ID: 562530
Sample Name: Contact.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 00:54:12
Date: 29/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

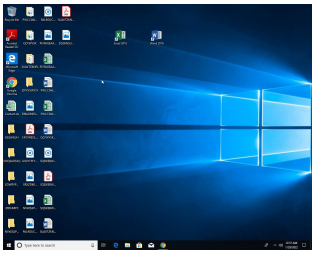
Windows Analysis Report

Contact.xls

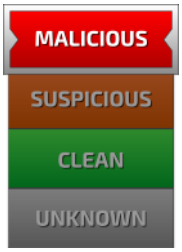
Overview

General Information

Sample Name:	Contact.xls
Analysis ID:	562530
MD5:	fa8570c3fca7bd0..
SHA1:	1e9a8f5de89b43..
SHA256:	0eb209a36a0f42..
Infos:	YARA



Detection

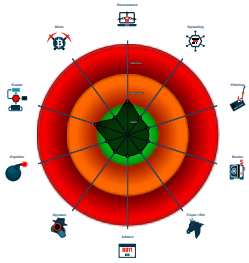


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through…
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6924 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Contact.xls	INDICATOR_OLE_Excel4Macros_DL2	Detects OLE Excel 4 Macros documents acting as downloaders	ditekSHen	• 0x47a3:$e2: 00 4D 61 63 72 6F 31 85 00 • 0x481d:$a1: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 00 01 3A 00 • 0x946:$x1: * #,##0 • 0x952:$x1: * #,##0 • 0x9fb:$x1: * #,##0 • 0xa0a:$x1: * #,##0 • 0xa36:$x1: * #,##0

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

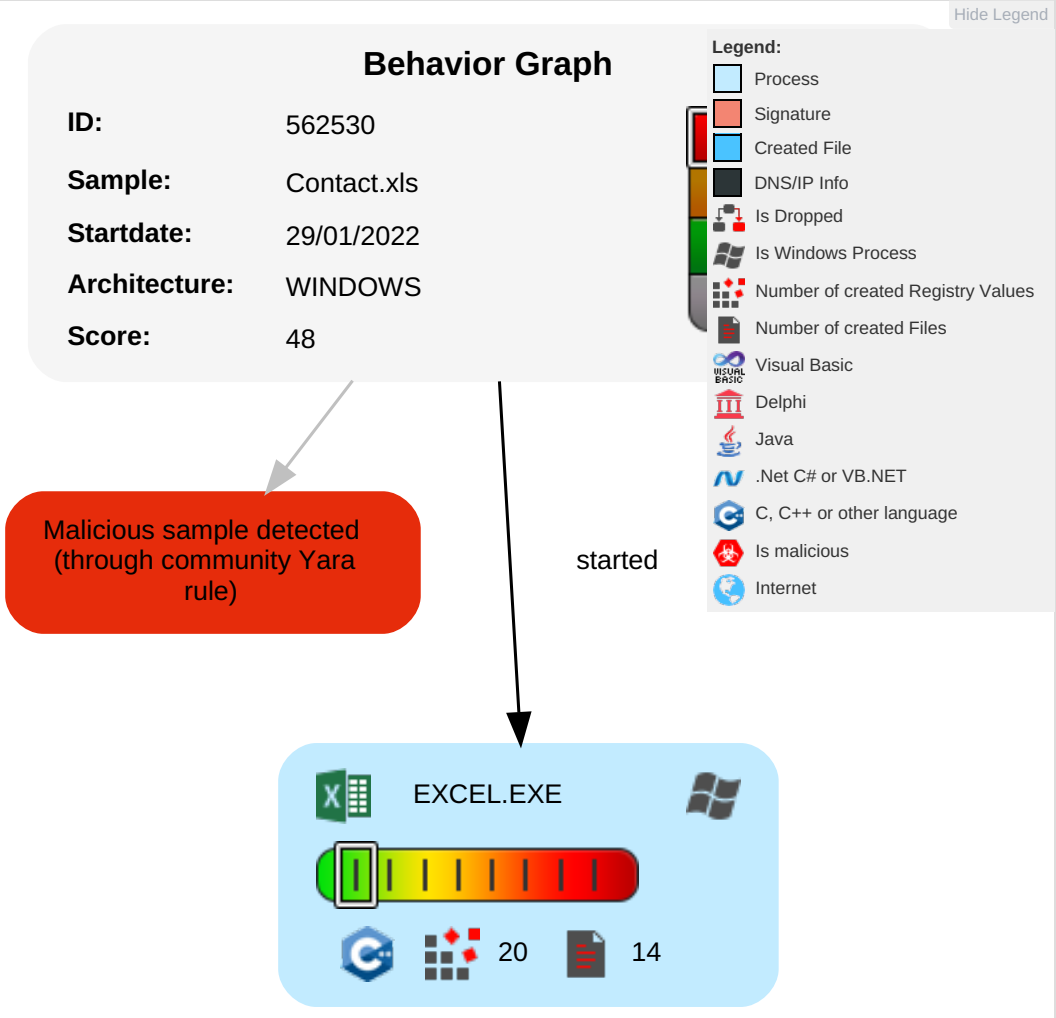
System Summary

Malicious sample detected (through community Yara rule)

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

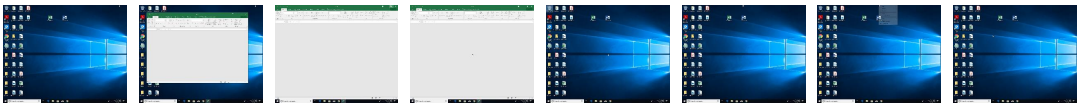
Behavior Graph

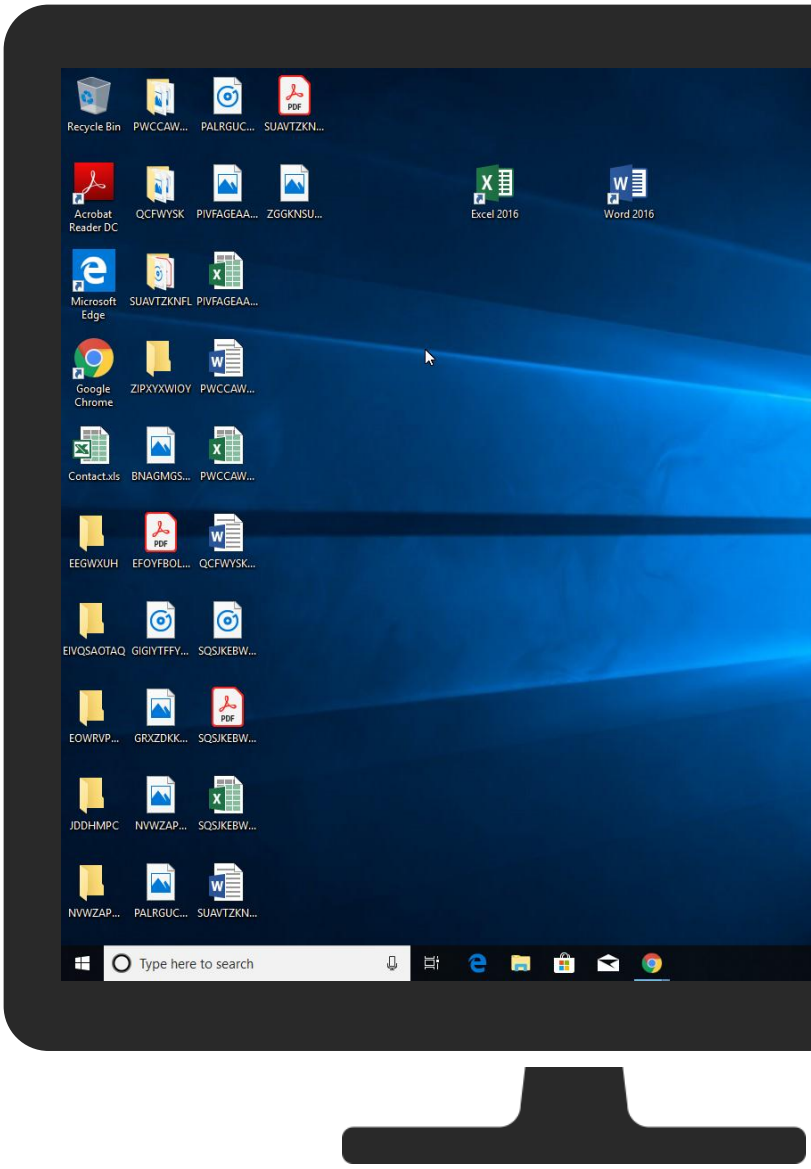


Screenshots

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
Contact.xls	2%	Virustotal		Browse

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	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://login.microsoftonline.com/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://shell.suite.office.com:1443	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://autodiscover-s.outlook.com/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://roaming.edog.	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://cdn.entity.	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://powerlift.acompli.net	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://cortana.ai	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://api.aadrm.com/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://api.microsoftstream.com/api/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://cr.office.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://graph.ppe.windows.net	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://store.office.cn/addinstemplate	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://web.microsoftstream.com/video/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://dataservice.o365filtering.com/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/autodiscover/autodiscover.json	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://ncus.contentsync.	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://weather.service.msn.com/data.aspx	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://apis.live.net/v5.0/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://management.azure.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://outlook.office365.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://wus2.contentsync.	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://api.office.net	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://entitlement.diagnostics.office.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://outlook.office.com/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://outlook.office365.com/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://webshell.suite.office.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://management.azure.com/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://devnull.onenote.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://ncus.pagecontentsync.	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://messaging.office.com/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://augloop.office.com/v2	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://skyapi.live.net/Activity/	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high
http://https://dataservice.o365filtering.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://api.cortana.ai	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com	E0DB925F-1BA5-41F7-8DD1-432043A67229.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562530
Start date:	29.01.2022
Start time:	00:54:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Contact.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.winXLS@1/1@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: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.109.76.68, 52.109.12.24, 52.109.12.21, 52.109.12.22
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, prod-w.nexus.live.com.akadns.net, config.officeapps.live.com, prod.configsvc1.live.com.akadns.net, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information

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\E0DB925F-1BA5-41F7-8DD1-432043A67229

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):	5.35476002489255
Encrypted:	false
SSDEEP:	1536:CcQIfgxrBdA3guwQ/Q9DQW+zUk4F77nXmvidZXQE5LWmE9:q8Q9DQW+zwXFU
MD5:	1699BDC3C621D1023B7B57503CAC2B03
SHA1:	CC2DBEE7C9D80FA878610036F0BD0B0E0DF7F158
SHA-256:	063DE7CB194B5326454517A9D8719A5FB0A725C14CF276FD1D358C4BF8762AD5
SHA-512:	414CD718B316969A3DC8894D100126799CC331EF2AC4F26AB14E94FA8D63C9BC3DE9B2811781F13E7C9991536AFD59F4825F9AA1B209EA774D28648A40C0FD2
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="2022-01-28T23:55:06">.. 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:

Static File Info

General

File type:	Composite Document File V2 Document, Can't read SAT
Entropy (8bit):	6.4919219658612315
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Contact.xls
File size:	52470
MD5:	fa8570c3fca7bd0ecc8b2afbc9a2a088
SHA1:	1e9a8f5de89b43a7cb81003f3106cabaaefc4769
SHA256:	0eb209a36a0f427cb97875cc2f0838077e5c3568c84782773a5bf2e101d7dc9a
SHA512:	4b560f493efb55f4496b4f47de8c6aed5e332ea65e78ac9e4944efa92f27e49b9516756b7cf67fae361c7013263126b9fdf1832de058d75714a8caceefdd5d33
SSDEEP:	1536:1I+Hymsbck3hbdlylKsgqopeJBWhZFGkE+cMLxAAISQ5gQ7X:1I+HymsYk3hbdlylKsgqopeJBWhZFGkU
File Content Preview:	.....>.....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: EXCEL.EXE PID: **6924**, Parent PID: **744**

General

Target ID:	0
Start time:	00:55:04
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:	0xfa0000
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

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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