ID: 791304
Sample Name:
101POH0000000166.rtf
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:06:51
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

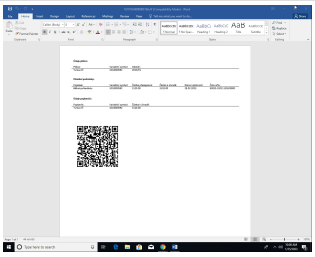
Windows Analysis Report

101POH0000000166.rtf

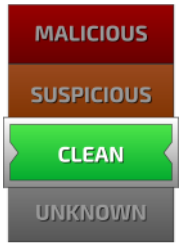
Overview

General Information

Sample Name:	101POH0000000166.rtf
Analysis ID:	791304
MD5:	5241cc04162b71..
SHA1:	3a9e51c888314e..
SHA256:	5dcd3d5273d069..
Infos:	



Detection

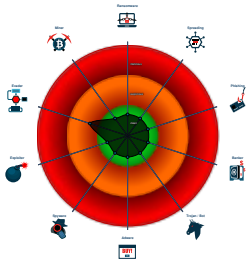


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Sample execution stops while proce…
- Found a high number of Window / U…
- Document misses a certain OLE str…

Classification



Analysis Advice

No malicious behavior found, analyze the document also on other version of Office / Acrobat

Sample monitors window changes (e.g. starting applications), analyze the sample with the 'Simulates keyboard and window changes' cookbook

Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 5888 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - splwow64.exe (PID: 5060 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

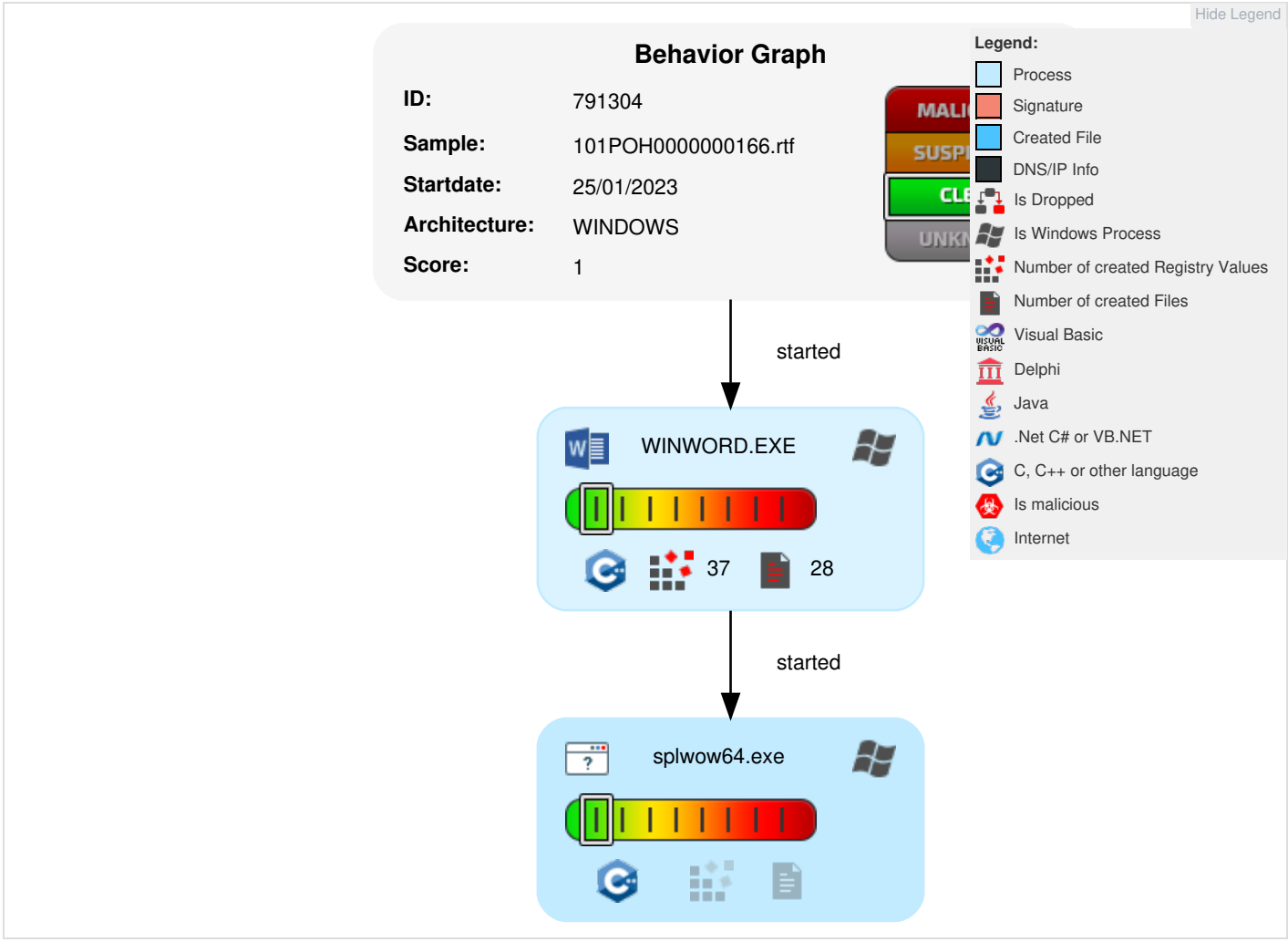
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

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	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 Virtualization/Sandbox Evasion	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

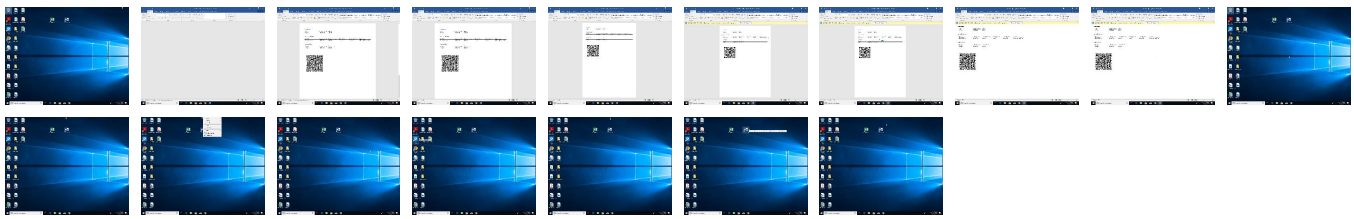
Behavior Graph

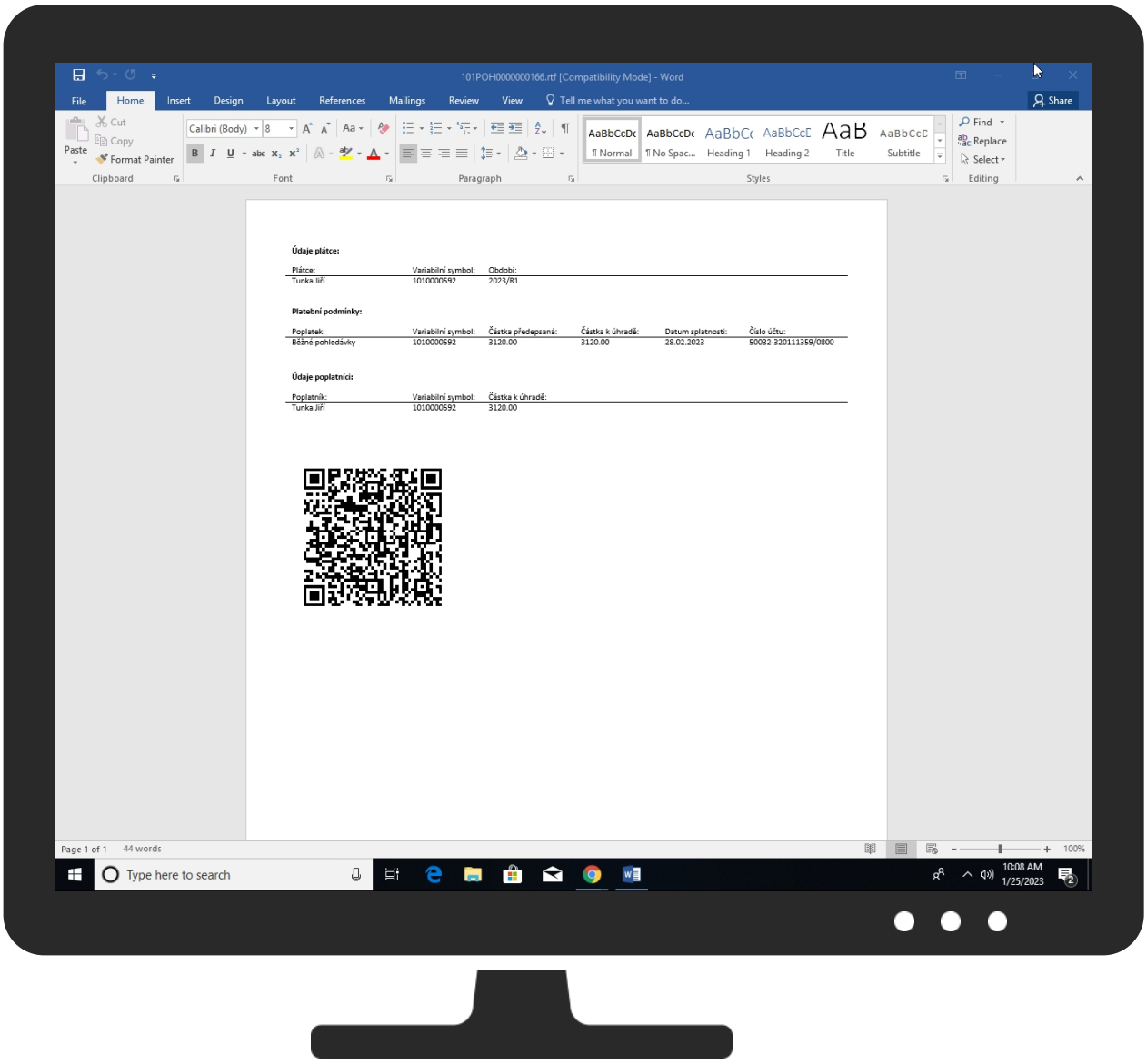


Screenshots

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
101POH0000000166.rtf	0%	Virustotal		Browse

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://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	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://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://api.scheduler.	0%	URL Reputation	safe	
http://https://my.microsoftpersonalcontent.com	0%	URL Reputation	safe	
http://https://my.microsoftpersonalcontent.com	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	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://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.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://d.docs.live.net	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://wus2.contentsync.	0%	URL Reputation	safe	
http://https://make.powerautomate.com	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://login.microsoftonline.com/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://shell.suite.office.com:1443	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://autodiscover-s.outlook.com/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://cdn.entity.	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://powerlift.acompli.net	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://cortana.ai	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://api.aadrm.com/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://api.microsoftstream.com/api/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://cr.office.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://graph.ppe.windows.net	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://api.scheduler.	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://my.microsoftpersonalcontent.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://messaging.engagement.office.com/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://web.microsoftstream.com/video/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://dataservice.o365filtering.com/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://consent.config.office.com/consentcheckin/v1.0/consents	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://d.docs.live.net	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://ncus.contentsync.	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://weather.service.msn.com/data.aspx	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://apis.live.net/v5.0/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://messaging.lifecycle.office.com/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://pushchannel.1drv.ms	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://management.azure.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://outlook.office365.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://wus2.contentsync.	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://make.powerautomate.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/odc/insertmedia	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://api.office.net	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://entitlement.diagnostics.office.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://outlook.office.com/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://outlook.office365.com/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://webshell.suite.office.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://management.azure.com/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://devnull.onenote.com	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high
http://https://messaging.action.office.com/	913A360A-E69B-44A8-AAEF-E0FC3C105644.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	791304
Start date and time:	2023-01-25 10:06:51 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	101POH0000000166.rtf
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
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:	CLEAN
Classification:	clean1.winRTF@3/11@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .rtf • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.109.76.141, 20.126.111.161, 20.25.84.51
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, config.officeapps.live.com, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, nexus.officeapps.live.com, officeclient.microsoft.com, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
10:08:18	API Interceptor	831x Sleep call for process: splwow64.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

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\913A360A-E69B-44A8-AAEF-E0FC3C105644

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	151918
Entropy (8bit):	5.356066360620777
Encrypted:	false
SSDEEP:	1536:u+C7/gfYB5BQguwULQ9DQN+zQVk4F77nXmvidlXRHE6Lcz6I:CmQ9DQN+zwXeI
MD5:	8B7A4BB6EDE458DDFF3DA534D9EF4EBE
SHA1:	8137EBDC29DAD252FFB8A29CADFE40B3B5BB49D7
SHA-256:	37EDD3EA1C817DDA8D2BB9F7CB1EB79B97BE1555A9DC618AB728185E68DB9002
SHA-512:	4D3FD220B4D631F781C567DE6B0CF724A4DF6627DB25F269FF6C34C238432CCA8FF4424CB6DF7969AB8B519FE3A3E2A1885D6362D7B62E9B9DB21DF5ACCC0451
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="2023-01-25T09:07:46">.. Build: 16.0.16116.30525-->.. <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:authentication="1">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. <o:ticket o:policy="MBI_SSL_SHORT" o:idprovider="1" o:target="[MAX.AuthHost]" o:headerValue="Passport1.4 from-PP='{}&p=''" />.. <o:ticket o:idprovider="3" o:headerValue="Bearer {}" o:resourceId="[MAX.ResourceId]" o:authorityUrl="[ADALAuthorityU

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3C004465.wmf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

File Type:	Windows metafile
Category:	dropped
Size (bytes):	478
Entropy (8bit):	3.2862654741844266
Encrypted:	false
SSDEEP:	12:MuU6p0HnM+vdd81lHZsflpgtjsXFb/BQ9/OK51lHNTbCUG6mt:5V0s+vdd/syXFq9/jbXLi
MD5:	FB5F72BAEA228ED186CF1FE0860855E5
SHA1:	6FC93D61DC7471038C2F583DBF6FD130B49EFDED
SHA-256:	9B4486623D83E0DE5271E37EDA5BDD53129D84A7B082B5A085555BBE2A9445D6
SHA-512:	EDB58C937D5A4FF6C56C31A602BF911761E1569F2BFDA3AD7CC47C1D0D83E64B779170478D3CDF09EA3B514BD130B644B14F023F8902A2098F217EF7611A3B3 1
Malicious:	false
Reputation:	low
Preview:	.....@."Calibri.....-.....-.....-.....2.T..... .6.....-.....-.....%..... .....-.....-.....'.....2.Z.C..... .6.....'....."System..8....._n...Xs....._n.....-.....-.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\533700F4.wmf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Windows metafile
Category:	dropped
Size (bytes):	478
Entropy (8bit):	3.284842812454819
Encrypted:	false
SSDEEP:	12:MuU6p0HnM+vdd81lHCpjsXFb/BQ9/OKJ1lHfUTbvUtS6mt:5V0s+vddkXFq9/8bMdi
MD5:	8BE490498AB15138A6F7118CCA6DD943
SHA1:	B868098E3FF295849ED403EFD31DBA8640BA98EA
SHA-256:	82AF4F0BCF67F9C2CB58A4D8225269A9D9E2FC64CD5388B9C94EBE1DFB0148C5
SHA-512:	05B477111DFBB7EE82B77E04073C45D108A0942323F1B08219302AB3925E605967C257AD6C2C0CB5FAF6C46159EE7209A79BB29EABD1A2B81513AA9DD1D6BF1 9
Malicious:	false
Reputation:	low
Preview:	.....@."Calibri.....-.....-.....-.....2.S..... .6.....-.....-.....%..... .....-.....-.....'.....2.Y.C..... .6.....'....."System..P....._n...Xs....._n.....-.....-.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D520B722.wmf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Windows metafile
Category:	dropped
Size (bytes):	478
Entropy (8bit):	3.259187408297638
Encrypted:	false
SSDEEP:	12:MuU6p0HnM+vdd81lHEWWjsXFzBQ9/OKJ1lHfUTb5Uq6mt:5V0s+vddhAXFq9/8bKni
MD5:	7004D2BD5C3FE4E26B2550E5DCB0837E
SHA1:	B37F916D6F3C7B554D0ADF974C77C07F97AFEE7B
SHA-256:	6E76541EAD410B4DC4A790BEB7F150639206EE9677A5F14E8AA511249FA3DD09
SHA-512:	B92627328D6F4211B4F4238A82F88A4A682B5D545E0649ECF1CA2587752A229274305726FB911EFDAC487FB2002C194C9FCF55CECADE3C540F806198D697AA54
Malicious:	false
Reputation:	low
Preview:	.....@."Calibri.....-.....-.....-.....2.U..... .6.....-.....-.....%..... .....-.....-.....'.....2.Y.C..... .6.....'....."System....._n...Xs....._n.....-.....-.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRF{9B880850-96FA-42C0-A89A-62B76274DB3A}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.44230746225032513
Encrypted:	false
SSDEEP:	6:rl912N0xs+CFQXCB9Xh9Xh9XNIlqwAZ0R0/lS81:rl3lKFQCb77aAZ+sS0
MD5:	26E8ABEE9C8228E7765C051F1702DB74

SHA1:	03852E2952982F620A36BDC3BF673D4536CD999A
SHA-256:	0A4CB8B9D09B1D26BB2AB2EB4E794B2C25CFA58AC02AED98650505A44B755061
SHA-512:	B02E796275FA3DBB6EE83F4D3B35965712C1A9F8CD31D29CAD6C8867326F4CA607B1192B56539196CDDAAF9DBD8D2AADB2D4B456980FE05DE55236CC6D20234
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{C47AA337-7EB7-42EC-A441-6A672102AA66}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	3.521297672370757
Encrypted:	false
SSDEEP:	96:v4XC+Ojc75AGGz2CGGX/De4GGz9CGGXi/CnGGGGGz7ivGGGGGhGGz2n2GGdkGGzu:2Sj4590/yA06pi3naUn51M
MD5:	061D7817FD3BA6556BFE5874F1EB237C
SHA1:	CF93D6C7AF2DCD595B25C532C167F19E2D163901
SHA-256:	EB0B1BAADDE288D1562F94C267DCB6C58944BB3D7B1C8DDEDC7E0257BE06B8D6
SHA-512:	3E769EEE5B7F19CE8ACB7AB5479E0172EAB8EE21FEEFF797EBB3FFDA8832132787F2E808C033D3F9494D45B9D137501BC4CC373CC8E4AD639B2B9D5412EFF5EC
Malicious:	false
Reputation:	low
Preview:	V.y.k.o.u.k.a.l. .M.a.r.t.i.n.H.a.m.r.l.e. .L.u.k...a.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.o.f.f.i.c.e./.w.o.r.d./.2.0.0.3./.w.o.r.d.m.l.2.4.5.0.....).(.).(.).(.).(.).(.)...d.a.j.e. .p.l...t.c.e.:.....P.l...t.c.e.:...V.a.r.i.a.b.i.l.n... .s.y.m.b.o.l.:...O.b.d.o.b...:.....T.u.n.k.a. .J.i.Y... ...1.0.1.0.0.0.0.5.9.2...2.0.2.3./.R.1.....P.l.a.t.e.b.n... .p.o.d.m...n.k.y.:.....P.o.p.l. a.t.e.k.:...V.a.r.i.a.b.i.l.n... .s.y.m.b.o.l.:.....s.t.k.a. .p.Y.e.d.e.p.s.a.n...:.....V...`...h...j.....Z...\.....Z...x...z...|..... ...x.mxmxmeWN.....hF8..mH..nH..u....h.]...h....5..CJ..\..aJ.....h9...CJ..aJ.....h.O...h.9(.CJ..aJ.....h.9(.CJ..aJ.....hkK..CJ..aJ.....h.U*..h.9(.CJ..aJ.....h.O...h.O..5..CJ..\..aJ.. ...h^y.....h.P...h.P..CJ..aJ.....h.P...h^y..CJ..aJ.....hv....h.L..CJ..aJ.....h....CJ..aJ.....h^+..CJ..aJ.....j....U..mH..nH..sH..u.....h..H..hHx;.5..CJ..\..aJ....CJ..O

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{DC16EFFE-5C6A-4DAD-AD70-F1D7DEACD209}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\101POH0000000166.rtf.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Aug 16 20:38:45 2022, mtime=Wed Jan 25 17:07:46 2023, atime=Wed Jan 25 17:07:43 2023, length=62509, window=hide
Category:	dropped
Size (bytes):	1085
Entropy (8bit):	4.644677391614972
Encrypted:	false
SSDEEP:	12:8GV60Uh5uElPCH2CE5yWlSYEE0+WUbjiHEYjAo/uuKmPEkD9Qug5Qus4t2Y+xlBx:8x1yOmfAoWudDrg3s7aB6m
MD5:	52F01CB3D6103F276364B0A58B695580
SHA1:	1F65C76BB191FD1DCCAE05CE62663F6B669A3715

SHA-256:	6716BE49C42106427C5D2950BFCBB61701E2D989910007505ADCBB1460FF1855
SHA-512:	9562620CC5E568387F88B26615091F72D235461BD2390F5958C4BAD8B340D953C4B202F7F5212E73206AF4411FFD972CF39064F8A369104A55F304194DDB04E5
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....[a...0..dA...0..-.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..9V.....:.....q\..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....U...user.<.....Ny.9V.....S.....M&.h.a.r.d.z.....~.1.....U...Desktop.h.....Ny.9V.....Y.....>.....y.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....v.2.-...9V.. .101POH~1.RTF..Z.....U.9V.....R.....1.0.1.P.O.H.0.0.0.0.0.0.0.1.6.6...r.t.f.....Z.....-.....Y.....>.S.....C:\Users\user\Desktop\101POH0000000166.rtf..+.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.1.0.1.P.O.H.0.0.0.0.0.0.0.1.6.6...r.t.f.....:.,.LB.)...As...`.....X.....841618.....!a..%.H.VZAj.....-..!a..%.H.VZAj.....-.....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.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	98
Entropy (8bit):	4.458045745065579
Encrypted:	false
SSDEEP:	3:bDuMJlSVV6TtDpFomxWlMovfSVV6TtDpFov:bCohzNfDhzy
MD5:	367DBA4A1CA76B848CFED08CFF5F159E
SHA1:	B9B99123A315D775DF4B30001C701CAB4E115EFC
SHA-256:	47237A3D7CE212A3864500A5FBCFE3CD8B40C082828F4CFD61729CBAF41C5550
SHA-512:	0783435988B451052735D3661B8FF9EFBF8AC5C2B8941C22B7F6027FA99D97401609994D32F87F65277DE562A1D5967E4EF02CFC2D2976C8C9CE61BDCB253A52
Malicious:	false
Preview:	[folders]..Templates.LNK=0..101POH0000000166.rtf.LNK=0..[misc??????]..101POH0000000166.rtf.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.1999049754400093
Encrypted:	false
SSDEEP:	3:Rl/Zdp3bXIolyll8sMl3WC/JM86Xf:RtZrrXIolyIFMlm+M8C
MD5:	2701C6672DE94A2FE5F0828D09DABE5D
SHA1:	86A723401C79AC27A33EEEE5010C49B0C06F57A1
SHA-256:	8F6683C438476E6DC8BB66F4F3C7005DD9F30319FE8FEC56737067173EF0F305
SHA-512:	A9196FE2F84E7437408EE8D0148C0E1AC93DC8FD713D6CDBCD88BC15F281B790D233DED6EA94E7C34748465C8C7DDE58E2BE5EE123AF9859FC15B8D56B3AE E42
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....95*.....`.....-.....9A+...^li@.kiT.ki`.kiDBliZRli..9.,.....H...

C:\Users\user\Desktop\~$1POH0000000166.rtf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.1876236012137684
Encrypted:	false
SSDEEP:	3:Rl/Zdp3bX6elDlTsMl3WC/JM86Xf:RtZrrX6elGMlm+M8C
MD5:	0BB14C08C1D460B1D3D62C92312238D6
SHA1:	5724B78D9D2322017BC3EB6C14047799BD733C6A
SHA-256:	45F18D283F29146B3F70A6DB689572FE6EE304FD25E4F0115D8DCCE3D3719C42
SHA-512:	1B59A96506C13D4B1C8349862131CFAE86268439FB610A304980B8B85087EAA319F6D78D58B3A51B6D6C2F3687A40CC5182D7FBF1FAC4B61F1F9699873E313CE
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....95*.....w.0...&...-.....9A+...^li@.kiT.ki`.kiDBliZRli..9.,.....H...

Static File Info

General

File type:	Rich Text Format data, version 1, ANSI, code page 1250, default middle east language ID 1025
Entropy (8bit):	5.093553657575787
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	101POH0000000166.rtf
File size:	62509
MD5:	5241cc04162b7134f0e28d75286e8403
SHA1:	3a9e51c888314e69aa258492da237c1d4737f6b6
SHA256:	5dcd3d5273d069fe4825f22323aed5b7eaa8c745f5974e757c1919fbbcf6bcae
SHA512:	abc30c3ff84203c961cb3cb8a1ec054bbc6fe0c6a5f20d17fd2c271a9cf9673bd56334bdafc20c10b1d6a86744818a17746b1d6b8c2867b732f89ea57239caeb
SSDEEP:	768:vY3FFpreHEHtWr2FT+QA/qMMsKQcwnUUNBfOyYNLoJ0B:vYhSfrW+FM0lh0HB
TLSH:	D75397F800579359E36371A5AF1AF04D792BF52808F244E8B1EFC6FD50BB6A8D072625
File Content Preview:	{\rtf1\adeflang1025\ansi\ansicpg1250\uc1\adeff0\deff0\stshfdbch0\stshfloch31506\stshfhich31506\stshfbi31506\deflang1029\deflangfe1029\themelang1029\themelangfe0\themelangcs0{\fonttbl{\f0\fbidi \froman\fcharset238\fprq2{*\panose 02020603050405020304}Times

File Icon

Icon Hash:	74f4c4c6c1cac4d8

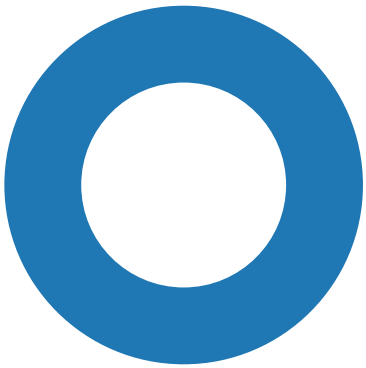
Static RTF Info

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 5888, Parent PID: 800

General

Target ID:	0
Start time:	10:07:43
Start date:	25/01/2023
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x1170000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	65438A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	65438A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	65438A84	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	65425805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	65425805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\256E1	success or wait	1	65425805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	65425805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	65425805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	success or wait	1	65425805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	success or wait	1	65425805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	65425805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	65425805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\256E1	256E1	binary	04 00 00 00 00 17 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 BF 83 A1 03 E8 30 D9 01 E1 56 02 00 E1 56 02 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	65425805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 FF FF FF FF 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	File Path	unicode	C:\Users\user\AppData\Local\Temp\imgs.htm	success or wait	1	65425805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2023-01-25T10:08	success or wait	1	65425805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	65425805	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000F01FEC\Usage	ProductFiles	dword	1446576144	1446576145	success or wait	1	65425805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000F01FEC\Usage	ProductFiles	dword	1446576145	1446576146	success or wait	1	65425805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	WordPerfect 5.x	success or wait	1	65425805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	success or wait	1	65425805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	65425805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	WordPerfect 5.x	WordPerfect 6.x - 7.0	success or wait	1	65425805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT632.CNV	success or wait	1	65425805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	doc	wpd doc	success or wait	1	65425805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\256E1	256E1	binary	04 00 00 00 00 17 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 BF 83 A1 03 E8 30 D9 01 E1 56 02 00 E1 56 02 00 00 00 00 00 DB 04 00 00	04 00 00 00 00 17 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	65425805	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 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 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 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 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 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 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 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 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 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 E1 56 02 00 E1 56 02 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 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 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 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 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 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 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 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 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 FF FF FF FF 00 00 00 00 00 00 00 00				

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

Analysis Process: splwow64.exe PID: **5060**, Parent PID: **5888**

General

Target ID:	12
Start time:	10:08:17
Start date:	25/01/2023
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff726e90000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly