ID: 321050
Sample Name:
sviluppo_economico_18__257.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:26:32
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

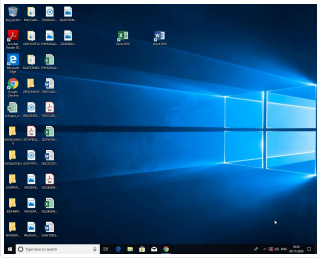
Analysis Report sviluppo_economico_18__257.xls

Overview

General Information

Sample Name:	sviluppo_economico_18__257.xls
Analysis ID:	321050
MD5:	497b53c6668e12..
SHA1:	ae46204ffd41a64..
SHA256:	f07973faea77882..

Most interesting Screenshot:



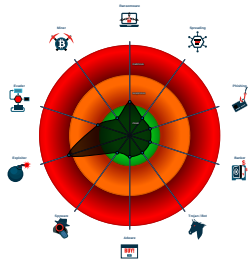
Detection

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: 4156 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

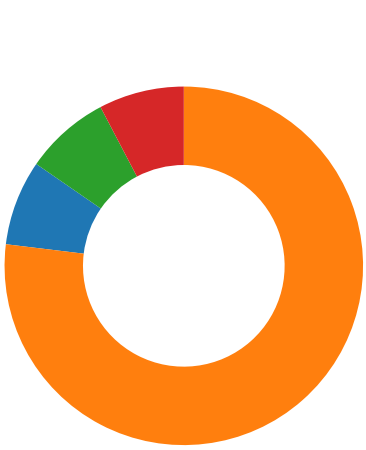
Initial Sample

Source	Rule	Description	Author	Strings
sviluppo_economico_18__257.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

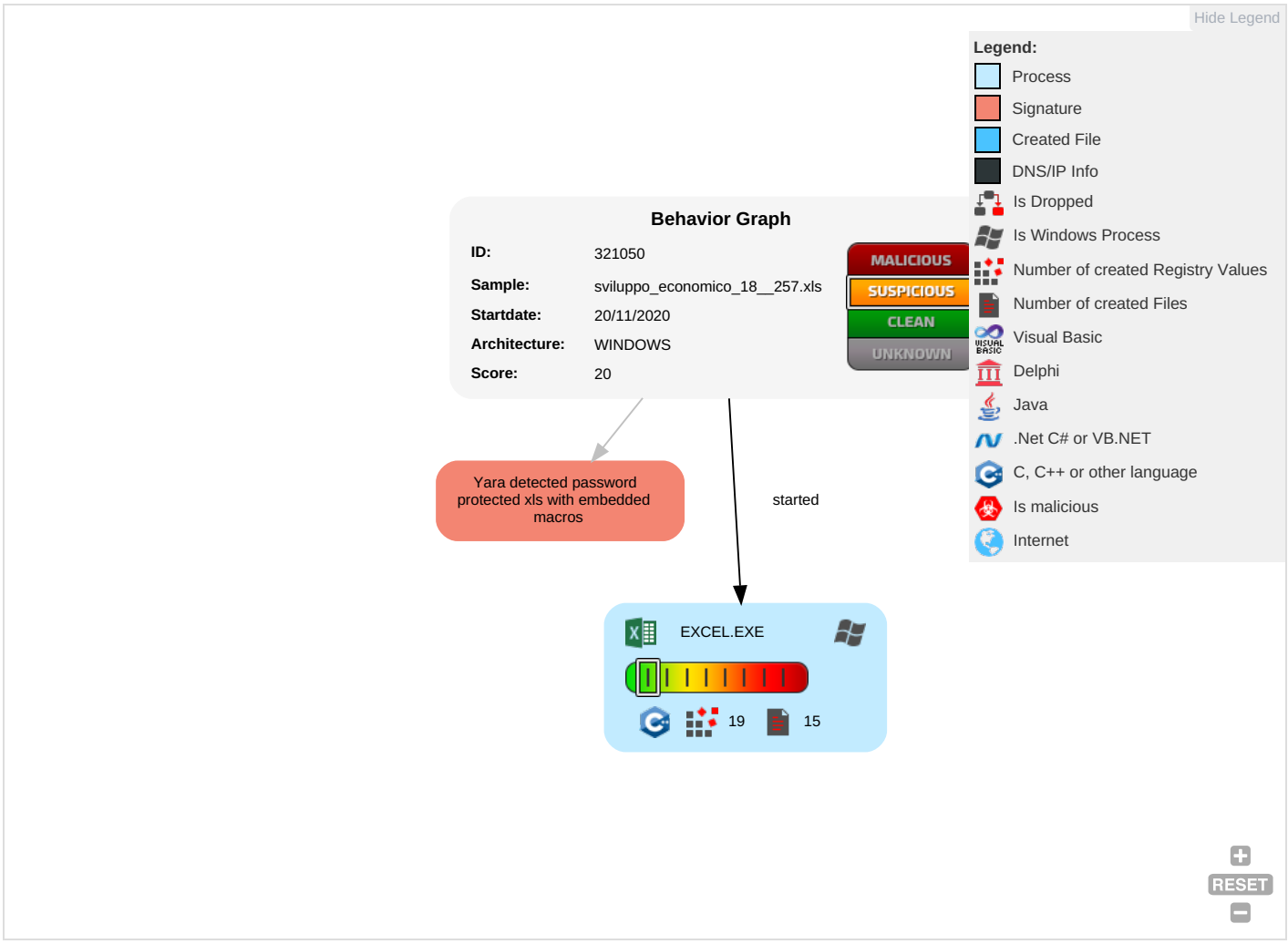
HIPS / PFW / Operating System Protection Evasion:

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	Rootkit	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

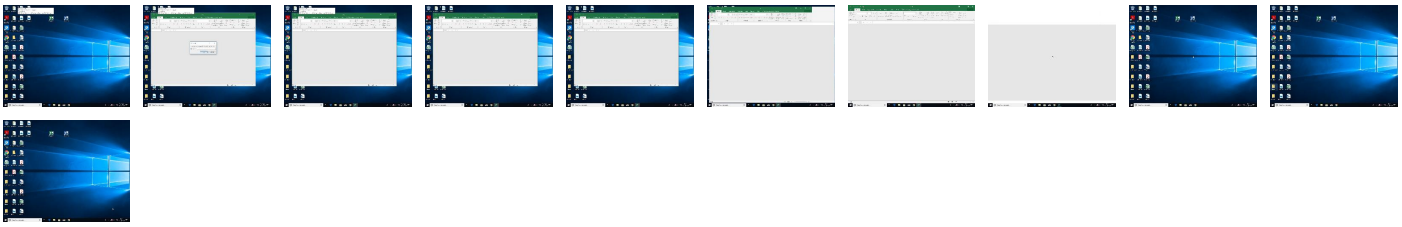
Behavior Graph



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

Source	Detection	Scanner	Label	Link
sviluppo_economico_18__257.xls	6%	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://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
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://powerlift.acompli.net	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://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
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://cortana.ai	0%	URL Reputation	safe	
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://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%	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://res.getmicrosoftkey.com/api/redemptionevents	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://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%	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://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://wus2-000.pagecontentsync.	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://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%	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://dev0-api.acompli.net/autodetect	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://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
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://dataservice.o365filtering.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://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%	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://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
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://ncus-000.contentsync.	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://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%	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://skyapi.live.net/Activity/	0%	URL Reputation	safe	
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://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%	URL Reputation	safe	
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	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://login.microsoftonline.com/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://shell.suite.office.com:1443	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://cdn.entity.	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://wus2-000.contentsync.	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://cortana.ai	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://api.aadrm.com/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://api.microsoftstream.com/api/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://cr.office.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://graph.ppe.windows.net	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://store.office.cn/addinstemplate	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://web.microsoftstream.com/video/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://graph.windows.net	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://dataservice.o365filtering.com/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://weather.service.msn.com/data.aspx	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://apis.live.net/v5.0/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://management.azure.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://outlook.office365.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://incidents.diagnostics.office.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://api.office.net	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://asgsmsproxyapi.azurewebsites.net/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://entitlement.diagnostics.office.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://autodiscover-s.outlook.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://templatelogging.office.com/client/log	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://management.azure.com/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://ncus-000.contentsync.	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://devnull.onenote.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://messaging.office.com/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://augloop.office.com/v2	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://skyapi.live.net/Activity/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://dataservice.o365filtering.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://directory.services.	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://onedrive.live.com/embed?	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high
http://https://augloop.office.com	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.bingapis.com/api/v7/urlpreview/search?appid=E93048236FE27D972F67C5AF722136866DF65FA2	AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B.0.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321050
Start date:	20.11.2020
Start time:	10:26:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sviluppo_economico_18__257.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:	21
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 • Changed system and user locale, location and keyboard layout to Italian - Italy • 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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.42.151.234, 52.109.32.27, 52.109.88.39, 52.109.8.23, 23.210.248.85, 51.104.144.132, 205.185.216.42, 205.185.216.10, 20.54.26.129, 104.43.139.144, 51.11.168.160, 95.101.22.134, 95.101.22.125 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, config.officeapps.live.com, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.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\AC42BFC9-8440-46A9-BF44-EB2CB8D5BA2B	
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):	129952
Entropy (8bit):	5.378335030279484
Encrypted:	false
SSDEEP:	1536:7cQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:pmQ9DQW+zBX8u
MD5:	DCB47E168C66B597A4A3AD88A0DFC606
SHA1:	ECFC2F0651D274BF1E644D085E9C52313BE674DA
SHA-256:	51D53E177B926C0B90AE56DD2CBA71420E882B74DA62228FA488E0BEE65FBC1F
SHA-512:	CF9C84881631D6D6D0324253BA3787B7E416F2EE67858A5A0EE3B9FA03AB1EC7FC9CD7FE4F8EC6FDB2841EBE60D29EC4D41B02C641EE9E2AE3F9375CF50A9 3B
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="2020-11-20T09:27:35">.. Build: 16.0.13518.30530-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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: veeREfBOcKbNRq, Last Saved By: administrator, Name of Creating Application: Microsoft Excel, Create Time/Date: Wed Nov 18 21:59:48 2020, Last Saved Time/Date: Wed Nov 18 22:46:55 2020, Security: 1
Entropy (8bit):	7.657541825457614
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	sviluppo_economico_18__257.xls
File size:	406528
MD5:	497b53c6668e127364bc30f56555399b
SHA1:	ae46204ffd41a649ce4fb9ab24e0add934b68549
SHA256:	f07973faea77882d308d04ea19d66110e3ed3e65c2b8acc 45fb6e6fffb5180f4
SHA512:	92e760cbf9ac4bcbfeecf232b6c4f3dbddf0e7287e9795e4 10f68bfea0e0c7e7739d48d5bebab0a1c9e09aa442658c7 d406cb586e9dc0f02c0a8227c5f66d1c2
SSDEEP:	6144:io0aQoiZJoBOKsuHzGNpT6rLh/s7UpT2ETflvilcM SvcseT8O:1wZ6BOKseGNgfa7ET8SvmH
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "sviluppo_economico_18__257.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:	veeREfBOcKbNRq
Last Saved By:	administrator
Create Time:	2020-11-18 21:59:48
Last Saved Time:	2020-11-18 22:46:55
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:	0.749350878342
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . P . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . F o g l i o 1 . . . . . F o g l i o 2 . . . . F o g l i o 3 . . . . . F o g l i o 4 . . . . . t X C l h W q g
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 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 0c 02 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 be 01 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.330245496252
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . ` . . . . . x . . . . . v e e R E f B O c K b N R q . . . . . a d m i n i s t r a t o r . . . . . M i c r o s o f t E x c e l . @ . . . . b . ! . . . . @ . . . . Y . . . . .
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 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 b0 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 78 00 00 00 0c 00 00 00 90 00 00 00 0d 00 00 00 9c 00 00 00 13 00 00 00 a8 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: 393436

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	393436
Entropy:	7.75690503676
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 . . . . . % . . . C . . P . . . . . h ; ~ . <) . X . . . 9 . , # . . . . . v / . 4 . . . . . y . . I . . . . . \ \ . p . 5 . R . B @ . . . . .
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 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
Nov 20, 2020 10:27:20.820866108 CET	64185	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:20.847958088 CET	53	64185	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:21.478976965 CET	65110	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:21.506289959 CET	53	65110	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:23.817430019 CET	58361	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:23.853261948 CET	53	58361	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:24.890496016 CET	63492	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:24.926238060 CET	53	63492	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:26.118782043 CET	60831	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:26.145806074 CET	53	60831	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:35.239835978 CET	60100	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:35.279100895 CET	53	60100	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:35.571603060 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:35.638370991 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:36.581835985 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:36.618887901 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:37.585036039 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:37.620615959 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:39.582700968 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:39.620450974 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:40.617322922 CET	50141	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:40.644412994 CET	53	50141	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:43.598619938 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:43.636204004 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:46.419555902 CET	53023	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:46.446671963 CET	53	53023	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:48.327178001 CET	49563	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:48.354605913 CET	53	49563	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:49.325272083 CET	51352	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:49.352189064 CET	53	51352	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:49.804657936 CET	59349	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:49.843851089 CET	53	59349	8.8.8.8	192.168.2.3
Nov 20, 2020 10:27:50.169934034 CET	57084	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:27:50.197022915 CET	53	57084	8.8.8.8	192.168.2.3
Nov 20, 2020 10:28:00.867996931 CET	58823	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:28:00.894996881 CET	53	58823	8.8.8.8	192.168.2.3
Nov 20, 2020 10:28:01.959742069 CET	57568	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:28:01.986718893 CET	53	57568	8.8.8.8	192.168.2.3
Nov 20, 2020 10:28:03.156800032 CET	50540	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:28:03.183762074 CET	53	50540	8.8.8.8	192.168.2.3
Nov 20, 2020 10:28:07.912851095 CET	54366	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:28:07.939990044 CET	53	54366	8.8.8.8	192.168.2.3
Nov 20, 2020 10:28:09.216999054 CET	53034	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:28:09.252787113 CET	53	53034	8.8.8.8	192.168.2.3
Nov 20, 2020 10:28:12.365748882 CET	57762	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:28:12.392900944 CET	53	57762	8.8.8.8	192.168.2.3
Nov 20, 2020 10:28:13.192749023 CET	55435	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:28:13.228507042 CET	53	55435	8.8.8.8	192.168.2.3
Nov 20, 2020 10:28:24.735367060 CET	50713	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:28:24.762434006 CET	53	50713	8.8.8.8	192.168.2.3
Nov 20, 2020 10:28:29.796464920 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:28:29.833558083 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 10:28:59.741245985 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:28:59.768280029 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 10:29:01.941852093 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 10:29:01.985625982 CET	53	56579	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 4156 Parent PID: 792

General

Start time:	10:27:33
Start date:	20/11/2020
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:	0xb90000
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 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