ID: 320546
Sample Name: SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:21:30
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

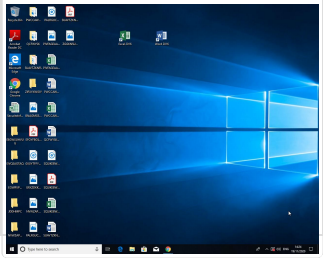
Analysis Report SecuriteInfo.com.Macro.Trojan-Downlo…

Overview

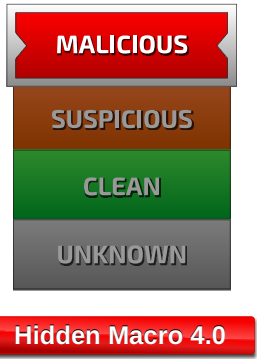
General Information

Sample Name:	SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.xls
Analysis ID:	320546
MD5:	66de86a7d9ba80..
SHA1:	8c0dcef8ad7aeb1..
SHA256:	bc3b0df0a90971d.

Most interesting Screenshot:



Detection



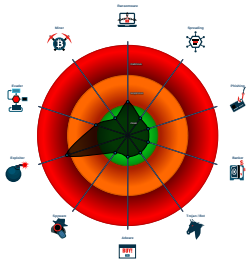
Hidden Macro 4.0

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

Signatures

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

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 4120 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

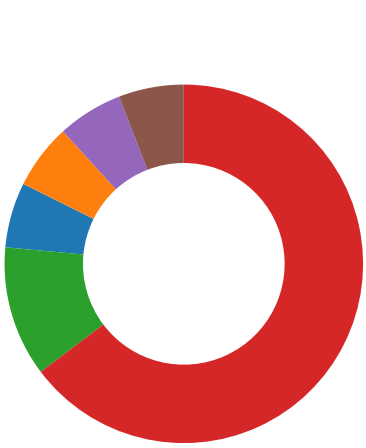
Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.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

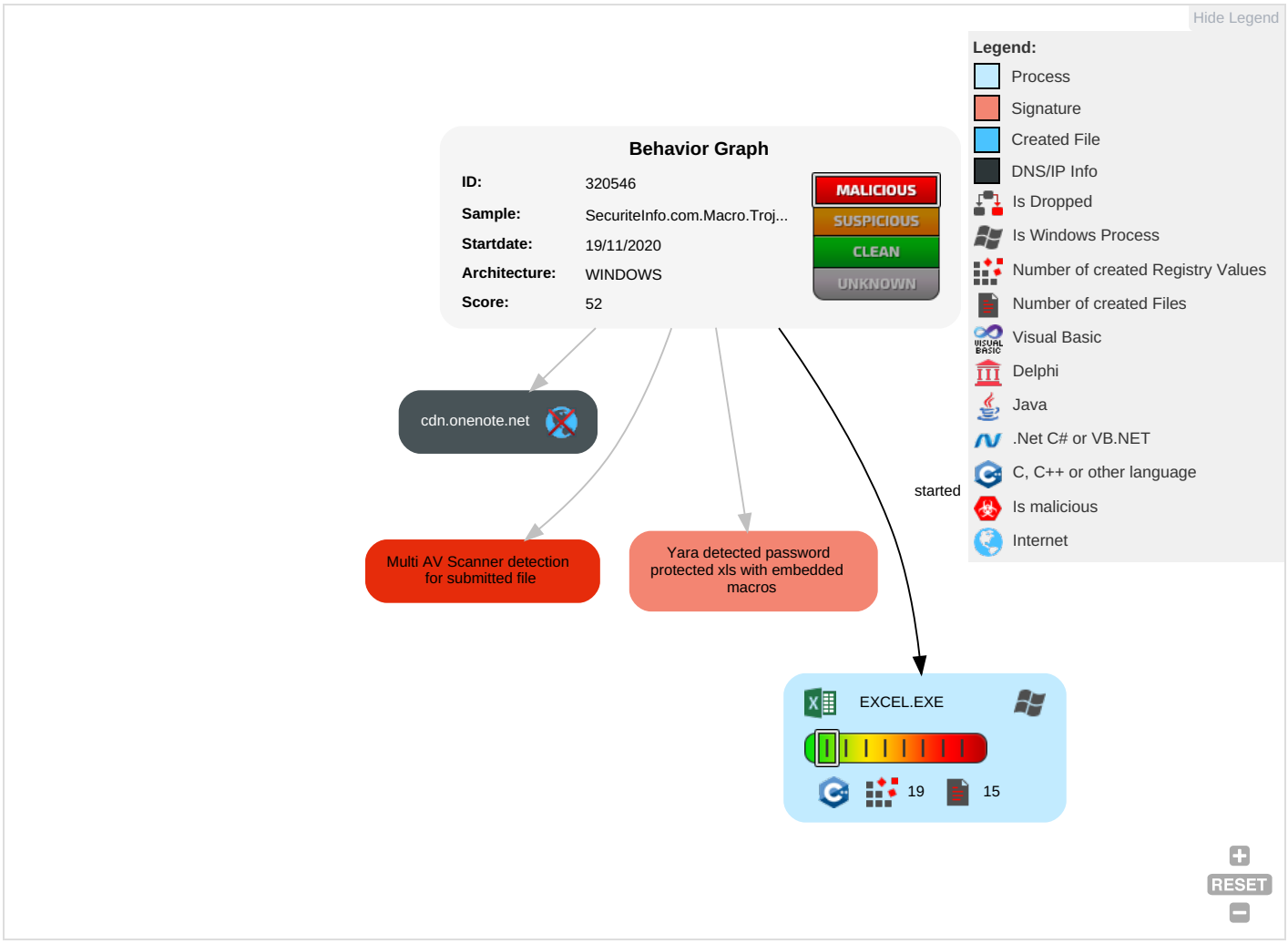
HIPS / PFW / Operating System Protection Evasion:

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	Exploitation for Client Execution 1	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	Non-Application Layer Protocol 1	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	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

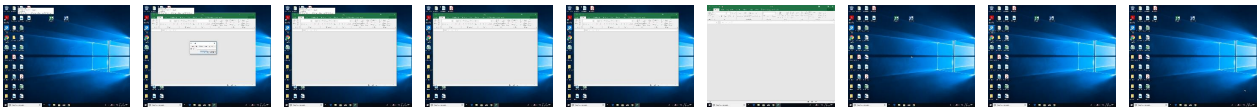
Behavior Graph



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
SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.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	
http://https://wus2-000.contentsync.	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://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://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://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://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%	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://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://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://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://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://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%	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://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://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	

Source	Detection	Scanner	Label	Link
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.onenote.net	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://login.microsoftonline.com/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://shell.suite.office.com:1443	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://cdn.entity.	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://wus2-000.contentsync.	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://powerlift.acompli.net	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://cortana.ai	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://api.aadrm.com/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://api.microsoftstream.com/api/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://cr.office.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://graph.ppe.windows.net	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://store.office.cn/addinstemplate	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://web.microsoftstream.com/video/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://graph.windows.net	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://dataservice.o365filtering.com/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://weather.service.msn.com/data.aspx	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://apis.live.net/v5.0/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://management.azure.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://outlook.office365.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://incidents.diagnostics.office.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://api.office.net	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://entitlement.diagnostics.office.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://autodiscover-s.outlook.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://templatelogging.office.com/client/log	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://management.azure.com/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://ncus-000.contentsync.	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://devnull.onenote.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://messaging.office.com/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://augloop.office.com/v2	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://skyapi.live.net/Activity/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://dataservice.o365filtering.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://directory.services.	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://onedrive.live.com/embed?	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://augloop.office.com	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high
http://https://www.bingapis.com/api/v7/urlpreview/search?appid=E93048236FE27D972F67C5AF722136866DF65FA2	9A117202-9EA1-4504-99F4-F46D76CBF970.0.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320546
Start date:	19.11.2020
Start time:	14:21:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.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:	MAL
Classification:	mal52.expl.winXLS@1/1@1/0

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): 104.42.151.234, 52.109.32.27, 52.109.88.39, 104.43.193.48, 52.109.8.25, 51.132.208.181, 104.84.56.60, 23.14.92.88, 23.14.92.27, 20.54.26.129, 104.108.60.202, 104.123.31.226, 51.11.168.160, 2.16.106.105, 2.16.106.113, 51.104.144.132 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, 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, e15275.g.akamaiedge.net, a1449.dscg2.akamai.net, arc.msn.com, cdn.onenote.net.edgekey.net, wildcard.weather.microsoft.com.edgekey.net, audownload.windowsupdate.nsatc.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, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, config.officeapps.live.com, e1553.dspg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/320546/sample/SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.xls

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\9A117202-9EA1-4504-99F4-F46D76CBF970	
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):	5.378315015594326
Encrypted:	false
SSDEEP:	1536:pcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:jmQ9DQW+zBX8u
MD5:	5415095E50480ADD9F231767F987AFA2
SHA1:	9426458D50397B697133055E46445FD1A2C057AB
SHA-256:	95743C94995233DBC0AB7F21927DA0979ADF10C46CD22BAB3852BF469095FB72
SHA-512:	F0B550E4B281AD837901C0FEC9BC7CDB2762C9FB8F8D19A99E3D205565918A02D65C3A2792CDDFDDEA49366126B591436D10EB8AF73684C0A551E724709830E
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="2020-11-19T13:22:32">.. Build: 16.0.13517.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: bOpMKmUlXbBbmg, 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 23:17:00 2020, Security: 1
Entropy (8bit):	7.6578858889050165
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.xls
File size:	418304
MD5:	66de86a7d9ba80c175fe166a81d25c4d
SHA1:	8c0dcef8ad7aeb1e77bc8a18f19d270af61c94e3
SHA256:	bc3b0df0a90971d83f87af531671216d238ce21b6272aa2758b178cbb1320276
SHA512:	c7b1885f70898bf90e677962c595df8d6d1a7b840a9c14647957726c59f67c4b8073c1a2289143dca6e92b58ec9f32e574b6f365c5315500c7eee3eeec6bd8a6
SSDEEP:	12288:t6Qtw5NtDtkd1zsRXSqUXVIF/MZX3BhAOepArPmHQeq:G5bpY1zstSNXuVKX4OepArMJq
File Content Preview:	.....>...../.....(...)...*.....+...,...-.....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.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:	bOpMKmUlXbBbmg
Last Saved By:	administrator
Create Time:	2020-11-18 22:00:31
Last Saved Time:	2020-11-18 23:17:00
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:	0.839708850949
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 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 . . . . . E T M v d g B d
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 4c 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 01 02 00 00

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

General	
Stream Path:	\x5SummaryInformation

General	
File Type:	data
Stream Size:	4096
Entropy:	0.327276850068
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . ` . . . . . x . . . . . b O p M K m U l X b B b r g . . . . . 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 ; . . . . @ . . . . ~ . . . . .
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: 405135

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	405135
Entropy:	7.75501180979
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 . . . . . D . I r " . . . v f \ \ . W p . . . . . t . . - . . . 1 . . . . . . m . . . 7 F V - . ! .) . # . . . . . \ \ . p . . . . . 7 . * . ` . / .
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 14:22:30.767960072 CET	50620	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:30.795135021 CET	53	50620	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:31.854453087 CET	64938	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:31.891474009 CET	53	64938	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:32.189357042 CET	60152	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:32.246296883 CET	53	60152	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:32.967861891 CET	57544	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:32.994967937 CET	53	57544	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:33.188743114 CET	60152	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:33.226749897 CET	53	60152	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:34.214438915 CET	60152	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:34.249897957 CET	53	60152	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:36.220263004 CET	60152	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:36.257525921 CET	53	60152	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:38.014018059 CET	55984	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:38.041222095 CET	53	55984	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:38.988238096 CET	64185	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:39.023794889 CET	53	64185	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:39.849150896 CET	65110	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:39.876204014 CET	53	65110	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:40.220809937 CET	60152	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:40.256076097 CET	53	60152	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:40.994908094 CET	58361	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:41.030278921 CET	53	58361	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:43.892469883 CET	63492	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:43.919558048 CET	53	63492	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:47.841114998 CET	60831	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:47.868073940 CET	53	60831	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:48.725825071 CET	60100	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 14:22:48.763019085 CET	53	60100	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:54.273874044 CET	53195	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:54.300936937 CET	53	53195	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:55.275489092 CET	50141	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:55.302467108 CET	53	50141	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:56.093519926 CET	53023	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:56.131140947 CET	53	53023	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:57.305331945 CET	49563	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:57.332411051 CET	53	49563	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:58.262403011 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:58.289391994 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 14:22:59.093350887 CET	59349	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:22:59.128614902 CET	53	59349	8.8.8.8	192.168.2.3
Nov 19, 2020 14:23:00.815629959 CET	57084	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:23:00.861135960 CET	53	57084	8.8.8.8	192.168.2.3
Nov 19, 2020 14:23:01.821779013 CET	58823	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:23:01.848959923 CET	53	58823	8.8.8.8	192.168.2.3
Nov 19, 2020 14:23:03.415399075 CET	57568	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:23:03.442403078 CET	53	57568	8.8.8.8	192.168.2.3
Nov 19, 2020 14:23:05.492049932 CET	50540	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:23:05.519011021 CET	53	50540	8.8.8.8	192.168.2.3
Nov 19, 2020 14:23:06.555135965 CET	54366	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:23:06.582597017 CET	53	54366	8.8.8.8	192.168.2.3
Nov 19, 2020 14:23:07.593278885 CET	53034	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:23:07.620311022 CET	53	53034	8.8.8.8	192.168.2.3
Nov 19, 2020 14:23:07.851814032 CET	57762	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:23:07.891577005 CET	53	57762	8.8.8.8	192.168.2.3
Nov 19, 2020 14:23:08.162103891 CET	55435	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:23:08.206183910 CET	53	55435	8.8.8.8	192.168.2.3
Nov 19, 2020 14:23:20.706362009 CET	50713	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:23:20.706922054 CET	56132	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:23:20.743141890 CET	53	50713	8.8.8.8	192.168.2.3
Nov 19, 2020 14:23:20.754509926 CET	53	56132	8.8.8.8	192.168.2.3
Nov 19, 2020 14:23:22.735336065 CET	58987	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:23:22.762392998 CET	53	58987	8.8.8.8	192.168.2.3
Nov 19, 2020 14:23:28.462939978 CET	56579	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:23:28.504091024 CET	53	56579	8.8.8.8	192.168.2.3
Nov 19, 2020 14:23:57.168675900 CET	60633	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:23:57.195882082 CET	53	60633	8.8.8.8	192.168.2.3
Nov 19, 2020 14:24:31.111319065 CET	61292	53	192.168.2.3	8.8.8.8
Nov 19, 2020 14:24:31.138313055 CET	53	61292	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 19, 2020 14:23:20.706362009 CET	192.168.2.3	8.8.8.8	0xeee5	Standard query (0)	cdn.onenote.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 14:23:20.743141890 CET	8.8.8.8	192.168.2.3	0xeee5	No error (0)	cdn.onenote.net	cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 4120 Parent PID: 792

General

Start time:	14:22:30
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:	0x360000
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