ID: 320145
Sample Name:
sviluppo_economico_19__56.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 04:21:31
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

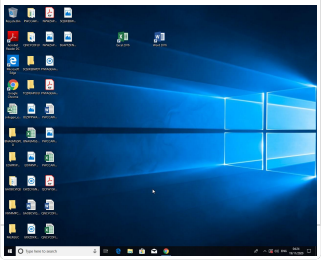
Analysis Report sviluppo_economico_19__56.xls

Overview

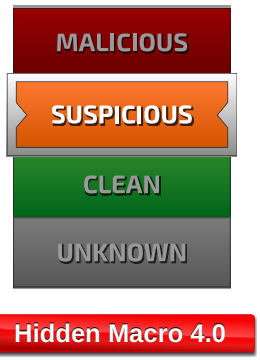
General Information

Sample Name:	sviluppo_economico_19__56.xls
Analysis ID:	320145
MD5:	fc6b65df2045577..
SHA1:	f609f1769ad094f…
SHA256:	c6d2905ab73ac5..
Tags:	gozi isfb italy pwmise u rsnif xls

Most interesting Screenshot:



Detection



Hidden Macro 4.0

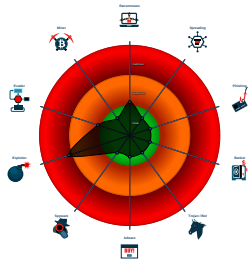
Score:	20
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Yara detected password protected x…

Unable to load, office file is protecte…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 2336 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

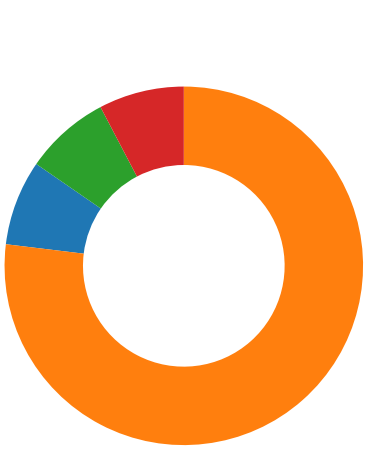
Initial Sample

Source	Rule	Description	Author	Strings
sviluppo_economico_19__56.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

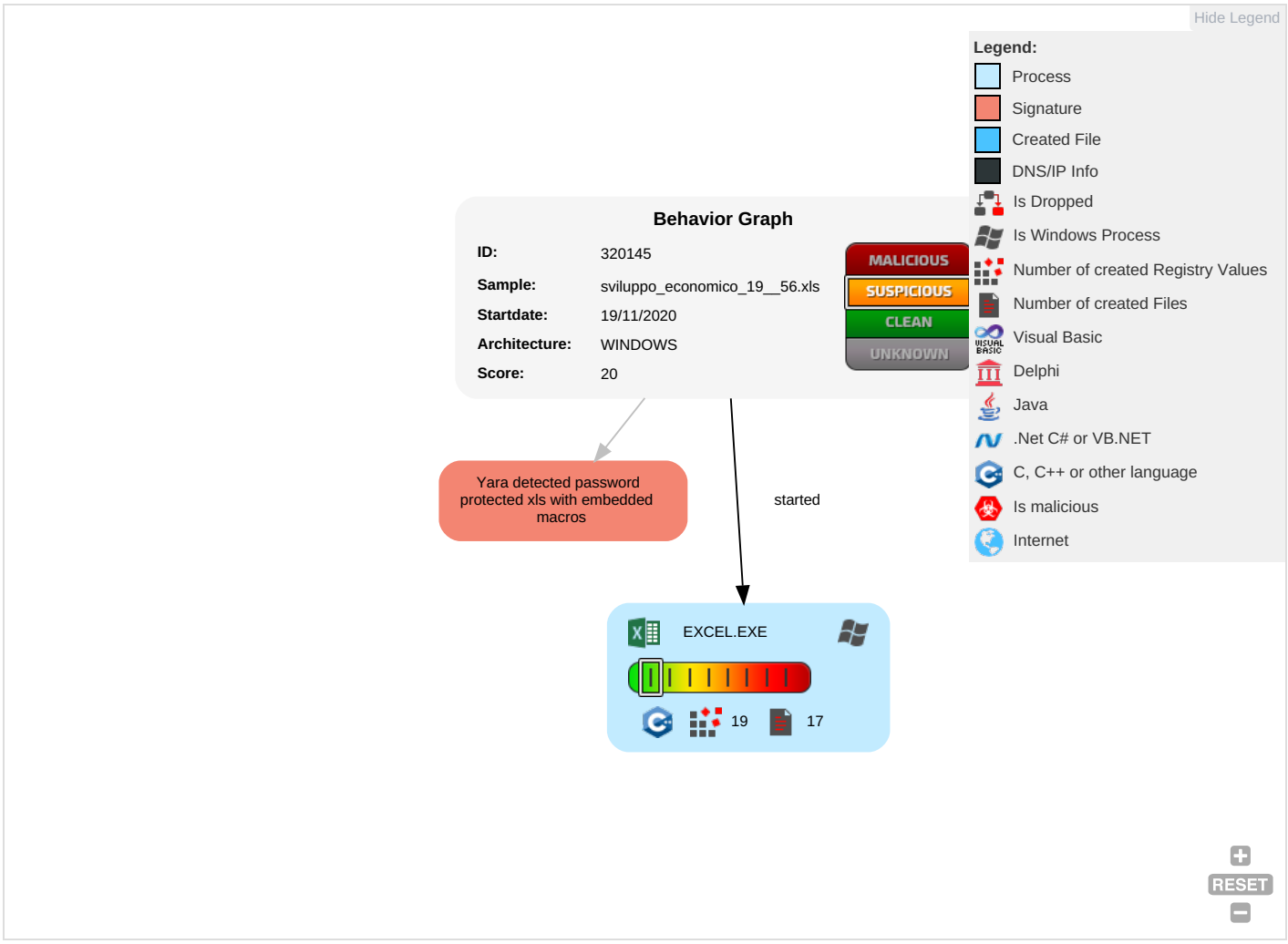
HIPS / PFW / Operating System Protection Evasion:

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

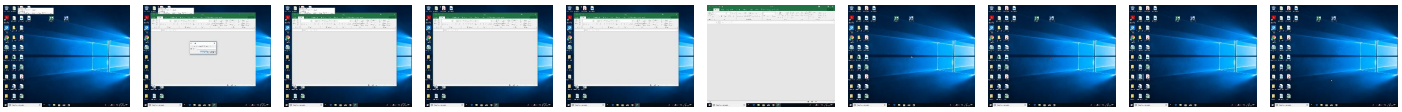
Behavior Graph



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_19__56.xls	5%	Virustotal		Browse
sviluppo_economico_19__56.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	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://login.microsoftonline.com/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://shell.suite.office.com:1443	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://cdn.entity.	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://wus2-000.contentsync.	422A0605-7770-4385-B61B-FC57751D7C47.0.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	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://powerlift.acompli.net	422A0605-7770-4385-B61B-FC57751D7C47.0.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	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://cortana.ai	422A0605-7770-4385-B61B-FC57751D7C47.0.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	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://api.aadrm.com/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://api.microsoftstream.com/api/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://cr.office.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://graph.ppe.windows.net	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://store.office.cn/addinstemplate	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	422A0605-7770-4385-B61B-FC57751D7C47.0.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=	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://web.microsoftstream.com/video/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://graph.windows.net	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://dataservice.o365filtering.com/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://weather.service.msn.com/data.aspx	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://apis.live.net/v5.0/	422A0605-7770-4385-B61B-FC57751D7C47.0.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	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://management.azure.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://outlook.office365.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://incidents.diagnostics.office.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://api.office.net	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://asgsmsproxyapi.azurewebsites.net/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://entitlement.diagnostics.office.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://autodiscover-s.outlook.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://templatelogging.office.com/client/log	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://management.azure.com/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://ncus-000.contentsync.	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://devnull.onenote.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://messaging.office.com/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://augloop.office.com/v2	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://skyapi.live.net/Activity/	422A0605-7770-4385-B61B-FC57751D7C47.0.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	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://dataservice.o365filtering.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://directory.services.	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://onedrive.live.com/embed?	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://augloop.office.com	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high
http://https://www.bingapis.com/api/v7/urlpreview/search?appid=E93048236FE27D972F67C5AF722136866DF65FA2	422A0605-7770-4385-B61B-FC57751D7C47.0.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320145
Start date:	19.11.2020
Start time:	04:21:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sviluppo_economico_19__56.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, 104.43.139.144, 13.88.21.125, 52.109.76.6, 52.109.12.22, 52.109.76.36, 52.109.8.25, 51.11.168.160, 23.54.113.104, 20.54.26.129, 52.147.198.201, 51.104.139.180, 23.10.249.43, 23.10.249.26, 51.104.144.132 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus15.cloudapp.net, umwatsonrouting.trafficmanager.net, config.officeapps.live.com, 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, 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\422A0605-7770-4385-B61B-FC57751D7C47	
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):	5.378325196320136
Encrypted:	false
SSDEEP:	1536:bcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:JmQ9DQW+zBX8u
MD5:	7B65B0C8702ABE61B011BF43AB19C154
SHA1:	1F80B74147AB7A75C77EC523BEEE8ED85D6DC6EC
SHA-256:	ABEA6D7C4BC5AA3C0E361F34BF3B383B146529E7B83F20A9B1E6E8277E7BA9DE
SHA-512:	A5817013669CB9080861FBDFDFBA02305BFF32001A518C019039B9879421CED7B292151DD703D11A621A81684F75FE09F68EA229F655BF97C1889C1C2F7BAE76
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="2020-11-19T03:22:28">.. 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: xPBFfTQKcawSqwsF, Last Saved By: administrator, Name of Creating Application: Microsoft Excel, Create Time/Date: Wed Nov 18 22:00:31 2020, Last Saved Time/Date: Wed Nov 18 22:21:10 2020, Security: 1
Entropy (8bit):	7.659448672689523
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	sviluppo_economico_19__56.xls
File size:	414208
MD5:	fc6b65df2045577c2ebe213e9fb519c2
SHA1:	f609f1769ad094fb3c670a6ac7f35d6524a889f9
SHA256:	c6d2905ab73ac56ef9d7baa9ec840c21e9a60b7ce579ea13e3641c841abdfbcd
SHA512:	ee087c38a4664527e7c14134e5231423fc48eeb0efd2604c32a72384e42c1c3b1e90b9f8bdfcf963253311ff96bd90a92c66e30dd72229085147d137c238dd7d
SSDEEP:	12288:XK0Tm48IZAh+7LS2uuKcB2Gj/S7JpJxSsf:XK0648IzXS2uuyT3Rf
File Content Preview:	.....>.....'..... ...!..."...#...$...%...&..... .....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "sviluppo_economico_19__56.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel

Indicators	
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:	xPBFfTQKcawSqwsF
Last Saved By:	administrator
Create Time:	2020-11-18 22:00:31
Last Saved Time:	2020-11-18 22:21:10
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

<table>
<tr><th>General</th><th></th></tr>
<tr><td>Stream Path:</td><td>\x5DocumentSummaryInformation</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Stream Size:</td><td>4096</td></tr>
<tr><td>Entropy:</td><td>0.892479989061</td></tr>
<tr><td>Base64 Encoded:</td><td>False</td></tr>
<tr><td>Data ASCII:</td><td>. . . . . + , . . 0 . . . l . . . . 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 . . . . . h L p Z V K e V</td></tr>
<tr><td>Data Raw:</td><td>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 6c 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 21 02 00 00</td></tr>
</table>

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

<table>
<tr><th>General</th><th></th></tr>
<tr><td>Stream Path:</td><td>\x5SummaryInformation</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Stream Size:</td><td>4096</td></tr>
<tr><td>Entropy:</td><td>0.336117908835</td></tr>
<tr><td>Base64 Encoded:</td><td>False</td></tr>
<tr><td>Data ASCII:</td><td>. . . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . .
. . . d . . . . | . . . . x P B F f T Q K c a w S q
w s 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 . @ . . . . . c ; .
. . . @ . . . .</td></tr>
<tr><td>Data Raw:</td><td>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 b4 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 64 00 00 00 12 00 00 00 7c 00 00 00 0c 00 00 00 94 00 00 00 0d 00 00 00 a0 00 00 00 13 00 00 00 ac 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 14 00 00 00</td></tr>
</table>

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 401387

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

General	
Stream Size:	401387
Entropy:	7.75378745111
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 . . . . . @ . l . " . . " l . . . . ? g C , . . : v O . . . K . . . . . E . . . = J . . u c f . c . f c . 7 . > . . . . . d . . . . . \\ . p . V 9 . . + . . . V V . R
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 04:22:15.298053980 CET	64185	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:15.310302973 CET	53	64185	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:16.138633013 CET	65110	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:16.151722908 CET	53	65110	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:16.812279940 CET	58361	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:16.825476885 CET	53	58361	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:17.972285032 CET	63492	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:17.985461950 CET	53	63492	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:19.015402079 CET	60831	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:19.028686047 CET	53	60831	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:19.918514013 CET	60100	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:19.931662083 CET	53	60100	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:24.586469889 CET	53195	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:24.598942041 CET	53	53195	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:26.893038988 CET	50141	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:26.906095028 CET	53	50141	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:27.829644918 CET	53023	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:27.849960089 CET	53	53023	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:27.973016977 CET	49563	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:27.985770941 CET	53	49563	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:28.207758904 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:28.227411985 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:29.219065905 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:29.237343073 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:29.990937948 CET	59349	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:30.003751993 CET	53	59349	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:30.234622002 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:30.247847080 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:31.024291039 CET	57084	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:31.037141085 CET	53	57084	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:32.250001907 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:32.269772053 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:36.266005993 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:36.279248953 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:41.734649897 CET	58823	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:41.747140884 CET	53	58823	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:47.514435053 CET	57568	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:47.553998947 CET	53	57568	8.8.8.8	192.168.2.3
Nov 19, 2020 04:22:54.440675020 CET	50540	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:22:54.467658997 CET	53	50540	8.8.8.8	192.168.2.3
Nov 19, 2020 04:23:05.045866013 CET	54366	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:23:05.058587074 CET	53	54366	8.8.8.8	192.168.2.3
Nov 19, 2020 04:23:05.807609081 CET	53034	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:23:05.821290016 CET	53	53034	8.8.8.8	192.168.2.3
Nov 19, 2020 04:23:06.510889053 CET	57762	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 04:23:06.523519039 CET	53	57762	8.8.8.8	192.168.2.3
Nov 19, 2020 04:23:07.184571028 CET	55435	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:23:07.197916031 CET	53	55435	8.8.8.8	192.168.2.3
Nov 19, 2020 04:23:16.320549965 CET	50713	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:23:16.332897902 CET	53	50713	8.8.8.8	192.168.2.3
Nov 19, 2020 04:23:20.985014915 CET	56132	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:23:21.003365040 CET	53	56132	8.8.8.8	192.168.2.3
Nov 19, 2020 04:23:51.004482031 CET	58987	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:23:51.017627001 CET	53	58987	8.8.8.8	192.168.2.3
Nov 19, 2020 04:23:52.602401972 CET	56579	53	192.168.2.3	8.8.8.8
Nov 19, 2020 04:23:52.615916014 CET	53	56579	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2336 Parent PID: 792

General

Start time:	04:22:26
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:	0x8b0000
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