ID: 320271
Sample Name:
sviluppo_economico_19__582.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:24:29
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report sviluppo_economico_19__582.xls 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
Signature Overview 4
HIPS / PFW / Operating System Protection Evasion: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 15
Static File Info 15
General 15
File Icon 15
Static OLE Info 15
General 15
OLE File "sviluppo_economico_19__582.xls" 16
Indicators 16
Summary 16
Document Summary 16
Streams 16
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 16
General 16
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 16
General 16
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 397491 16
General 17
Network Behavior 17
UDP Packets 17
Code Manipulations 18

Statistics 18
System Behavior 18
Analysis Process: EXCEL.EXE PID: 4228 Parent PID: 792 18
General 18
File Activities 18
Registry Activities 18
Disassembly 19

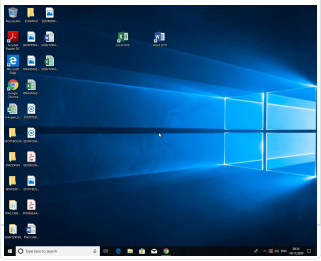
Analysis Report sviluppo_economico_19__582.xls

Overview

General Information

Sample Name:	sviluppo_economico_19__582.xls
Analysis ID:	320271
MD5:	b3b91ca3c10da9..
SHA1:	7fe3e551c432e2e..
SHA256:	be6a92f7d1f695d..
Tags:	gozi isfb italy pwmise u rsnif xls

Most interesting Screenshot:



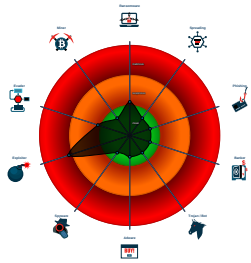
Detection

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

Signatures

Yara detected password protected x...

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 4228 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

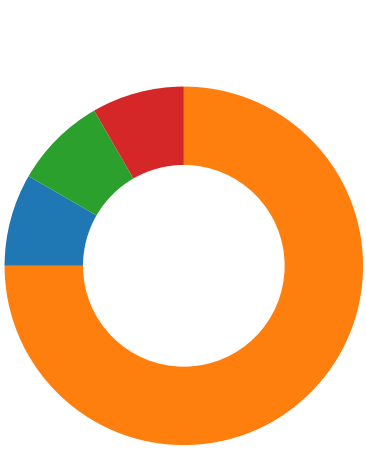
Initial Sample

Source	Rule	Description	Author	Strings
sviluppo_economico_19__582.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

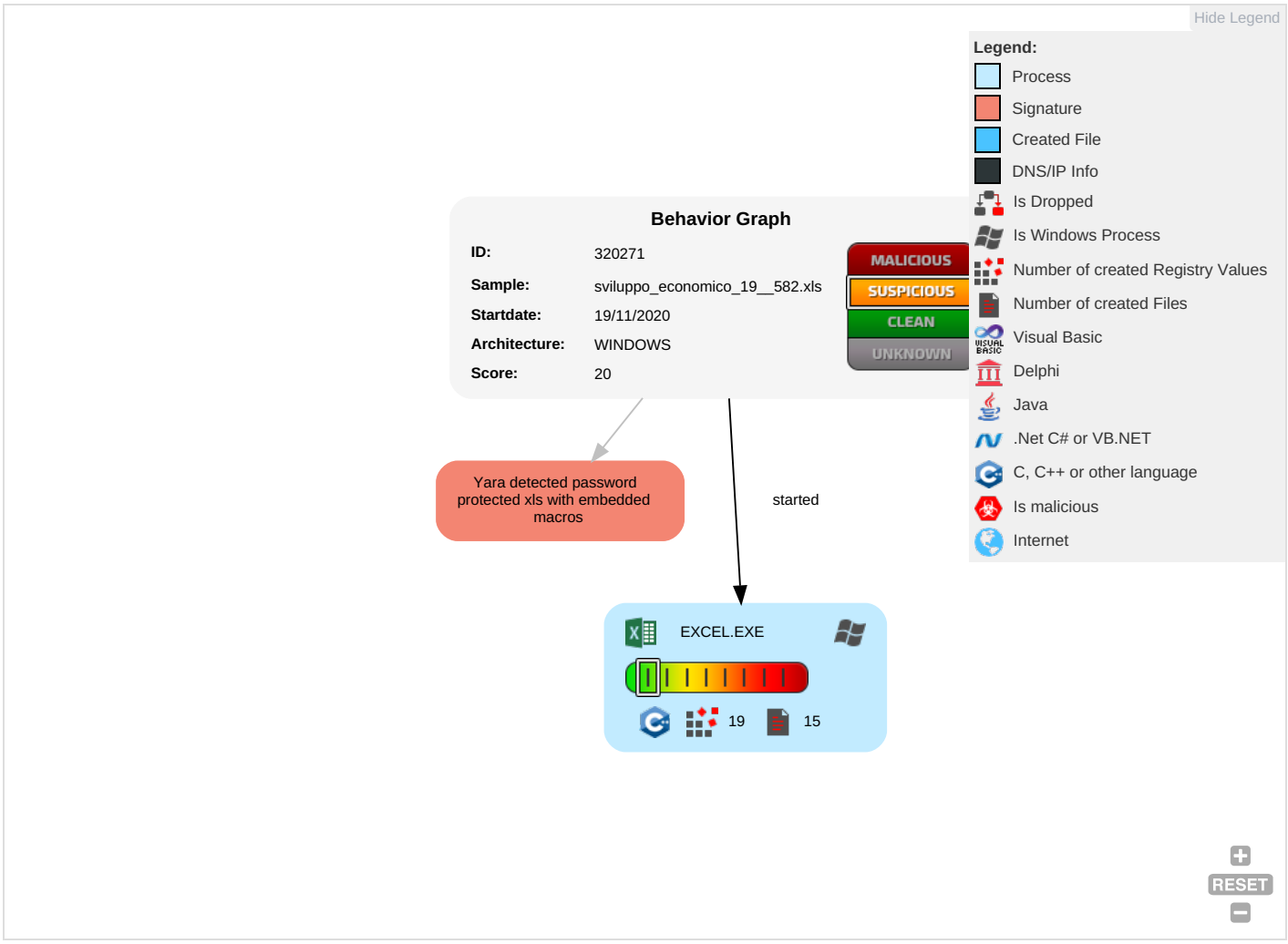
HIPS / PFW / Operating System Protection Evasion:

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

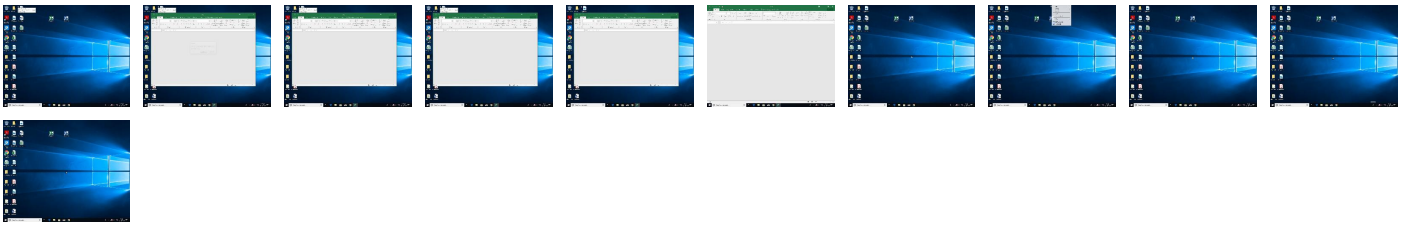
Behavior Graph



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__582.xls	9%	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	
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	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://login.microsoftonline.com/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://shell.suite.office.com:1443	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://cdn.entity.	8297EA92-5B5A-40E7-9D56-BE0D4337985D.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	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://wus2-000.contentsync.	8297EA92-5B5A-40E7-9D56-BE0D4337985D.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	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://cortana.ai	8297EA92-5B5A-40E7-9D56-BE0D4337985D.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	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://api.aadrm.com/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://api.microsoftstream.com/api/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://cr.office.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://graph.ppe.windows.net	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://store.office.cn/addinstemplate	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	8297EA92-5B5A-40E7-9D56-BE0D4337985D.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=	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	8297EA92-5B5A-40E7-9D56-BE0D4337985D.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	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://web.microsoftstream.com/video/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://graph.windows.net	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://dataservice.o365filtering.com/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://weather.service.msn.com/data.aspx	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://apis.live.net/v5.0/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.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	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://management.azure.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://outlook.office365.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://incidents.diagnostics.office.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://api.office.net	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://asgsmsproxyapi.azurewebsites.net/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://entitlement.diagnostics.office.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://autodiscover-s.outlook.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://templatelogging.office.com/client/log	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://management.azure.com/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://ncus-000.contentsync.	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://devnull.onenote.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://messaging.office.com/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://augloop.office.com/v2	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://skyapi.live.net/Activity/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.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	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://dataservice.o365filtering.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://directory.services.	8297EA92-5B5A-40E7-9D56-BE0D4337985D.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	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://onedrive.live.com/embed?	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high
http://https://augloop.office.com	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.bingapis.com/api/v7/urlpreview/search?appid=E93048236FE27D972F67C5AF722136866DF65FA2	8297EA92-5B5A-40E7-9D56-BE0D4337985D.0.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320271
Start date:	19.11.2020
Start time:	08:24:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sviluppo_economico_19__582.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:	22
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): 13.64.90.137, 52.109.88.8, 52.109.12.21, 52.109.12.22, 13.88.21.125, 52.147.198.201, 168.61.161.212, 52.255.188.83, 51.104.139.180, 23.54.113.104, 20.54.26.129, 8.248.89.254, 8.250.153.254, 8.248.133.254, 8.248.141.254, 8.247.206.126, 51.104.144.132, 23.10.249.43, 23.10.249.26, 51.11.168.160 • 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, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, 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\8297EA92-5B5A-40E7-9D56-BE0D4337985D	
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):	5.378343533771266
Encrypted:	false
SSDEEP:	1536:IcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:CmQ9DQW+zBX8u
MD5:	AEE8052C450965C7B506302AE59098B0
SHA1:	633E5FA97D805501B7A63E68F7E0423A3D4065B6
SHA-256:	2050ABBD1C0F0BC1595A20D55E906F7621A62820132A5FAB9351B14FA818CA6F
SHA-512:	ACD0AD5722B368A38D61BFD25391D66FE35B6A3A63F4F3CA627AB25B3349BDAB9822B0240B429C08AA0EAF3B63441C75E10F478F9B4512D04C8108228B8E387
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="2020-11-19T07:32:53">.. 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: jkuSNqrYfxGvb, 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 23:28:25 2020, Security: 1
Entropy (8bit):	7.664377829908077
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	sviluppo_economico_19__582.xls
File size:	410624
MD5:	b3b91ca3c10da94ad224c3a179249e3b
SHA1:	7fe3e551c432e2e3bdea3ddba8b87362e580dfb8
SHA256:	be6a92f7d1f695d18ba9e0661a1fdc3a440a7b87443cfe02a92d3f88ff08cf2c
SHA512:	12b55b17a99f6d59b0405c46d5cecb3ee655051d74928e2dff63955aff040062aa5c7409cbe94cd974ad8d895c2234172ea12bdcfb8f49bf222ef87f91ae3040
SSDEEP:	12288:UqocNxZF+FrbvNEky+0UJM1LsiE08Nyyl8o9W:qILFeNK1nyNDl6
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__582.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:	jkuSNqrYfxGvb
Last Saved By:	administrator
Create Time:	2020-11-18 22:00:31
Last Saved Time:	2020-11-18 23:28:25
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:	0.52957734561
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . h . . . . . 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 . . . . . s K k K V P h R
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 68 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 1a 01 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.331222058752
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . ` . . . . . x . . . . . j k u S N q r Y f x G v b . . . . . 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 ; . . . . @ . . . 2 . . . . .
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: 397491

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	397491
Entropy:	7.76369492327
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 . . . . . S s . U Y d e . _ .] . . T z 4 . . . K . . s . . . . . & . . . . M . . M , ... S (. * . . . I . . . . . N < . . . . \\ . p . . z , . . \\ . . q . . .
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 08:32:39.886395931 CET	63492	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:32:39.899633884 CET	53	63492	8.8.8.8	192.168.2.3
Nov 19, 2020 08:32:53.327373028 CET	60831	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:32:53.375006914 CET	53	60831	8.8.8.8	192.168.2.3
Nov 19, 2020 08:32:53.638134956 CET	60100	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:32:53.680135965 CET	53	60100	8.8.8.8	192.168.2.3
Nov 19, 2020 08:32:54.641807079 CET	60100	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:32:54.675518036 CET	53	60100	8.8.8.8	192.168.2.3
Nov 19, 2020 08:32:55.657548904 CET	60100	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:32:55.671287060 CET	53	60100	8.8.8.8	192.168.2.3
Nov 19, 2020 08:32:56.720805883 CET	53195	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:32:56.733654976 CET	53	53195	8.8.8.8	192.168.2.3
Nov 19, 2020 08:32:57.658206940 CET	60100	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:32:57.671255112 CET	53	60100	8.8.8.8	192.168.2.3
Nov 19, 2020 08:32:57.787684917 CET	50141	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:32:57.800474882 CET	53	50141	8.8.8.8	192.168.2.3
Nov 19, 2020 08:32:58.670957088 CET	53023	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:32:58.683398962 CET	53	53023	8.8.8.8	192.168.2.3
Nov 19, 2020 08:32:59.362883091 CET	49563	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:32:59.375587940 CET	53	49563	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:00.210163116 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:00.222789049 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:00.903146029 CET	59349	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:00.915853977 CET	53	59349	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:01.673763990 CET	60100	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:01.687288046 CET	53	60100	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:01.837308884 CET	57084	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:01.850414038 CET	53	57084	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:06.323082924 CET	58823	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:06.336226940 CET	53	58823	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:07.037147045 CET	57568	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:07.050311089 CET	53	57568	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:07.440414906 CET	50540	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:07.452807903 CET	53	50540	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:07.915446043 CET	54366	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:07.928471088 CET	53	54366	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:09.231560946 CET	53034	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:09.250157118 CET	53	53034	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:16.513292074 CET	57762	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:16.526757002 CET	53	57762	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:17.578903913 CET	55435	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:17.591027975 CET	53	55435	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:27.935483932 CET	50713	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 08:33:27.970251083 CET	53	50713	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:29.011394978 CET	56132	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:29.024473906 CET	53	56132	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:42.573879957 CET	58987	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:42.586471081 CET	53	58987	8.8.8.8	192.168.2.3
Nov 19, 2020 08:33:46.804490089 CET	56579	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:33:46.823556900 CET	53	56579	8.8.8.8	192.168.2.3
Nov 19, 2020 08:34:18.092844963 CET	60633	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:34:18.106056929 CET	53	60633	8.8.8.8	192.168.2.3
Nov 19, 2020 08:34:19.993172884 CET	61292	53	192.168.2.3	8.8.8.8
Nov 19, 2020 08:34:20.008012056 CET	53	61292	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 4228 Parent PID: 792

General

Start time:	08:32:52
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:	0x800000
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