ID: 651264
Sample Name:
message_tracking_1655942871715.xlsx
Cookbook: default.jbs
Time: 18:07:57
Date: 23/06/2022
Version: 35.0.0 Citrine

Table of Contents

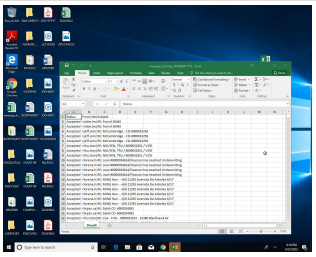
Windows Analysis Report

message_tracking_1655942871715.xlsx

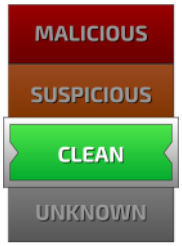
Overview

General Information

Sample Name:	message_tracking_1655942871715.xlsx
Analysis ID:	651264
MD5:	f58a136e486dfe3.
SHA1:	fd61fe4344e0194.
SHA256:	596f05e887818b..
Infos:	



Detection

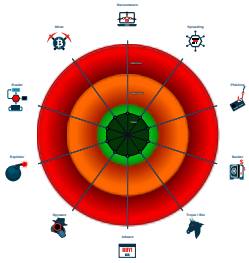


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- EXCEL.EXE (PID: 7108 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

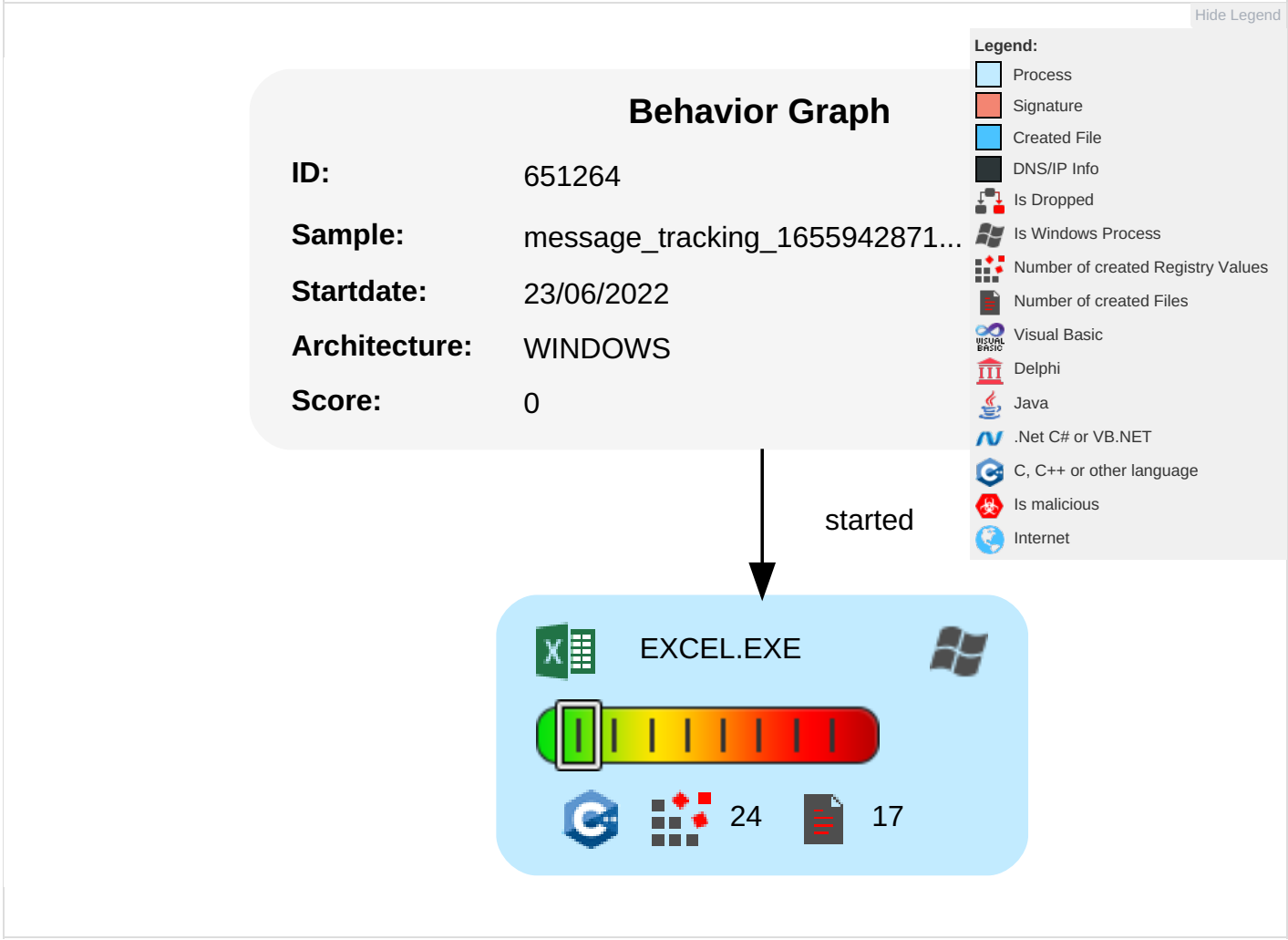
Joe Sandbox Signatures

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	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

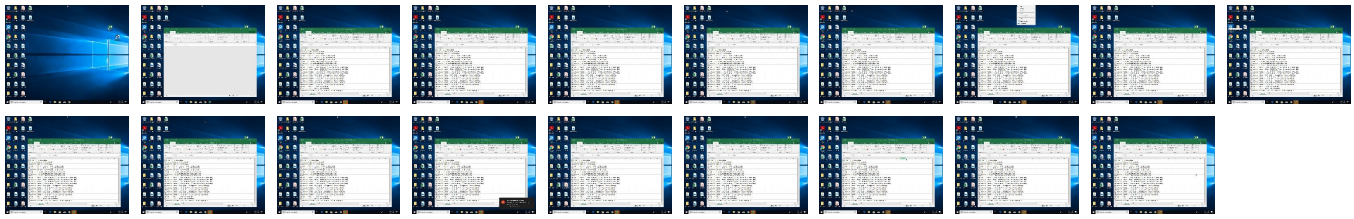
Behavior Graph

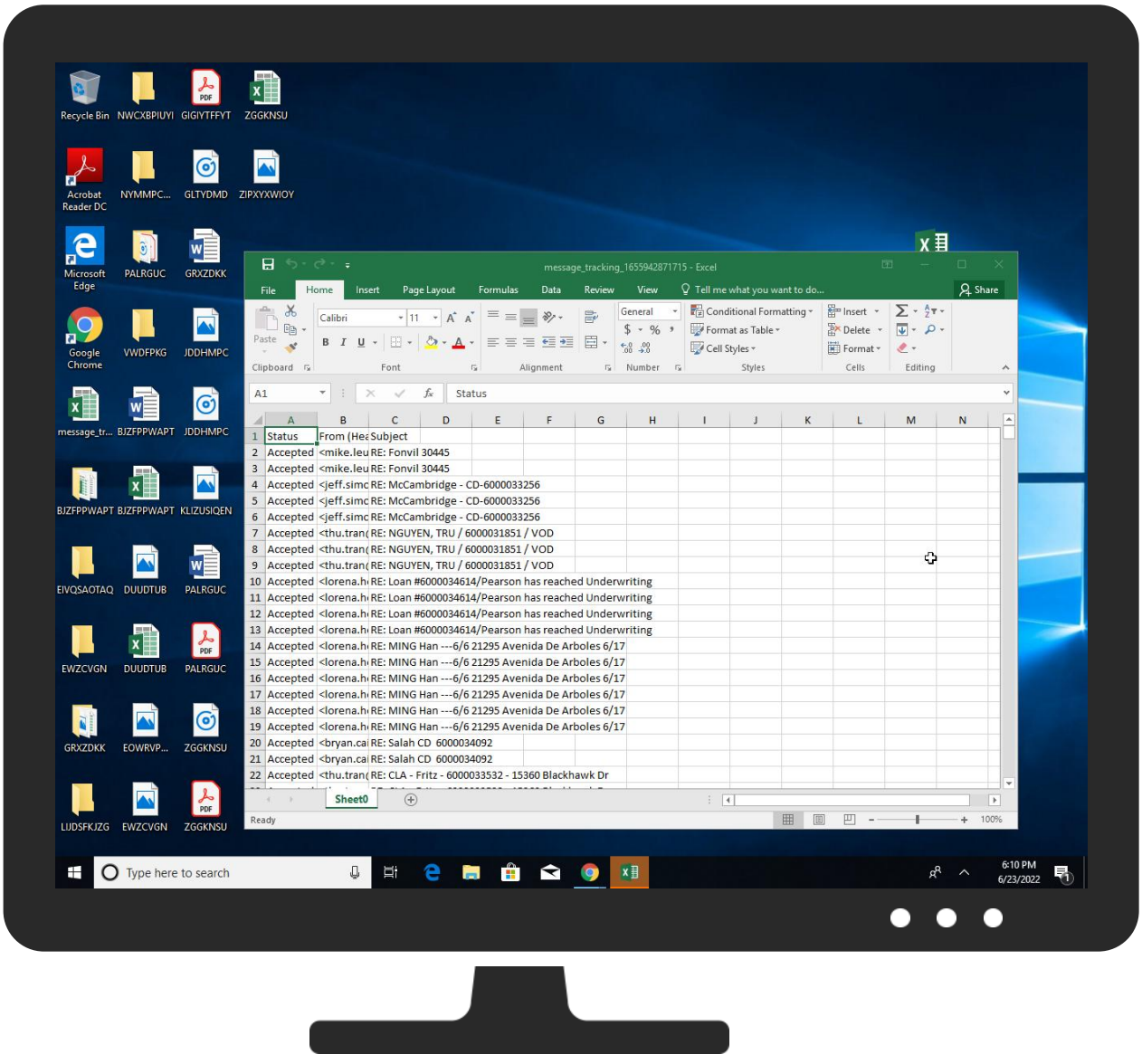


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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	

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	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://login.microsoftonline.com/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://shell.suite.office.com:1443	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://autodiscover-s.outlook.com/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://roaming.edog.	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://cdn.entity.	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://powerlift.acompli.net	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://cortana.ai	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://api.aadrm.com/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://api.microsoftstream.com/api/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://cr.office.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://graph.ppe.windows.net	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://store.office.cn/addinstemplate	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://web.microsoftstream.com/video/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://dataservice.o365filtering.com/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/autodiscover/autodiscover.json	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://ncus.contentsync.	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://weather.service.msn.com/data.aspx	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://apis.live.net/v5.0/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://messaging.lifecycle.office.com/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://management.azure.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://outlook.office365.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://wus2.contentsync.	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://api.office.net	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://entitlement.diagnostics.office.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://outlook.office.com/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://outlook.office365.com/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://webshell.suite.office.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://management.azure.com/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.windows.net/common/oauth2/authorize	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://devnull.onenote.com	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://messaging.action.office.com/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://ncus.pagecontentsync.	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://messaging.office.com/	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://augloop.office.com/v2	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	14FAC50B-DCF4-41CB-B655-19278342466F.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	651264
Start date and time: 23/06/202218:07:57	2022-06-23 18:07:57 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	message_tracking_1655942871715.xlsx
Cookbook file name:	default.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
Number of analysed new started processes analysed:	17
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@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:	• Found application associated with file extension: .xlsx • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.109.32.24, 52.109.88.40, 52.109.12.22
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, licensing.mp.microsoft.com, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information

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\14FAC50B-DCF4-41CB-B655-1927 8342466F

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):	149126
Entropy (8bit):	5.356719938993684
Encrypted:	false
SSDEEP:	1536:JcQW/gxgB5BQguw5/Q9DQC+zQWk4F77nXmvidkXx5ETLKz6e:QJQ9DQC+zcXwI
MD5:	79C5AF0D95104907ACEDFD81720A7444
SHA1:	4B3EB41EFC9EAB59A4933C83838EAE9DD095124B
SHA-256:	F88916160CF4AD8FA9A9732E8345E795CEEF2A47B91CB109FE014F2D4DA1532C
SHA-512:	A51A4D78AFE4987ADB7BF28F993892750237DBA9ABDCB147555AE99B34B6ACB91525DCEC087C742478EED103B04240D50F5CF4A3D3CB9517BFB54CAB6F55FBBF
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="2022-06-23T16:09:01">.. Build: 16.0.15420.30525-->.. <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:	Microsoft OOXML
Entropy (8bit):	7.9596137165530765
TrID:	• ZIP compressed archive (8000/1) 100.00%
File name:	message_tracking_1655942871715.xlsx
File size:	89336
MD5:	f58a136e486dfe359bbe2edca42fcd9b
SHA1:	fd61fe4344e019499a9f6374bf8675f0204aa115
SHA256:	596f05e887818b885e18ed3d5f3f46ed06d128c087aa2c294cffeecb9be212de
SHA512:	9a8fe10095579ebe687c0d71f5be1b6859c7e7e14dd06adbc0c0b3658b1b1b6f867a1126f882156ca1bb4c071310b78c63520bf22433104a63bc8fc84a140638
SSDEEP:	1536:E+q4i/JRYja0Y70G1g99qO4tHq50vCrjXkyNTcvs+mkX86THlFYFt4RehgJstjz0:E+BihRYjgz12KKmvCrbkylkMeF2Ft8e8
TLSH:	3693F2BA938118D1D7F0B9BE47F88DC3375B3AB4C64B8A81DE0870FA21B5D115629ED1
File Content Preview:	PK.....T.....[Content_Types].xml.S.n.0.....*6.PU..C.....\{.X.%....].8.R..q.cfgfW.d.q.ZCB.|..|.*.*h...},^.{Va.^K.<4l..f..b..+....>.. ....D."xB....tL..R-e..v4..*..>..h....Z...z.....Q2S,...H.....v.`o"...U..R..C(2q..qa9S...&.....(.A...p

File Icon

Icon Hash:	74ecd0d2d6d6d0dc

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: EXCEL.EXE PID: **7108**, Parent PID: **812**

General

Target ID:	0
Start time:	18:08:59
Start date:	23/06/2022
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:	0x50000
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
unknown	0	55	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	1B51E4	WriteFile
unknown	55	110	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	1B5241	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	C20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	C211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	C213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	C213B	RegSetValueExW

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

Disassembly

No disassembly