ID: 320147
Sample Name:
sviluppo_economico_18__49.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 04:27:33
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

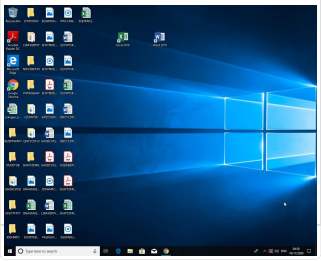
Analysis Report sviluppo_economico_18__49.xls

Overview

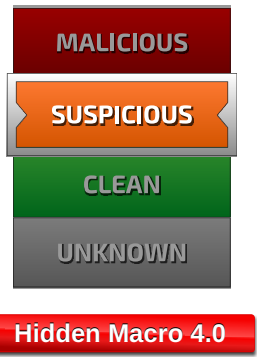
General Information

Sample Name:	sviluppo_economico_18__49.xls
Analysis ID:	320147
MD5:	1f820167d901345.
SHA1:	d495f5482d4646f..
SHA256:	5294eb9f95967fc..
Tags:	gozi isfb italy pwmise u rsnif xls

Most interesting Screenshot:



Detection



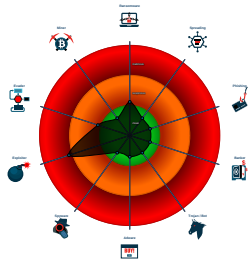
Score:	20
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Yara detected password protected x…

Unable to load, office file is protecte…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6600 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

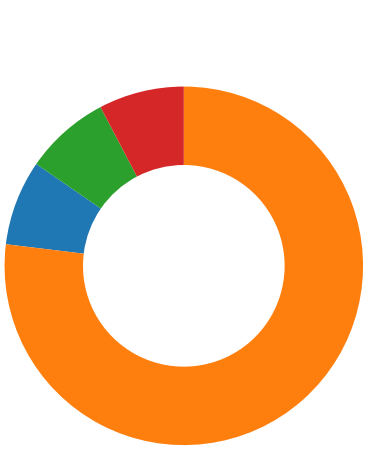
Initial Sample

Source	Rule	Description	Author	Strings
sviluppo_economico_18__49.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

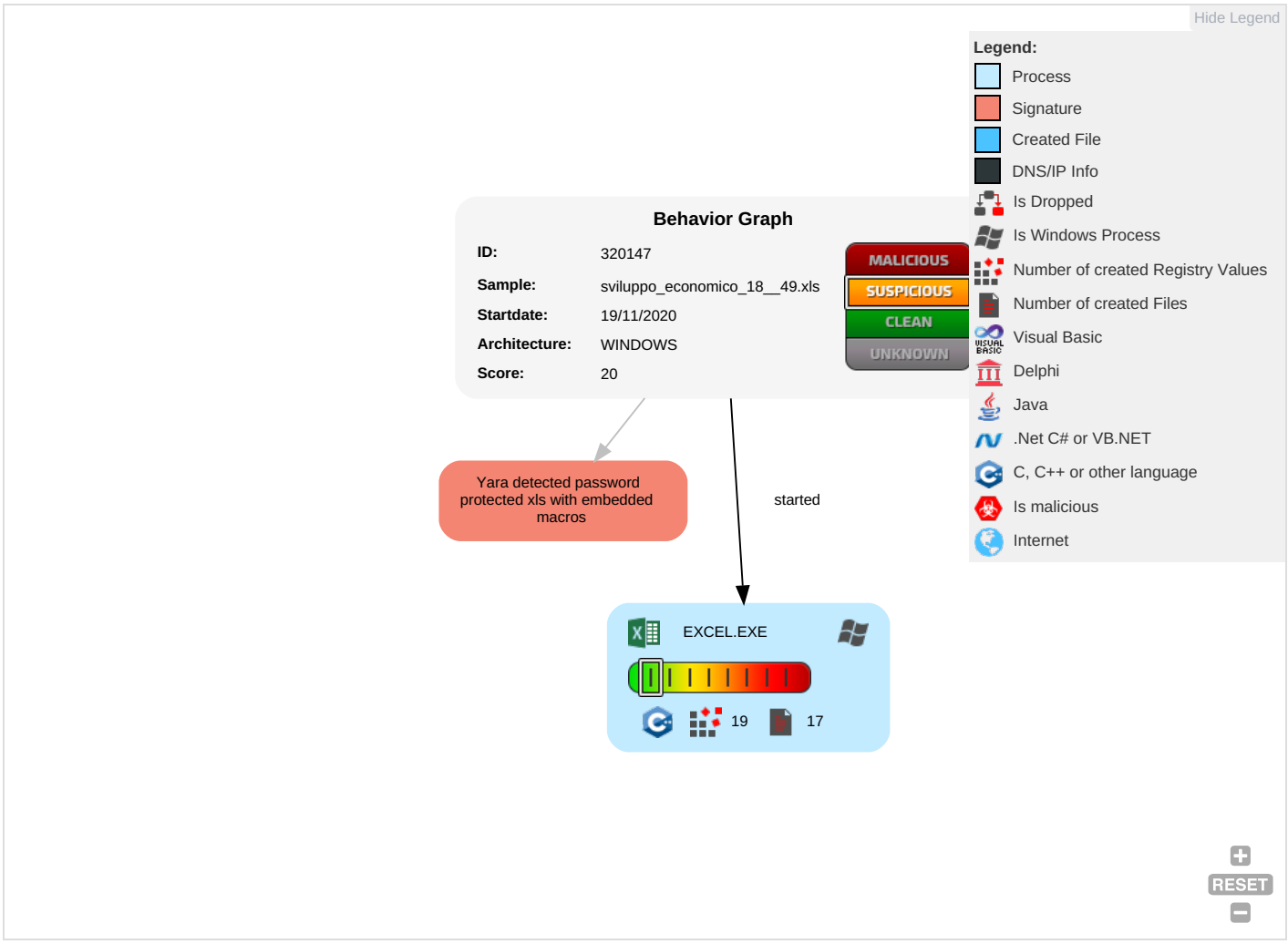
HIPS / PFW / Operating System Protection Evasion:

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

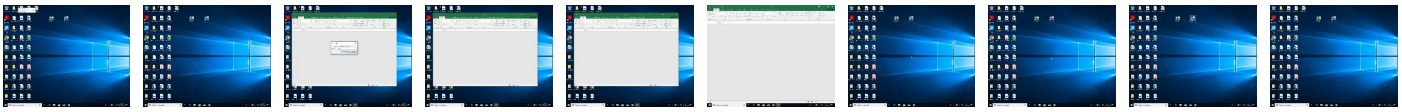
Behavior Graph



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__49.xls	5%	Virustotal		Browse
sviluppo_economico_18__49.xls	8%	ReversingLabs		

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	

Source	Detection	Scanner	Label	Link
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	
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	

Source	Detection	Scanner	Label	Link
http://https://prod-global-autodetect.acompli.net/autodetect	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://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%	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	

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	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://login.microsoftonline.com/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://shell.suite.office.com:1443	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://cdn.entity.	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://wus2-000.contentsync.	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.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	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://powerlift.acompli.net	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://rpsticket.partnerservices.getmicrosoftkey.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://cortana.ai	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.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	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://api.aadrm.com/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://api.microsoftstream.com/api/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://cr.office.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://ecs.office.com/config/v2/Office	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://graph.ppe.windows.net	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://officeci.azurewebsites.net/api/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://store.office.cn/addinstemplate	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.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=	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://globaldisco.crm.dynamics.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://web.microsoftstream.com/video/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://graph.windows.net	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://dataservice.o365filtering.com/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://weather.service.msn.com/data.aspx	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://apis.live.net/v5.0/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.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	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://management.azure.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://outlook.office365.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://incidents.diagnostics.office.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://api.office.net	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://incidents.diagnosticssdf.office.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://asgsmsproxyapi.azurewebsites.net/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://entitlement.diagnostics.office.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://autodiscover-s.outlook.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://templatelogging.office.com/client/log	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://management.azure.com/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://ncus-000.contentsync.	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://devnull.onenote.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://messaging.office.com/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://augloop.office.com/v2	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://skyapi.live.net/Activity/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.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	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://dataservice.o365filtering.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://directory.services.	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://onedrive.live.com/embed?	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://augloop.office.com	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high
http://https://www.bingapis.com/api/v7/urlpreview/search?appid=E93048236FE27D972F67C5AF722136866DF65FA2	E49A654B-53F8-483C-9403-C27BA9EE9E6F.1.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320147
Start date:	19.11.2020
Start time:	04:27:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sviluppo_economico_18__49.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:	24
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, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 23.54.113.53, 13.88.21.125, 52.255.188.83, 40.88.32.150, 52.109.32.27, 52.109.8.25, 52.109.76.36, 104.43.193.48, 23.54.113.104, 51.104.139.180, 20.54.26.129, 205.185.216.10, 205.185.216.42, 23.10.249.26, 23.10.249.43 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, 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, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, config.officeapps.live.com, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.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\E49A654B-53F8-483C-9403-C27BA9EE9E6F	
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):	5.378338165090134
Encrypted:	false
SSDEEP:	1536:8cQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:emQ9DQW+zBX8u
MD5:	A1BBD17E5598BF3ECA8E58D8921DFBF7
SHA1:	AC998281670386A753BADF778CB6E2A88C5C2345
SHA-256:	95428C3AB316FD912AE328CA694A3A01921AB41BE0FBE640A6E7528C8E35291A
SHA-512:	C8F32395DE1642CE18FCC97A2D21545C2E26461EAA637A900A3EFFE5B196717AF6A7C55394FE7592D3A5C618C542F593E9EBF2B99927EA4446F00A13E85128DA
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="2020-11-19T03:28:29">.. Build: 16.0.13517.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: ILDbqjTBEYBF, 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 22:20:16 2020, Security: 1
Entropy (8bit):	7.658923216957258
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	sviluppo_economico_18__49.xls
File size:	418816
MD5:	1f820167d901345a2f14fd588fe0260b
SHA1:	d495f5482d4646f8535785d4317e8b1b2a986ce0
SHA256:	5294eb9f95967fc0bb8b148edbed12826b818e747f779ad3c87ad76e21783443
SHA512:	1eca2d82a73b5d952299b0fb17183450caae745a5cae419300c1404b0ed7c047ef425741912ee3b721312aeeeb4f752b8487c234ebf26975086c7dd9da045d3e
SSDEEP:	6144:ZdD6vFpLfmmge3jNmsP0wkRRX3ejHgBcrVDS+SlhnLviCkxJIa/7962p/07XHKJk:fGrndPVkDdm+fLv38V7xe3v/T
File Content Preview:	.....>.....0.....)...*...+....-...../..... .....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "sviluppo_economico_18__49.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:	ILDbqjTBEYBF
Last Saved By:	administrator
Create Time:	2020-11-18 21:59:48
Last Saved Time:	2020-11-18 22:20:16
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:	0.709758224125
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 . . . . . U z J J H M j q
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 e8 01 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 9a 01 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.323237348927
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . ` . . . . . x . . . . . I L D b q j T B E Y B F . . . . . 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 . ! . . . . @ . . . P . . . . .
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 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: 405803

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	405803
Entropy:	7.75484404397
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 . . . . . X q . . i V 8 . . . . D . . H R . . * . < L . 3 O + R . r . H . . . . 2 / . q . . . . J . . . y . u . W . . . . . H . . . . . \\ . p . . q] . . . I . [. i .
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 19, 2020 04:28:15.601705074 CET	60985	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:15.614697933 CET	53	60985	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:16.952312946 CET	50200	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:16.970671892 CET	53	50200	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:17.359241009 CET	51281	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:17.372442007 CET	53	51281	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:18.491600037 CET	49199	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:18.504738092 CET	53	49199	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:20.309472084 CET	50620	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:20.322747946 CET	53	50620	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:21.043150902 CET	64938	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:21.055365086 CET	53	64938	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:27.952595949 CET	60152	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:27.966301918 CET	53	60152	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:29.043715954 CET	57544	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:29.064321041 CET	53	57544	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:29.371234894 CET	55984	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:29.418893099 CET	53	55984	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:30.156846046 CET	64185	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:30.168957949 CET	53	64185	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:30.373374939 CET	55984	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:30.391886950 CET	53	55984	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:31.247565031 CET	65110	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:31.259959936 CET	53	65110	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:31.374090910 CET	55984	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:31.387392998 CET	53	55984	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:32.591733932 CET	58361	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:32.604849100 CET	53	58361	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:33.374310970 CET	55984	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:33.387816906 CET	53	55984	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:33.669042110 CET	63492	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:33.682588100 CET	53	63492	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:34.335217953 CET	60831	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:34.347522974 CET	53	60831	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:36.100239038 CET	60100	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:36.113708973 CET	53	60100	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:36.824008942 CET	53195	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:36.836318016 CET	53	53195	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:37.389969110 CET	55984	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:37.403045893 CET	53	55984	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:37.475606918 CET	50141	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:37.488746881 CET	53	50141	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:39.199282885 CET	53023	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 04:28:39.212348938 CET	53	53023	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:41.481075048 CET	49563	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:41.493908882 CET	53	49563	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:42.490592957 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:42.504040956 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:43.177684069 CET	59349	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:43.191273928 CET	53	59349	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:43.987833977 CET	57084	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:44.000992060 CET	53	57084	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:45.112464905 CET	58823	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:45.125035048 CET	53	58823	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:50.284727097 CET	57568	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:50.309746027 CET	53	57568	8.8.8.8	192.168.2.3
Nov 19, 2020 04:28:50.486824036 CET	50540	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:28:50.499389887 CET	53	50540	8.8.8.8	192.168.2.3
Nov 19, 2020 04:29:03.419907093 CET	54366	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:29:03.453732967 CET	53	54366	8.8.8.8	192.168.2.3
Nov 19, 2020 04:29:05.252456903 CET	53034	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:29:05.265981913 CET	53	53034	8.8.8.8	192.168.2.3
Nov 19, 2020 04:29:24.418272018 CET	57762	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:29:24.431482077 CET	53	57762	8.8.8.8	192.168.2.3
Nov 19, 2020 04:29:28.465044022 CET	55435	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:29:28.483295918 CET	53	55435	8.8.8.8	192.168.2.3
Nov 19, 2020 04:29:58.408273935 CET	50713	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:29:58.420909882 CET	53	50713	8.8.8.8	192.168.2.3
Nov 19, 2020 04:30:32.189897060 CET	56132	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:30:32.204168081 CET	53	56132	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 6600 Parent PID: 792

General

Start time:	04:28:27
Start date:	19/11/2020
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:	0x890000
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