desktop\\tymczasowy\\do reconow\\RE Account 122800 reconciliation (Inventory - Expenses to be landed).msg.....r...C:\\Users\\JUSTYN~1.BER\\AppData\\Local\\Temp\\R
Data Raw:	c2 d9 01 00 02 00 52 45 20 41 63 63 6f 75 6e 74 20 31 32 32 38 30 30 20 72 65 63 6f 6e 63 69 6c 69 61 74 69 6f 6e 20 28 49 6e 76 65 6e 74 6f 72 79 20 2d 20 45 78 70 65 6e 73 65 73 20 74 6f 20 62 65 20 6c 61 6e 64 65 64 29 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 44 65 73 6b 74 6f 70 5c 74 79 6d 63 7a 61 73 6f 77 79 5c 64 6f 20 72 65 63

OLE File "/opt/package/joesandbox/database/analysis/562532/sample/RU419 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:	2017-03-29T09:51:12Z
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: 91431	
General	
Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	91431
Entropy:	5.35400764395
Base64 Encoded:	True
Data ASCII:	# e . . . . R E E M E A G o o d s I n T r a n s i t o l d e r t h a n 9 0 d a y s R U . m s g . C : \ \ U s e r s \ \ j u s t y n a . b e r n a s \ \ D e s k t o p \ \ R e c o n M A R - 2 0 1 6 \ \ m o j e \ \ S E P - 1 6 \ \ r a p o r t y \ \ R E E M E A G o o d s I n T r a n s i t o l d e r t h a n 9 0 d a y s R U . m s g . . . . . \ \ . . . 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 \ \ R E E M E A G o o d s I n T r a n s i t o l d e r t
Data Raw:	23 65 01 00 02 00 52 45 20 45 4d 45 41 20 47 6f 6f 64 73 20 49 6e 20 54 72 61 6e 73 69 74 20 6f 6c 64 65 72 20 74 68 61 6e 20 39 30 20 64 61 79 73 20 52 55 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 44 65 73 6b 74 6f 70 5c 52 65 63 6f 6e 20 4d 41 52 2d 32 30 31 36 5c 6d 6f 6a 65 5c 53 45 50 2d 31 36 5c 72 61 70 6f 72 74 79 5c 52 45 20 45

OLE File "/opt/package/joesandbox/database/analysis/562532/sample/RU419 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:	2017-03-29T09:51:12Z
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: 169303

General

Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	169303
Entropy:	7.19148621744
Base64 Encoded:	True
Data ASCII:	S . . . . . I n v o i c e 2 5 0 2 1 3 0 0 1 2 6 3 5 K T C - b o o k i n g w i t h 1 2 0 2 0 0 a c c o u n t . m s g . C : \ \ U s e r s \ \ j u s t y n a . b e r n a s \ \ D e s k t o p \ \ R e c o n M A R - 2 0 1 6 \ \ m o j e \ \ A U G - 1 6 \ \ I n v o i c e 2 5 0 2 1 3 0 0 1 2 6 3 5 K T C - b o o k i n g w i t h 1 2 0 2 0 0 a c c o u n t . m s g . . . . . d . . . 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 \ \ I n v o i c e 2 5 0 2 1 3 0 0 1 2 6 3 5 K T C
Data Raw:	53 95 02 00 02 00 49 6e 76 6f 69 63 65 20 32 35 30 32 31 33 30 30 31 32 36 33 35 4b 54 43 20 2d 20 62 6f 6f 6b 69 6e 67 20 77 69 74 68 20 31 32 30 32 30 30 20 61 63 63 6f 75 6e 74 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 44 65 73 6b 74 6f 70 5c 52 65 63 6f 6e 20 4d 41 52 2d 32 30 31 36 5c 6d 6f 6a 65 5c 41 55 47 2d 31 36 5c 49 6e 76 6f

OLE File "/opt/package/joesandbox/database/analysis/562532/sample/RU419 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:	2017-03-29T09:51:12Z
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: 35605

General	
Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	35605
Entropy:	3.8995864265
Base64 Encoded:	True
Data ASCII:	. . . . . E M E A G o o d s I n T r a n s i t o l d e r t h a n 9 0 d a y s I N M . m s g . C : \\ U s e r s \\ j u s t y n a . b e r n a s \\ D e s k t o p \\ R e c o n M A R - 2 0 1 6 \\ m o j e \\ A U G - 1 6 \\ R a p o r t y \\ E M E A G o o d s I n T r a n s i t o l d e r t h a n 9 0 d a y s I N M . m s g . . . . . Z . . . 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 \\ E M E A G o o d s I n T r a n s i t o l d e r t h a n 9 0
Data Raw:	11 8b 00 00 02 00 45 4d 45 41 20 47 6f 6f 64 73 20 49 6e 20 54 72 61 6e 73 69 74 20 6f 6c 64 65 72 20 74 68 61 6e 20 39 30 20 64 61 79 73 20 49 4e 4d 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 44 65 73 6b 74 6f 70 5c 52 65 63 6f 6e 20 4d 41 52 2d 32 30 31 36 5c 6d 6f 6a 65 5c 41 55 47 2d 31 36 5c 52 61 70 6f 72 74 79 5c 45 4d 45 41 20 47

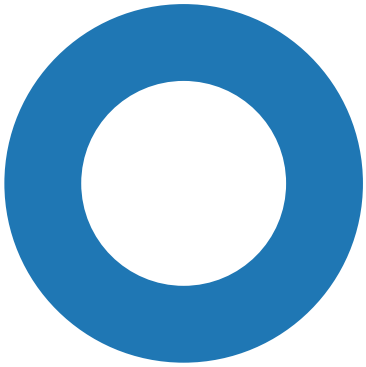
Network Behavior

No network behavior found

Statistics

Behavior

EXCEL.EXE
splwow64.exe



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **864**, Parent PID: **800**

General

Target ID:	0
Start time:	01:22:02
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:	0xeb0000
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

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: **5804**, Parent PID: **864**

General

Target ID:	2
Start time:	01:22:05
Start date:	29/01/2022
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff7801e0000

File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly