ID: 289537
Sample Name: 903.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:14:51
Date: 24/09/2020
Version: 30.0.0 Red Diamond

Table of Contents

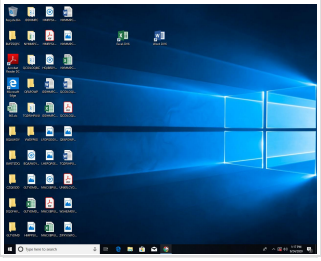
Analysis Report 903.xls

Overview

General Information

Sample Name:	903.xls
Analysis ID:	289537
MD5:	45d6724e12b540..
SHA1:	ab41e637f4bbdf1..
SHA256:	78dc7b7475fda91.

Most interesting Screenshot:



Detection

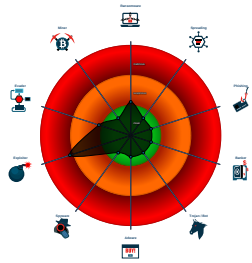
Hidden Macro 4.0

Score:	20
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Yara detected password protected x…
- Unable to load, office file is protecte…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 1196 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

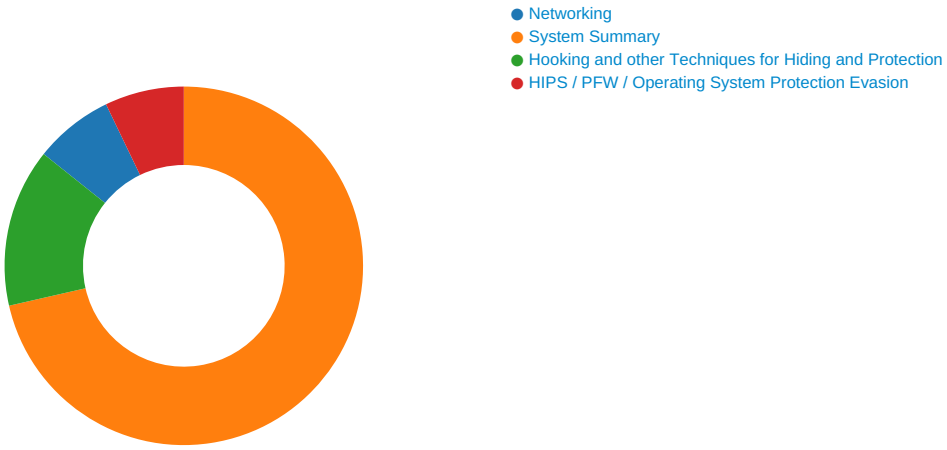
Initial Sample

Source	Rule	Description	Author	Strings
903.xls	JoeSecurity_PasswordProtectedXlsWithEmbeddedMacros	Yara detected password protected xls with embedded macros	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

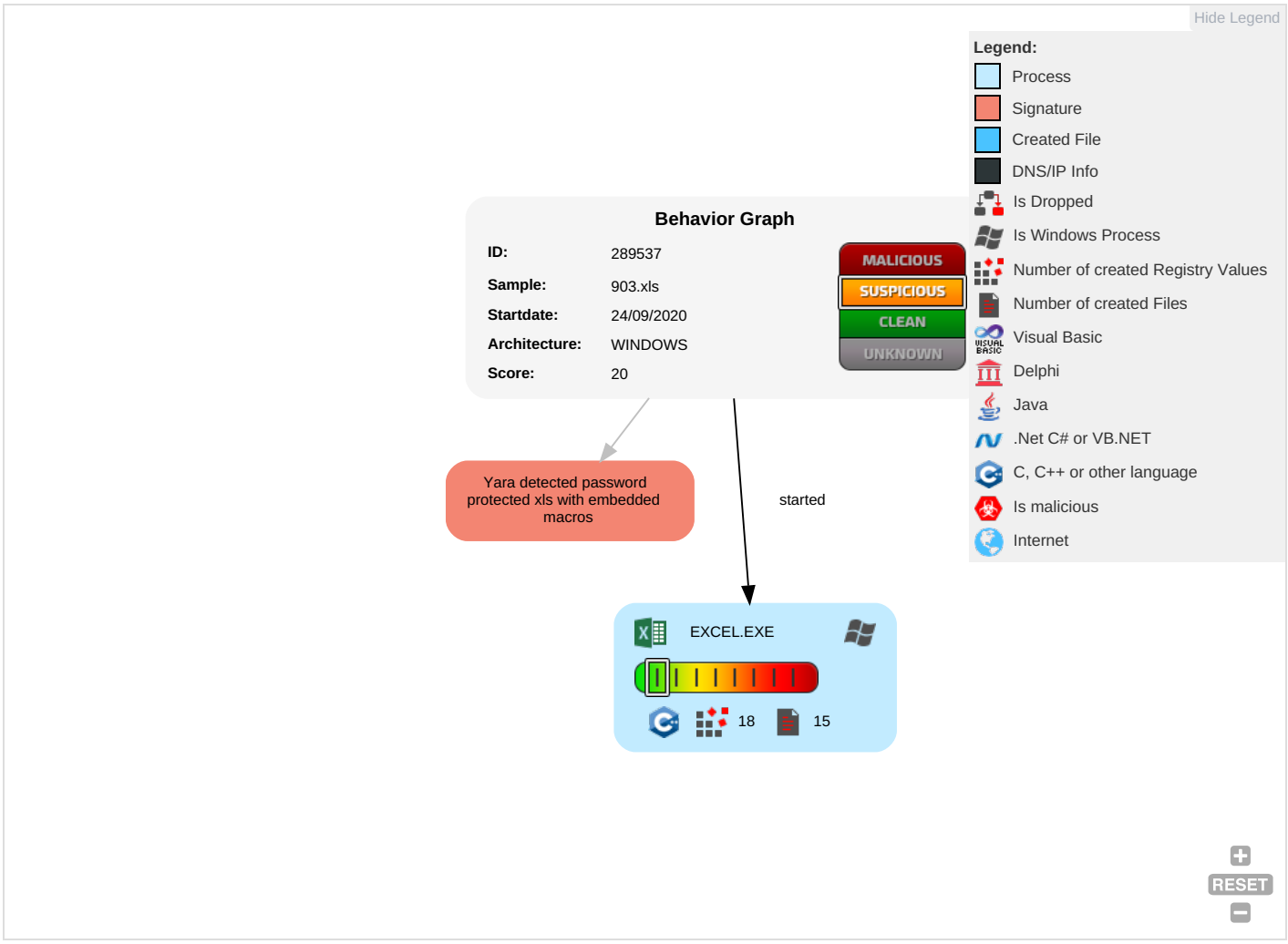
HIPS / PFW / Operating System Protection Evasion:

Yara detected password protected xls with embedded macros

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	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	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	Obfuscated Files or Information 1	LSASS Memory	System Information Discovery 1	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://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	Virustotal		Browse
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	Virustotal		Browse
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	Virustotal		Browse
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	Virustotal		Browse
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	Virustotal		Browse
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	Virustotal		Browse
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	Virustotal		Browse
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	Virustotal		Browse
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	Virustotal		Browse
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	Virustotal		Browse
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	Virustotal		Browse
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	Virustotal		Browse
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	Virustotal		Browse
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	Virustotal		Browse
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	Virustotal		Browse
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	Virustotal		Browse
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	Virustotal		Browse
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Virustotal		Browse
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	Virustotal		Browse
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	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	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://login.microsoftonline.com/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://shell.suite.office.com:1443	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://cdn.entity.	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.contentsync.	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://powerlift.acompli.net	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://cortana.ai	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://api.aadrm.com/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://api.microsoftstream.com/api/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://cr.office.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://graph.ppe.windows.net	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://store.office.cn/addinstemplate	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://web.microsoftstream.com/video/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://graph.windows.net	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://dataservice.o365filtering.com/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://weather.service.msn.com/data.aspx	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://apis.live.net/v5.0/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://management.azure.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://incidents.diagnostics.office.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://api.office.net	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://entitlement.diagnostics.office.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://templatelogging.office.com/client/log	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://management.azure.com/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://ncus-000.contentsync.	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://devnull.onenote.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://messaging.office.com/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://skyapi.live.net/Activity/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://dataservice.o365filtering.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://directory.services.	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://onedrive.live.com/embed?	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://augloop.office.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://www.bingapis.com/api/v7/urlpreview/search?appid=E93048236FE27D972F67C5AF722136866DF65FA2	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://clients.config.office.net/	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://api.diagnostics.office.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/GetFreeformSpeech	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high
http://https://settings.outlook.com	591CF5FC-6366-46BB-ACBC-6570F7EAF0A5.0.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	30.0.0 Red Diamond
Analysis ID:	289537
Start date:	24.09.2020
Start time:	13:14:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	903.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	w10x64 Windows 10 64 bit v1803 with Office Professional Plus 2016, 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:	16
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:	SUS
Classification:	sus20.expl.winXLS@1/1@0/0
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:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 51.143.111.7, 52.158.208.111, 52.109.76.6, 52.109.88.38, 52.109.8.24, 51.104.139.180, 80.239.152.136, 80.239.148.32, 93.184.221.240, 51.105.249.228, 13.78.168.230, 20.190.3.175, 20.54.26.129, 40.90.22.192, 40.90.22.190, 40.90.22.183, 40.90.22.187, 40.90.22.186, 40.90.22.191, 40.90.22.185, 40.90.22.184, 52.155.217.156, 23.210.248.85 • Excluded domains from analysis (whitelisted): umwatson.trafficmanager.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, am3p.wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, emea1.notify.windows.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, sls.update.microsoft.com, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, wu.ec.azureedge.net, sls.update.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, login.msa.msidentity.com, ris.api.iris.microsoft.com, sls.emea.update.microsoft.com.akadns.net, umwatsonrouting.trafficmanager.net, config.officeapps.live.com, europe.configsvc1.live.com.akadns.net, bay-main-ips.b.lg.prod.aadmsa.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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\591CF5FC-6366-46BB-ACBC-6570F7EAF0A5	
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
Size (bytes):	128139
Entropy (8bit):	5.376293264094705
Encrypted:	false
MD5:	395C2EFC4841357F546055A1D2D69E4A
SHA1:	900DE48191260B636A885CEAD32569715B21D4DD
SHA-256:	2CF2B0233C9791581704565FE05A43087573A60F2E330D5D7AEB27F4EE2744E6
SHA-512:	921646FE96DC86DDE455E6B33099B944FA0AA4CBDB8B280243F768DF55F6651D214FE59EEF7F7DC38232A5A5254A6D81C579E0917EF89273E844BC9F346CBC1
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="2020-09-24T11:15:46">.. Build: 16.0.13322.30528-->.. <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, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: SJzNXHGtfHdpEl, Last Saved By: test, Name of C reating Application: Microsoft Excel, Create Time/Date: Mon Sep 14 22:28:14 2020, Last Saved Time/Date: Wed Sep 23 17:00:44 2020, Security: 1
Entropy (8bit):	7.825080839475646
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	903.xls
File size:	273920
MD5:	45d6724e12b54092a46c8b8cf57bb316
SHA1:	ab41e637f4bbdf17beb50f4b67b7293aec162737
SHA256:	78dc7b7475fda91e1d378073404fe0dc0ee3b63054ddfe9a68c4bf79958dcbe6
SHA512:	ce870c88a6aa0acd5c68ad3470d9a09fb4ee5b98af6048475d3094e6a89fcc7ab7713fb008c1a7f9e3b217dfc56568db64c43690010568f76adaf527c854166c
SSDEEP:	6144:5wmPf2PmRG0qKX3LlVdOEfL23h9wEDu+zhRet+OkikL9c:6mH6QGeX3pX63h9wau+1K2iK9c
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "903.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary

Code Page:	1252
Author:	SJzNXHGtfHdpEl
Last Saved By:	test
Create Time:	2020-09-14 21:28:14
Last Saved Time:	2020-09-23 16:00:44
Creating Application:	Microsoft Excel
Security:	1

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.311454994264
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . P . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . S h e e t 1 . . . . . R M B . . . . . W o r k s h e e t s . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 ec 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 a7 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096

General	
Entropy:	0.29983696163
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . ` . . . . . p . . . . . S J z N X H G t f H d p E . . . . . t e s t . . . . . M i c r o s o f t E x c e l . @ . . . . + ... @ . . . . . f . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a8 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 60 00 00 00 12 00 00 00 70 00 00 00 0c 00 00 00 88 00 00 00 0d 00 00 00 94 00 00 00 13 00 00 00 a0 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 10 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 261961

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	261961
Entropy:	7.94785679197
Base64 Encoded:	True
Data ASCII:	. . . . . Z O . . . . . / . . . . . ~ . . . . . h . . . . . M . c . r . o . s . o . f . t . . E . n . h . a . n . c . e . d . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . v . 1 . . . 0 . . . . . @ . . .) % : . j . . " . . . . . m (. _ . . .	. G . . . . . ' s . 4 , . . . " . . . . . s ? . > . . . . . \ \ . p . . 6 . ` " . . 9 . . . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 2f 00 c8 00 01 00 04 00 02 00 0c 00 00 00 7e 00 00 00 0c 00 00 00 00 00 00 00 01 68 00 00 00 04 80 00 00 80 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 24, 2020 13:15:34.174993992 CEST	54349	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:34.198873043 CEST	53	54349	8.8.8.8	192.168.2.3
Sep 24, 2020 13:15:35.140310049 CEST	53542	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:35.164210081 CEST	53	53542	8.8.8.8	192.168.2.3
Sep 24, 2020 13:15:35.957680941 CEST	53765	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:35.981626987 CEST	53	53765	8.8.8.8	192.168.2.3
Sep 24, 2020 13:15:36.996678114 CEST	65041	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:37.021358967 CEST	53	65041	8.8.8.8	192.168.2.3
Sep 24, 2020 13:15:38.106875896 CEST	57757	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:38.130734921 CEST	53	57757	8.8.8.8	192.168.2.3
Sep 24, 2020 13:15:39.412358046 CEST	59610	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:39.436038971 CEST	53	59610	8.8.8.8	192.168.2.3
Sep 24, 2020 13:15:42.929389000 CEST	54464	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:42.953085899 CEST	53	54464	8.8.8.8	192.168.2.3
Sep 24, 2020 13:15:46.707751989 CEST	50291	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:46.740643978 CEST	53	50291	8.8.8.8	192.168.2.3
Sep 24, 2020 13:15:47.077507019 CEST	56058	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:47.124542952 CEST	53	56058	8.8.8.8	192.168.2.3
Sep 24, 2020 13:15:48.076734066 CEST	56058	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:48.119210005 CEST	53	56058	8.8.8.8	192.168.2.3
Sep 24, 2020 13:15:49.092973948 CEST	56058	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:49.124923944 CEST	53	56058	8.8.8.8	192.168.2.3
Sep 24, 2020 13:15:51.108592987 CEST	56058	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:51.140782118 CEST	53	56058	8.8.8.8	192.168.2.3
Sep 24, 2020 13:15:55.124562979 CEST	56058	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:55.158782005 CEST	53	56058	8.8.8.8	192.168.2.3
Sep 24, 2020 13:15:55.457623959 CEST	54745	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:15:55.481214046 CEST	53	54745	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:02.789006948 CEST	53300	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:02.822415113 CEST	53	53300	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:23.375921011 CEST	52249	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 24, 2020 13:16:23.401365042 CEST	53	52249	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:27.045079947 CEST	64857	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:27.077363014 CEST	53	64857	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:28.352828979 CEST	64910	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:28.376871109 CEST	53	64910	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:40.879653931 CEST	50958	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:40.933229923 CEST	53	50958	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:41.769880056 CEST	64790	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:41.817795992 CEST	53	64790	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:42.695602894 CEST	60578	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:42.746799946 CEST	53	60578	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:42.965356112 CEST	55649	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:42.989563942 CEST	53	55649	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:43.824038029 CEST	49562	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:43.855911016 CEST	53	49562	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:44.236777067 CEST	62011	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:44.277411938 CEST	53	62011	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:44.676872015 CEST	51439	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:44.709007978 CEST	53	51439	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:45.019618034 CEST	57912	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:45.051671028 CEST	53	57912	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:45.441704988 CEST	59192	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:45.484440088 CEST	53	59192	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:45.869708061 CEST	51691	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:45.901787043 CEST	53	51691	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:46.274405003 CEST	51666	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:46.306458950 CEST	53	51666	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:46.593210936 CEST	61945	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:46.625185013 CEST	53	61945	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:47.082827091 CEST	55918	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:47.114962101 CEST	53	55918	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:48.470242977 CEST	49183	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:48.502296925 CEST	53	49183	8.8.8.8	192.168.2.3
Sep 24, 2020 13:16:52.536869049 CEST	56284	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:16:52.570559025 CEST	53	56284	8.8.8.8	192.168.2.3
Sep 24, 2020 13:17:02.543766022 CEST	57903	53	192.168.2.3	8.8.8.8
Sep 24, 2020 13:17:02.593630075 CEST	53	57903	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 1196 Parent PID: 808

General

Start time:	13:15:45
Start date:	24/09/2020
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:	0x140000

File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

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