ID: 320589
Sample Name:
sviluppo_economico_19__98.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 15:37:48
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report sviluppo_economico_19__98.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
AV Detection: 5
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__98.xls" 15
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: 410329 16
General 17
Network Behavior 17
UDP Packets 17
Code Manipulations 18

Statistics 18
System Behavior 18
Analysis Process: EXCEL.EXE PID: 5384 Parent PID: 792 18
General 18
File Activities 18
Registry Activities 18
Disassembly 19

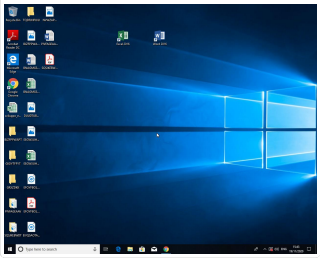
Analysis Report sviluppo_economico_19__98.xls

Overview

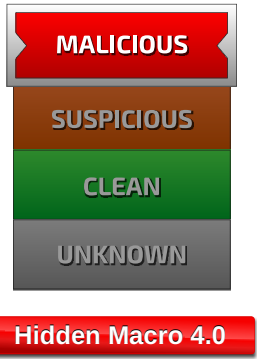
General Information

Sample Name:	sviluppo_economico_19__98.xls
Analysis ID:	320589
MD5:	f85cc34cca01836..
SHA1:	62cb04d273f22c4..
SHA256:	f93a962db6a8cfa..

Most interesting Screenshot:



Detection



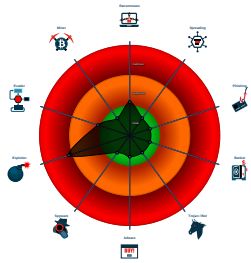
Hidden Macro 4.0

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected password protected x…
- Unable to load, office file is protecte…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5384 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

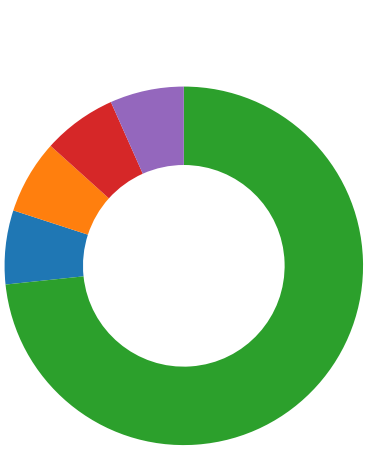
Initial Sample

Source	Rule	Description	Author	Strings
sviluppo_economico_19__98.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

AV Detection:

Multi AV Scanner detection for submitted file

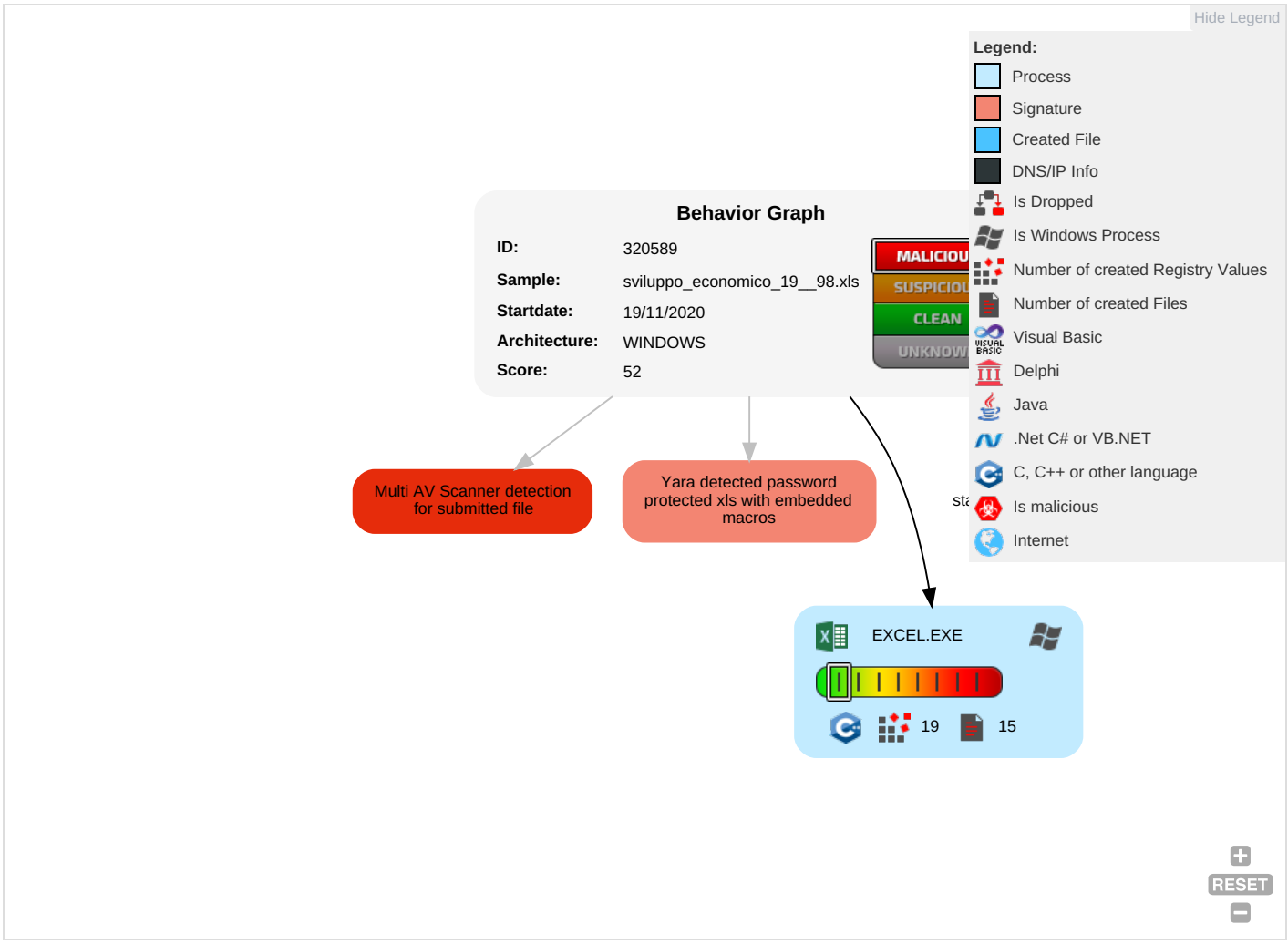
HIPS / PFW / Operating System Protection Evasion:

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

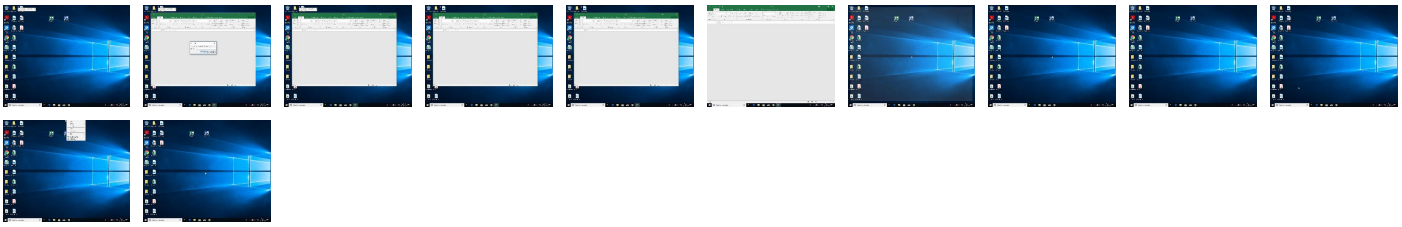
Behavior Graph



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__98.xls	8%	Virustotal		Browse
sviluppo_economico_19__98.xls	10%	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%	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	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://login.microsoftonline.com/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://shell.suite.office.com:1443	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://cdn.entity.	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://wus2-000.contentsync.	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.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	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://cortana.ai	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.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	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://api.aadrm.com/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://api.microsoftstream.com/api/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://cr.office.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://graph.ppe.windows.net	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://store.office.cn/addinstemplate	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.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=	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://web.microsoftstream.com/video/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://graph.windows.net	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://dataservice.o365filtering.com/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://weather.service.msn.com/data.aspx	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://apis.live.net/v5.0/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.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	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://management.azure.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://outlook.office365.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://incidents.diagnostics.office.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://api.office.net	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://asgsmsproxyapi.azurewebsites.net/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://entitlement.diagnostics.office.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://autodiscover-s.outlook.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://templatelogging.office.com/client/log	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://management.azure.com/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://ncus-000.contentsync.	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://devnull.onenote.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://messaging.office.com/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://augloop.office.com/v2	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://skyapi.live.net/Activity/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.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	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://dataservice.o365filtering.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://directory.services.	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://onedrive.live.com/embed?	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high
http://https://augloop.office.com	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.bingapis.com/api/v7/urlpreview/search?appid=E93048236FE27D972F67C5AF722136866DF65FA2	E0ED8BAC-9F96-4C65-A32A-441483C92CB1.0.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320589
Start date:	19.11.2020
Start time:	15:37:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sviluppo_economico_19__98.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:	26
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:	MAL
Classification:	mal52.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): 104.43.193.48, 52.147.198.201, 52.109.32.27, 52.109.12.21, 52.109.88.39, 23.210.248.85, 51.104.146.109, 205.185.216.42, 205.185.216.10, 20.54.26.129, 51.104.139.180, 92.122.213.194, 92.122.213.247, 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, 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, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, config.officeapps.live.com, 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\E0ED8BAC-9F96-4C65-A32A-441483C92CB1	
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):	5.378327306379209
Encrypted:	false
SSDEEP:	1536:1cQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:nmQ9DQW+zBX8u
MD5:	F8A7E5DD8DA49CEB2ADB7D081647669F
SHA1:	23ABC3C039FC08496CB089591B0EA707600AD768
SHA-256:	FF90EA81C7D3CB75DA4BB89382E69DADC3DFB3E2B282CDF1A9E0DF19CF2734EA
SHA-512:	7D77826784D994C9C403854E6D995F7245593AEFD2D44BDC8D939728BA80AD7AE6EF56651B9993B9A2FAF78981CCCDE1CEF2F9A2B5B61FF65F5567261AFB0F8
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="2020-11-19T14:41:32">.. 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: OXYWbyFNqEDTXZRqGxi, 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 22:26:33 2020, Security: 1
Entropy (8bit):	7.663256298038157
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	sviluppo_economico_19__98.xls
File size:	423424
MD5:	f85cc34cca018369113e5ea6aff1eae4
SHA1:	62cb04d273f22c440aca13dc344bd05ec7fb9b79
SHA256:	f93a962db6a8cfaf0513c5d2a36cf61b863c52f32ca7ab856cfe0b024001c9f3
SHA512:	434a43f2b2870596c2384fe678b24d4e2335d0c2bfd9826c23eba04d552e3791db3fa83c7ca1a574d6209ec247e0063cbc354fa3ff68029d9456d23bbb26cd98
SSDEEP:	6144:s9CdPZDiqSz9tpBWL5A4hXF+vu7lTcDHEHUEDagk6xrGgvmHfoiNzaU5AU/cp/:fdhsz7p0L++F+vfDkxagkArGBHflNu/
File Content Preview:	.....>.....9.....2...3...4...5...6...7...8.....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "sviluppo_economico_19__98.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:	OXYWbyFNqEDTXZRqGxi
Last Saved By:	administrator
Create Time:	2020-11-18 22:00:31
Last Saved Time:	2020-11-18 22:26:33
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 colspan="2">General</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>0.64107045361</td></tr>
<tr><td>Base64 Encoded:</td><td>False</td></tr>
<tr><td>Data ASCII:</td><td>. . . . . + , . . 0 . . . . P . . . . X . . . .
. d . . . . l . . . . t . . . . | . . . . h . . . .
. . . . 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 . . . . . X j z P k Y h F</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 b4 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 68 01 00 00</td></tr>
</table>

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

<table>
<tr><th colspan="2">General</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>0.348694171161</td></tr>
<tr><td>Base64 Encoded:</td><td>False</td></tr>
<tr><td>Data ASCII:</td><td>. . . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . .
. . . d . . . . | . . . . O X Y W b y F N q E D T
X Z R q G x i . . . . 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 ; . . . . @ . . . . . i . . . .</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: 410329

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	410329
Entropy:	7.75910354304
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 . . . . . a) _ . . . S . . . = . j . . . . X x . . + . ~ v ^ . p = ... R . . $ R . . B M . . . _ . . . . . _ . . . . \\ . p . k . B d 9 . . E . . B K
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 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 15:41:15.954950094 CET	64185	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:15.982069016 CET	53	64185	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:16.846503019 CET	65110	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:16.873733044 CET	53	65110	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:18.133800030 CET	58361	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:18.160774946 CET	53	58361	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:18.999408960 CET	63492	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:19.026453972 CET	53	63492	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:20.175544024 CET	60831	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:20.210936069 CET	53	60831	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:22.969084978 CET	60100	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:22.995865107 CET	53	60100	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:23.990010023 CET	53195	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:24.017407894 CET	53	53195	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:25.091245890 CET	50141	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:25.118285894 CET	53	50141	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:30.995492935 CET	53023	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:31.022440910 CET	53	53023	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:32.140877962 CET	49563	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:32.189080000 CET	53	49563	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:32.499978065 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:32.552670002 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:33.507258892 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:33.631208897 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:34.520112991 CET	59349	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:34.521812916 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:34.547127008 CET	53	59349	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:34.558454990 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:35.411463976 CET	57084	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:35.438574076 CET	53	57084	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:36.062640905 CET	58823	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:36.089689970 CET	53	58823	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:36.538332939 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:36.573633909 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:36.805690050 CET	57568	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:36.840802908 CET	53	57568	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:40.553368092 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:40.588821888 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:44.411493063 CET	50540	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:44.447098017 CET	53	50540	8.8.8.8	192.168.2.3
Nov 19, 2020 15:41:48.886693001 CET	54366	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:41:48.913783073 CET	53	54366	8.8.8.8	192.168.2.3
Nov 19, 2020 15:42:05.769618034 CET	53034	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 15:42:05.796716928 CET	53	53034	8.8.8.8	192.168.2.3
Nov 19, 2020 15:42:07.689606905 CET	57762	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:42:07.716733932 CET	53	57762	8.8.8.8	192.168.2.3
Nov 19, 2020 15:42:23.700062037 CET	55435	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:42:23.727077961 CET	53	55435	8.8.8.8	192.168.2.3
Nov 19, 2020 15:42:30.277544022 CET	50713	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:42:30.314619064 CET	53	50713	8.8.8.8	192.168.2.3
Nov 19, 2020 15:42:58.444713116 CET	56132	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:42:58.471815109 CET	53	56132	8.8.8.8	192.168.2.3
Nov 19, 2020 15:43:32.474759102 CET	58987	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:43:32.501848936 CET	53	58987	8.8.8.8	192.168.2.3
Nov 19, 2020 15:43:34.965167046 CET	56579	53	192.168.2.3	8.8.8.8
Nov 19, 2020 15:43:35.002229929 CET	53	56579	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 5384 Parent PID: 792

General

Start time:	15:41:30
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:	0xbd0000
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