ID: 324310
Sample Name: document-1387828094.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 05:08:23
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

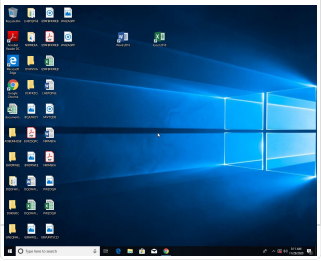
Analysis Report document-1387828094.xls

Overview

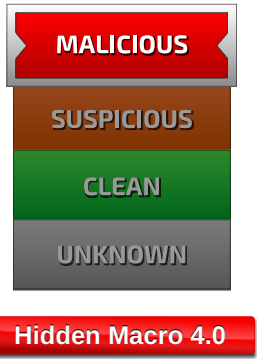
General Information

Sample Name:	document-1387828094.xls
Analysis ID:	324310
MD5:	57d6ae1173dbde..
SHA1:	2cdfca3712f5310..
SHA256:	4a1096abdae4eb..
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection

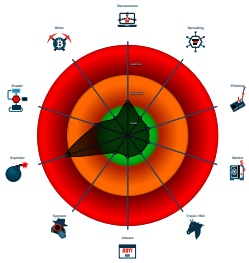


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected hidden Macro 4.0 in E…
- Document contains embedded VBA …
- Yara signature match

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 3984 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

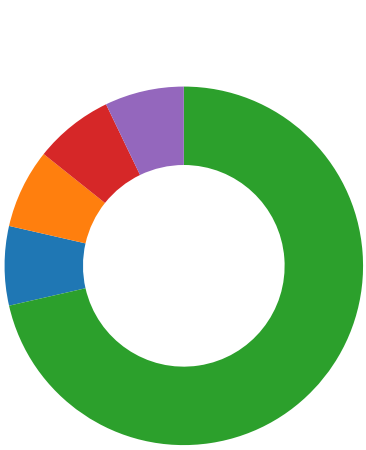
Initial Sample

Source	Rule	Description	Author	Strings
document-1387828094.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x502a2:$s1: Excel • 0x5131d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1387828094.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	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

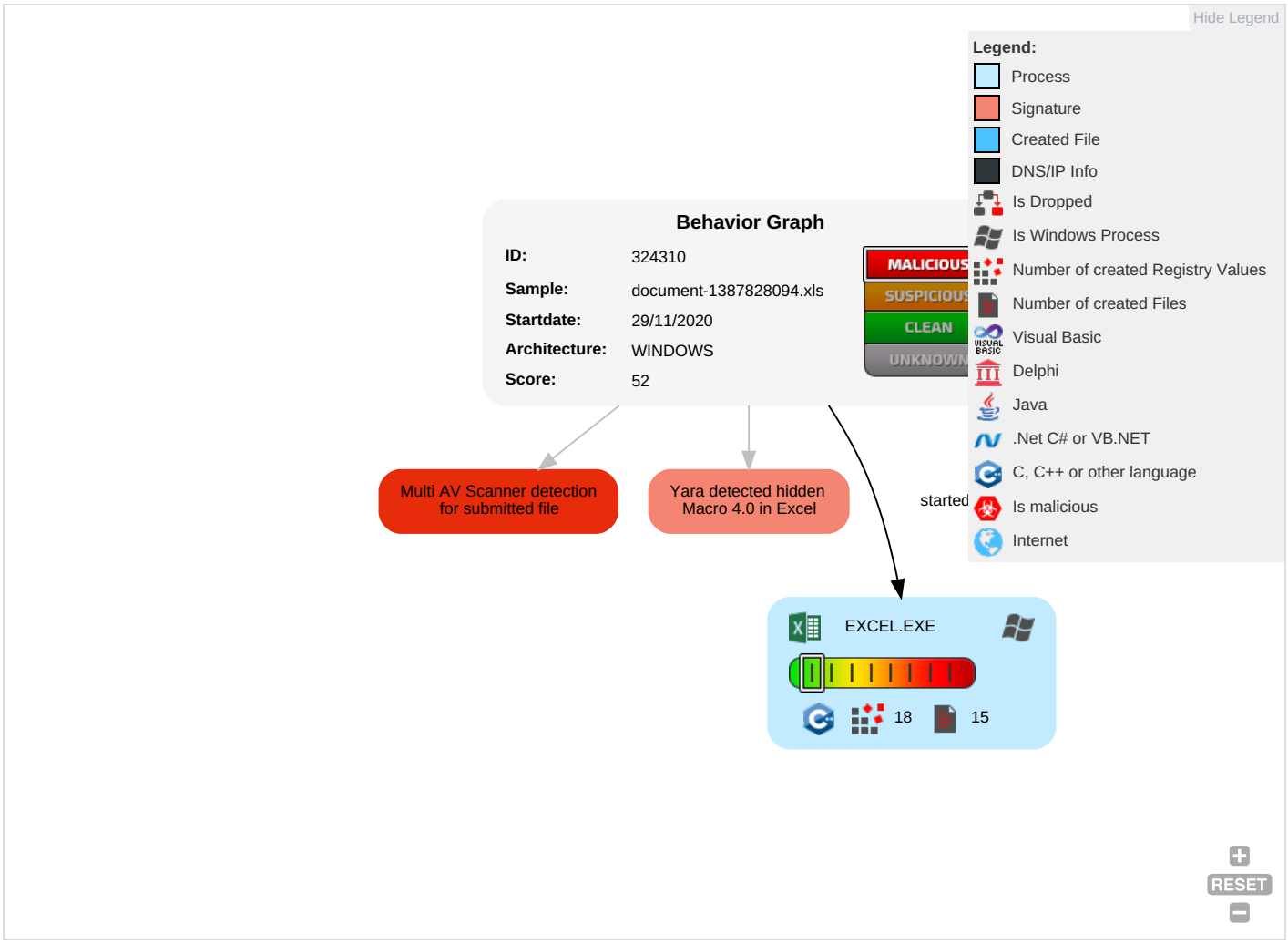
HIPS / PFW / Operating System Protection Evasion:

Yara detected hidden Macro 4.0 in Excel

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	Scripting 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	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	Scripting 1	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

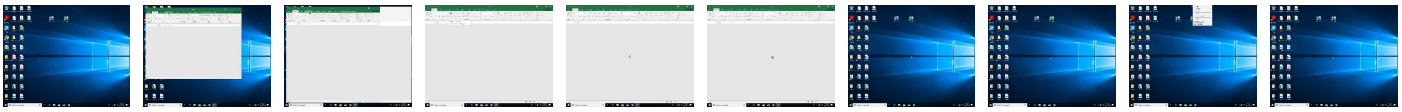
Behavior Graph



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
document-1387828094.xls	34%	Virustotal		Browse
document-1387828094.xls	11%	Metadefender		Browse
document-1387828094.xls	4%	ReversingLabs	Document-Word.Trojan.Heuristic	

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	

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	
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	

Source	Detection	Scanner	Label	Link
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://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	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://login.microsoftonline.com/	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://shell.suite.office.com:1443	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http:// https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://cdn.entity.	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://wus2-000.contentsync.	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.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	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http:// https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://cortana.ai	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.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	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://api.aadrm.com/	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://api.microsoftstream.com/api/	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://cr.office.com	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://graph.ppe.windows.net	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://store.office.cn/addinstemplate	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.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=	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	1C773311-3E6C-4F87-80CE-C57F90 4403B3.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://web.microsoftstream.com/video/	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://graph.windows.net	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://dataservice.o365filtering.com/	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://weather.service.msn.com/data.aspx	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://apis.live.net/v5.0/	1C773311-3E6C-4F87-80CE-C57F904403B3.0.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	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://management.azure.com	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://outlook.office365.com	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://incidents.diagnostics.office.com	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.office.net	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://entitlement.diagnostics.office.com	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://autodiscover-s.outlook.com	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://templatelogging.office.com/client/log	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://management.azure.com/	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://ncus-000.contentsync.	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://devnull.onenote.com	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://messaging.office.com/	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://augloop.office.com/v2	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://skyapi.live.net/Activity/	1C773311-3E6C-4F87-80CE-C57F904403B3.0.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	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://dataservice.o365filtering.com	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://directory.services.	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/embed?	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://augloop.office.com	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high
http://https://www.bingapis.com/api/v7/urlpreview/search?appid=E93048236FE27D972F67C5AF722136866DF65FA2	1C773311-3E6C-4F87-80CE-C57F904403B3.0.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324310
Start date:	29.11.2020
Start time:	05:08:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1387828094.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:	15
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 • 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): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.147.198.201, 52.109.76.68, 52.109.12.24, 52.109.88.39, 51.104.139.180, 52.155.217.156, 20.54.26.129, 13.107.4.50, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, elasticShed.au.au-msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, Edge-Prod-FRAr4a.env.au.au-msedge.net, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, skypedataprdcolcus16.cloudapp.net, afdap.au.au-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, au.au-msedge.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, au.c-0001.c-msedge.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\1C773311-3E6C-4F87-80CE-C57F904403B3	
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):	5.3783319566990135
Encrypted:	false
SSDEEP:	1536:IcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:CmQ9DQW+zBX8u
MD5:	7E4ECCBC1F6FD20BD6C423FA6663D077
SHA1:	A2D36CDB3FD96A1E2C25845A122347D22AD07DD2
SHA-256:	72A05080D2EFC679FD28C41B8A39C8F1547E460EE40047B1F2983BD7C42B0057
SHA-512:	F828D068E62530971B6B1EAF049A29EF404C62316EEB0487B1EF6B6C74C578E1FA6043F26D1F72A031104274FD52D55234C03D6DCA30CE2414534CC84A1A2C6E
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="2020-11-29T04:09:16">.. Build: 16.0.13518.30530-->.. <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 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Thu Nov 26 09:46:44 2020, Security: 0
Entropy (8bit):	7.520323755270079
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1387828094.xls
File size:	339968
MD5:	57d6ae1173dbde7042f89a088de5edb7
SHA1:	2cdfca3712f53104813befb773da278cbe0ff191
SHA256:	4a1096abdae4eb29f96055f0a4b385c8b6edabda3b6b4b0e20490730156bb0a4
SHA512:	9adeba88d565068f75b8989445ceaf5d722f451641c7d3e10bd798448ae6e0e12b22d8aff89cadbefbb7fe0520031c75e2b2b8b7111a3076b4aa461a9061fcd9
SSDEEP:	6144:+cKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDphYHceXVhca+fMHLty/x2zZ8kpTB:5izo8RnsIROnr6n75YL
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1387828094.xls"

Indicators	
Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
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:	True

Summary	
Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2020-11-26 09:46:44
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.367004077607
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . D o c u S i g n . . . . . 2 . . . . . 3 . . . . . 1 . . . . . 4 . . . . . 5 . . . . .
Data Raw:	fe ff 00 00 06 02 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 00 01 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 bf 00 00 00 02 00 00 00 e3 04 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.247032988068
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . T . . . . . ` . . . . . x . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . .
Data Raw:	fe ff 00 00 06 02 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 98 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 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 327649

General	
Stream Path:	Workbook

General	
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	327649
Entropy:	7.64867991795
Base64 Encoded:	True
Data ASCII:	. . . . f 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... l . . 9 P . 8 . . . . X . @ . . . . . .
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:09:04.015887976 CET	58028	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:04.043137074 CET	53	58028	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:04.837342978 CET	53097	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:04.864639997 CET	53	53097	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:05.537745953 CET	49257	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:05.565011024 CET	53	49257	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:06.313126087 CET	62389	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:06.351083040 CET	53	62389	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:07.113490105 CET	49910	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:07.149471998 CET	53	49910	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:15.051103115 CET	55854	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:15.078393936 CET	53	55854	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:16.124699116 CET	64549	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:16.146138906 CET	63153	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:16.161917925 CET	53	64549	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:16.181667089 CET	53	63153	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:16.452836990 CET	52991	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:16.489659071 CET	53	52991	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:17.459712029 CET	52991	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:17.495387077 CET	53	52991	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:18.440530062 CET	53700	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:18.475581884 CET	52991	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:18.476108074 CET	53	53700	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:18.510972977 CET	53	52991	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:19.267682076 CET	51726	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:19.295046091 CET	53	51726	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:20.110950947 CET	56794	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:20.138197899 CET	53	56794	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:20.491274118 CET	52991	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:20.527045012 CET	53	52991	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:20.913595915 CET	56534	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:20.940674067 CET	53	56534	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:21.758735895 CET	56627	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:21.785976887 CET	53	56627	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:22.392211914 CET	56621	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:22.419517994 CET	53	56621	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:23.204847097 CET	63116	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:23.240644932 CET	53	63116	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:24.013089895 CET	64078	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:24.040333033 CET	53	64078	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:24.507472038 CET	52991	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:24.542751074 CET	53	52991	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:24.787770987 CET	64801	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:24.814977884 CET	53	64801	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:27.631225109 CET	61721	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:09:27.666719913 CET	53	61721	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:28.299324036 CET	51255	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:28.326615095 CET	53	51255	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:28.930866957 CET	61522	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:28.966521978 CET	53	61522	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:29.119544983 CET	52337	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:29.154874086 CET	53	52337	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:44.472450018 CET	55046	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:44.560653925 CET	53	55046	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:45.128050089 CET	49612	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:45.163722038 CET	53	49612	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:45.579868078 CET	49285	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:45.630911112 CET	53	49285	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:45.907833099 CET	50601	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:45.945698977 CET	53	50601	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:46.280572891 CET	60875	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:46.316061974 CET	53	60875	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:46.453322887 CET	56448	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:46.497332096 CET	53	56448	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:46.704287052 CET	59172	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:46.740259886 CET	53	59172	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:47.265758038 CET	62420	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:47.301377058 CET	53	62420	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:47.826761961 CET	60579	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:47.854145050 CET	53	60579	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:48.519301891 CET	50183	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:48.554735899 CET	53	50183	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:48.845201015 CET	61531	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:48.880963087 CET	53	61531	8.8.8.8	192.168.2.4
Nov 29, 2020 05:09:54.245727062 CET	49228	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:09:54.273006916 CET	53	49228	8.8.8.8	192.168.2.4
Nov 29, 2020 05:10:03.237773895 CET	59794	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:10:03.265039921 CET	53	59794	8.8.8.8	192.168.2.4
Nov 29, 2020 05:10:03.518582106 CET	55916	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:10:03.568784952 CET	53	55916	8.8.8.8	192.168.2.4
Nov 29, 2020 05:10:05.896732092 CET	52752	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:10:05.933795929 CET	53	52752	8.8.8.8	192.168.2.4
Nov 29, 2020 05:10:38.796318054 CET	60542	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:10:38.823630095 CET	53	60542	8.8.8.8	192.168.2.4
Nov 29, 2020 05:10:40.686410904 CET	60689	53	192.168.2.4	8.8.8.8
Nov 29, 2020 05:10:40.722014904 CET	53	60689	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 3984 Parent PID: 800

General

Start time:	05:09:14

Start date:	29/11/2020
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:	0x930000
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