ID: 1303436
Sample Name: yFwFFUG8b5.rtf
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:37:47
Date: 05/09/2023
Version: 38.0.0 Beryl

Table of Contents

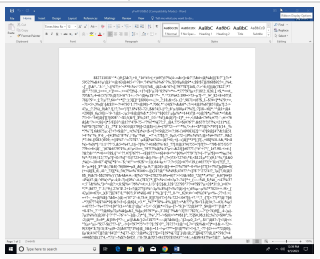
Windows Analysis Report

yFwFFUG8b5.rtf

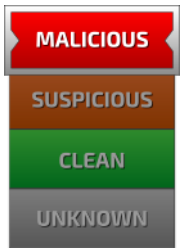
Overview

General Information

Sample Name:	yFwFFUG8b5.rtf
Original Sample Name:	59e7f344c86d2..
Analysis ID:	1303436
MD5:	cbf234faf143cd..
SHA1:	3a80997a9667...
SHA256:	59e7f344c86d2..
Infos:	



Detection

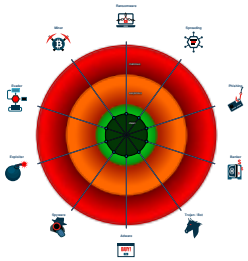


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Document embeds suspicious OLE2…
- Document contains embedded VBA…
- Yara signature match
- Document misses a certain OLE str…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 7452 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
yFwFFUG8b5.rtf	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x126e:$obj1: \objhtml • 0x12ab:$obj2: \objdata • 0x1293:$obj3: \objupdate

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

System Summary

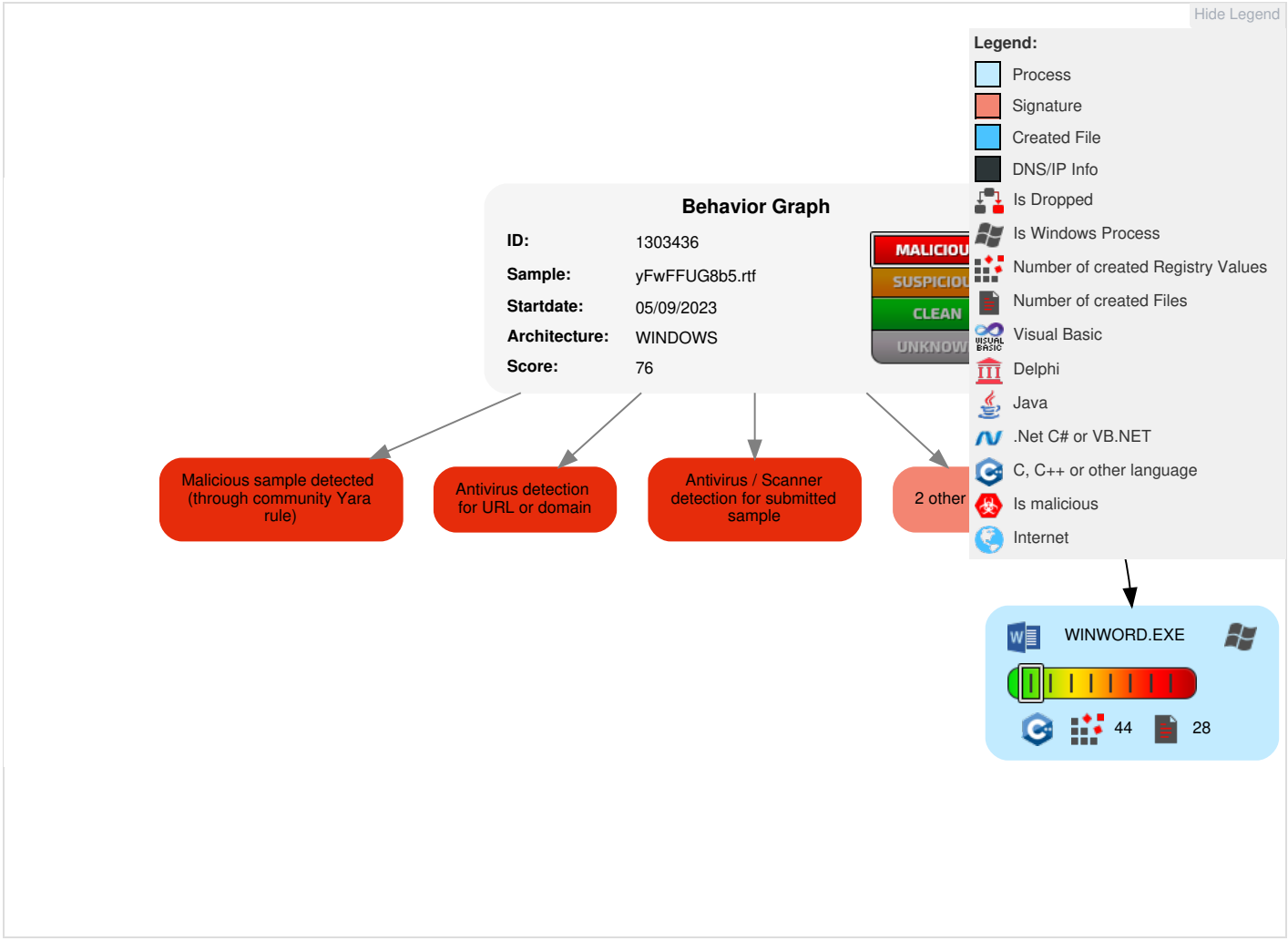
Malicious sample detected (through community Yara rule)

Document embeds suspicious OLE2 link

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	1 Scripting	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	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 Scripting	LSASS Memory	2 System Information 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

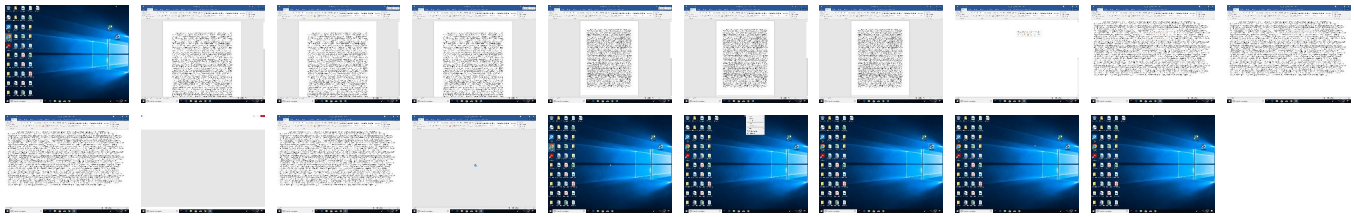
Behavior Graph

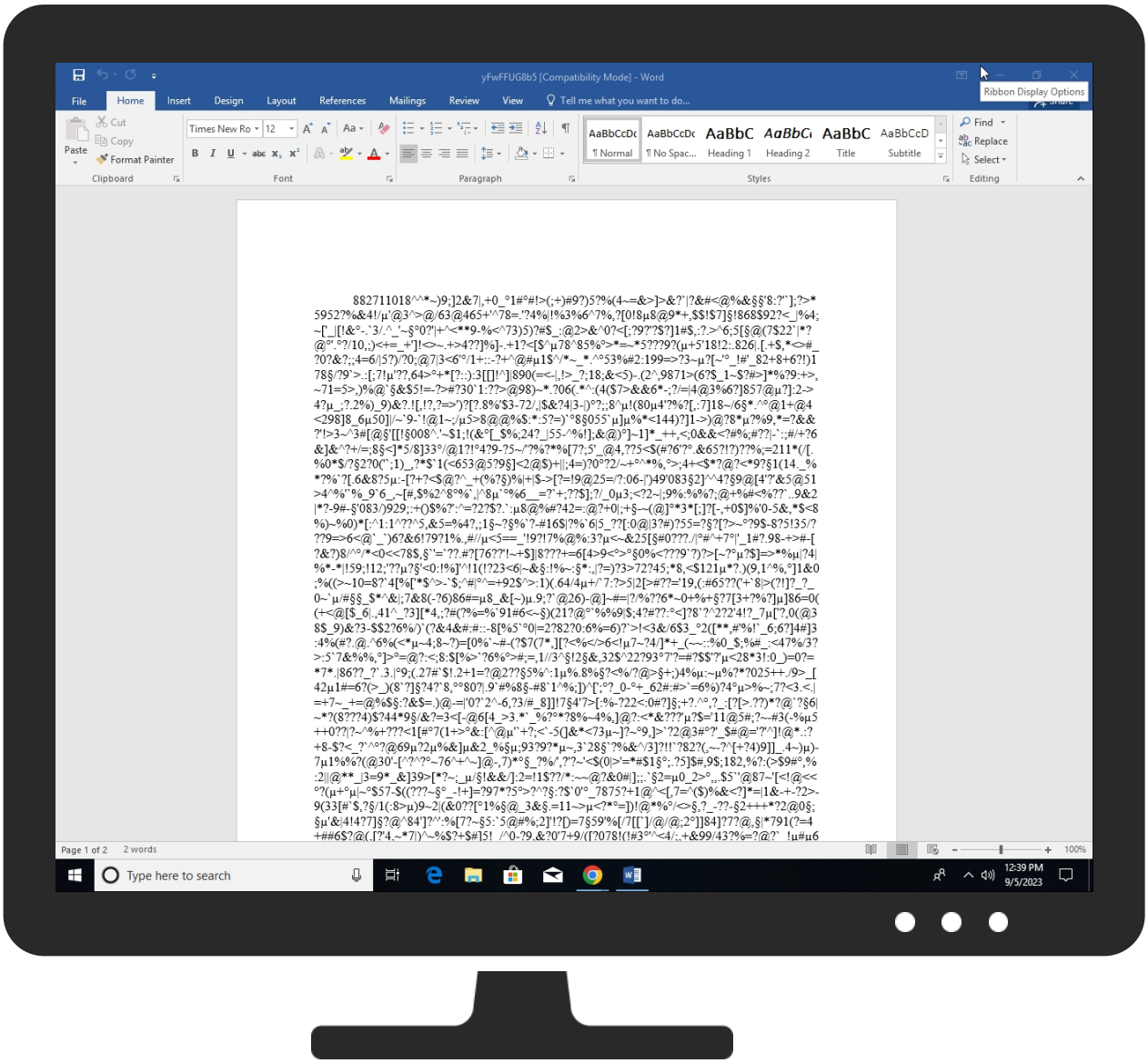


Screenshots

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
yFwFFUG8b5.rtf	39%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	
yFwFFUG8b5.rtf	100%	Avira	HEUR/Rtf.Malformed	

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	
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://api.scheduler.	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://login.windows.local	0%	URL Reputation	safe	
http://https://api.officescripts.microsoftusercontent.com/api	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	
http://wsvdyhrgebwhevawe.ydns.eu/fileone/Fnvtdhenapsfwu.exej	100%	Avira URL Cloud	phishing	

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	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://login.microsoftonline.com/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://shell.suite.office.com:1443	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://autodiscover-s.outlook.com/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://cdn.entity.	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://powerlift.acompli.net	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lookup.onenote.com/lookup/geolocation/v1	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://cortana.ai	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://api.aadrm.com/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://www.yammer.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://api.microsoftstream.com/api/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://cr.office.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://graph.ppe.windows.net	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://api.scheduler.	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://my.microsoftpersonalcontent.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://messaging.engagement.office.com/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://web.microsoftstream.com/video/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://dataservice.o365filtering.com/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://substrate.office.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://outlook.office365.com/autodiscover/autodiscover.json	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://consent.config.office.com/consentcheckin/v1.0/consents	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://d.docs.live.net	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://ncus.contentsync.	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://weather.service.msn.com/data.aspx	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://apis.live.net/v5.0/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://messaging.lifecycle.office.com/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://pushchannel.1drv.ms	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://management.azure.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://outlook.office365.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://wus2.contentsync.	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://make.powerautomate.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/api/addins/search	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://api.office.net	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://wsvdyhrgebwhevawe.ydns.eu/fileone/Fnvtdhenapsfwu.exej	~WRF{BC756FC3-E405-47FA-B8A9-6E6B44BDC6EF}.tmp.0.dr	true	• Avira URL Cloud: phishing	unknown
http://https://asgsmsproxyapi.azurewebsites.net/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://entitlement.diagnostics.office.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://outlook.office.com/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://login.windows.local	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://webshell.suite.office.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.microsoftonline.com	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://management.azure.com/	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false		high
http://https://api.officescripts.microsoftusercontent.com/api	32597437-DE6A-41FE-94A8-35F06685A9D8.0.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	38.0.0 Beryl
Analysis ID:	1303436
Start date and time:	2023-09-05 12:37:47 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
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
Sample file name:	yFwFFUG8b5.rtf
Original Sample Name:	59e7f344c86d2adef46011daccd3206e9fb87ad3edc3b88910daf4e5bc5c2401.rtf
Detection:	MAL
Classification:	mal76.winRTF@1/9@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, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.109.2.151, 20.126.111.161, 20.231.71.84
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, prod-w.nexus.live.com.akadns.net, config.officeapps.live.com, prod.configsvc1.live.com.akadns.net, us.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: yFwFFUG8b5.rtf

Simulations

Behavior and APIs

No simulations

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\32597437-DE6A-41FE-94A8-35F0 6685A9D8

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):	158646
Entropy (8bit):	5.348559102768841
Encrypted:	false
SSDEEP:	1536:e+C/FPgf3B7U9guw19Q9DQA+zQk5k4F77nXmvidlXRAE6Llj6k:ZDQ9DQA+zNXHD
MD5:	E4FC7AFF45B4EEE76F600FFE85F61270
SHA1:	77249587B1FE735A6E992CC3AB4D6C5EECDED081
SHA-256:	E00A2A9F444CA9EC28BEC72BC776BECADD1F8ED38E7A96D455AB52E1780FF90F
SHA-512:	3CF9C940038ECCD4AABC30B0E337A2F932B7BFB5BA678A9C5E23F8EE8A931063119D4419573948A98A9A973E9308CCF51C68A566076E2B3333974152C5E6D1A
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="2023-09-05T10:38:50">.. Build: 16.0.16827.30525-->.. <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.Word\~WRF{BC756FC3-E405-47FA-B8A9-6E6B44BDC6EF}.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):	1.1320092371798003
Encrypted:	false
SSDEEP:	24:raI8Utqoj73POWm9l7tfj9xBOjl5AzA03fazWKaBL/AkiF8:raZUtdPOWm9lRfj9xB85AzAE0yBLziF
MD5:	D4795CA46418A9530F320A7DA7B92281
SHA1:	AFF3A2D9DBF04A9BC696240A619860521F8AA7B7
SHA-256:	267C338D96813D1247723968CF080382E5631DF7316882D9F795E6A24E10CEED
SHA-512:	7E3AC67CE55AAC3F878C45B4FE4649A29FC60C01384191D20A156BAB2AA8185BE1B1E8D52C4269C8B190F2C9AC8C9841A92BA3F708B5F728D7D15103DFA3BE70
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{DC50A48E-EAAC-47AF-9927-355728D16EDF}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	10240
Entropy (8bit):	3.440344697982507
Encrypted:	false
SSDEEP:	192:JID2F0Q4qQowXlxvHbn5f9uqK/2Mo20nuonFO5ZvhlrBBzpZZ:JlDjHbHbnruqK/CjFO/jpZZ
MD5:	E48B2A8BF8B6AD374634D06D5995E82E
SHA1:	92A7EEDBCB7A414B6AE96DFB7F5444E291C465EE
SHA-256:	1167CC15A93FAC11D45496EB87D470A04DB44D7BD5C42D3E67E49D59AE4A1626
SHA-512:	E54AB65D1067914674CABAE1DE87129AD150D316546A78014F6D02BE8D34C8EC24C8F51163D50978EE7D914B00F6BE3A1560F096925F7A265FC1BFCF886F1A0
Malicious:	false
Reputation:	low
Preview:	....8.8.2.7.1.1.0.1.8.^.^.*.~.).9.;.].2.&.7.|.,.+.0._...1.#...#.!.>.(.;.+.).#.9.?.).5.?.%.(.4.~.=.&.>.].>.&.?.`.|.?.&.#.<.@.%.&.....'.8.:.?.'.`.].:.?.>.*.5.9.5.2.?.%.&.4.!./...'.@.3.^.>.@./.6.3.@.4.6.5.+.'.^.7.8.=...'.?.4.%.|.!.%.3.%.6.^.7.%.,.?.[.0.!.8...8.@.9.*.+.,.$.$.!.$.7.]....!.8.6.8.$.9.2.?.<._.|.%.4.:.~.[.'._.|.[.!.&...-...`.3./...^.__'.~.....0.?.'.|.+.^.<.*.*.9.-.%.<.^.7.3.).5.).?.#.$._.:.@.2.>.&.^.0.?.<.[.;.?.9.?.'.?.$.?.].1.#.$.,.:.?...>.^.6.;.5.[...@.(.7.$.2.2.`.|.*.?.@...'.....?./.1.0.,.;.).<.+.=._.+.'.].!.<.>.~...+.>.4.?.?.].%.].-...+.1.?.<.[.$.^...7.8.^.8.5.%...>.*.=.~.*.5.?.?.?.9.?.(...+.5.'.1.8.!.2.:...8.2.6.|...[...+.$.,.*.<.>.#._.?.0.?.&.?.;.;.4.=.6./.|.5.?.)./.?.0.;.@.7.|.3.<.6.'.../.1.+.:.:.-.?.+.^.@.#...1.$.^./.*.~._.*...^...5.3.%.#.2.:.1.9.9.=.>.?.3.~...?.[.~.'..._.!.#.'._.8.2.+.8.+.6.?.!.).1.7.8.../.?.9.`.>....:.[.;.7.!...'.?.?.,.6.4.>...+.*.[.?.:.::).:.3.[.[.].!.^.].|.8.9.0.(.=.<.-.|.,.!.>._.?.;.1.8.:.&.<.5.).-...(.2.^.,.9.8.7.1.>.(.6.?.$._.1.~.$.?.#.>.].*.%.?.9.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{F99806D6-F16F-4DA6-B3B6-FC251D46CB10}.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\index.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	78
Entropy (8bit):	4.820300539697694
Encrypted:	false
SSDEEP:	3:bDuMJlEsjdHQpulmxWIMovhPdHQpulv:bCERMuGPMu1
MD5:	544DEAA7709184F853BBB323A0EEC8B1
SHA1:	0C5E68C83F138FAA781AD8A2DB73AFCB49759835
SHA-256:	6B77993FCAAE20F46AE1305C8727E72D631538AE56FA24C8C9341E8E2AE9FB88
SHA-512:	0DCB4625CE2F6F3B9107F65382E95C31FE377E15A83A7254AD5B9429575C5E4E4B64484210874159140927 9F8654F5A23D52A2E8E8981DF0880563B9C92B7E31
Malicious:	false
Preview:	[folders]..Templates.LNK=0..yFwFFUG8b5.LNK=0..[misc??????]..yFwFFUG8b5.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\yFwFFUG8b5.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=Fri Aug 11 16:56:03 2023, mtime=Tue Sep 5 09:38:50 2023, atime=Tue Sep 5 09:38:46 2023, length=104980, window=hide
Category:	dropped
Size (bytes):	1060
Entropy (8bit):	4.720394737279126
Encrypted:	false
SSDEEP:	12:8VBpUdS6CHiX30xGX5D3R+W+1E9lqlgQRijEjAJ/y5jU4XRQDyX2i2A4t2Y+xIBx:883XV3FleFgUAJK5yDymPY7aB6m
MD5:	02905FA5F660730F36EE11D77437EE4C
SHA1:	8A9C26384BA692E0DD034ACC435645EDD4B5668C
SHA-256:	387899754F74140AD7ECF8376A996483AF7707EC1F1A459B518E3C0247801C6E
SHA-512:	294FE4DC8B00FC612E5050DC7547614A9565125EB7C3B7EDFBD1AACECA607F4B2B483573C2DBF4FD1175D2FB9C64F49404F582201C6A07E986066B00E5026AE
Malicious:	false
Preview:	L.....F.... ...Mcq.}...@.E(....n.P&.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L..%W.T.....:.....B..U.s.e.r.s...@.s.h.e.l.l .3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....W....user..>.....NM.%W.T.....S.....%.a.l.f.o.n.s.....~.1.....W....Desktop.h.....NM.%W.T.....Y.....>.....L.D.e.s.k.t.o.p...@.s.h .e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....j.2.....%W.T .YFWFFU~1.RTF..N.....W..%W.T.....y.F.w.F.F.U.G.8.b.5...r.t.f.....U.....-.....T.....>.S.....C:\Users\us er\Desktop\yFwFFUG8b5.rtf..%.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.y.F.w.F.F.U.G.8.b.5...r.t.f.....:..,.LB.)...Aw...`.....X.....124406.....!a..%.H.VZAj.....k.p8.....W ...!a..%.H.VZAj.....k.p8.....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...1

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):	2.35404893645518
Encrypted:	false
SSDEEP:	3:Rl/Zd4XXlbIOJOAk25llXXzpllJ:RtZm5AkgT
MD5:	82BAEF59A36E299C7D0FEAD72F2F9975
SHA1:	03C8E387DC64A59C94B2D9C329810DF4F09CABBE
SHA-256:	4971F01225E22C0FE0EE95A71689A9091A4BD1A44E4E46C5995D1469C71E4154
SHA-512:	7CD03BAE472E4A57C9C0D03E786720E77B5B280D231260845CAB8890C17B55F0B09F429190D6871B250FA9327BEADBB14314740C2C5CD62FC032C0213293D6B
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....H0.....2.....HA.....k.o`.....H.....T...

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	20
Entropy (8bit):	2.8954618442383215
Encrypted:	false
SSDEEP:	3:QVNliGn:Q9rn
MD5:	C4F79900719F08A6F11287E3C7991493
SHA1:	754325A769BE6ECCC664002CD8F6BDB0D0B8CA4D
SHA-256:	625CA96CCA65A363CC76429804FF47520B103D2044BA559B11EB02AB7B4D79A8
SHA-512:	0F3C498BC7680B4C9167F790CC0BE6C889354AF703ABF0547F87B78FEB0BAA9F5220691DF511192B36AD9F3F69E547E6D382833E6BC25CDB4CD2191920970C5
Malicious:	false

Preview:	..p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$wFFUG8b5.rtf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.358708735851251
Encrypted:	false
SSDEEP:	3:Rl/Zd4XXlblOJOAkszlNzpllIJ:RtZm5AkAT
MD5:	BE67E3F67222F2A441610F3051FA6BE1
SHA1:	6340B051E352E50EA25E8F8308A7742669DE99BD
SHA-256:	A87DE3F02D9DED3DEBD873DD92809D944C9794B32AE252877205279D858E291F
SHA-512:	543E89002ECFC70D7646A022B88C8DBBC67021219370601C97FCE7778354C07F6BE360AD1AE421BF4E7F7BE561CDAB7DB8DEDEB258F317487FE7559A4BE0B9EB
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....H0.....2.....HA.....k.o`.....H.....T...

Static File Info

General

File type:	Rich Text Format data, version 1
Entropy (8bit):	2.5430425756510457
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	yFwFFUG8b5.rtf
File size:	104'980 bytes
MD5:	cbf234faf143cd9fdc9702a6a976153c
SHA1:	3a80997a96677a0bacd43a14a776a5a3dd716cae
SHA256:	59e7f344c86d2adef46011daccd3206e9fb87ad3edc3b88910daf4e5bc5c2401
SHA512:	62edf48c3b9937284495b223eed254c981585714fb53f6409ca944b9266f44e00473c449b4efc0675f823100fef946a38895112c2ae9cef91200a3b57cdd3e3e
SSDEEP:	384:ojGD480k5SMgBeIPu92lqYz/ibe0sdOq0A/0mmmH:Pt04gBeIGEs/ibe0GO286
TLSH:	65A3336D938B4460CFA463BB831BAE0895FC776EB3589176B89C133037E9D79462603C
File Content Preview:	{\rtf1.....{*\lineColor816588099 |}.{\1882711018^^*~)9;]2&7|,+0_.1#.#!>(;+)#9?)5?%(4~=&>]>&?`|?&#<@%&..'8:?``];?>*5952?%&4!/.'@3^>@/63@465+'^78=.'?4%|!%3%6^7%,?[0!8.8@9*+,$$!$7].!868$92?<_\|%4;~['_\|[!&.-.`3/.^_'~..0?'\|+^<**9-%<^73)5)?#$_:@2>&^0?<[;?9?'?$

File Icon

Icon Hash:	39f5a98c818aacb3

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000012B5h								no

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 7452, Parent PID: 804

General

Target ID:	0
Start time:	12:38:47
Start date:	05/09/2023
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:	0xfa0000
File size:	1'937'688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	false

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$wFFUG8b5.rtf	success or wait	1	651A5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	651A5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	651A5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	651A5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2BC81	success or wait	1	651A5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	651A5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	651A5805	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	651A5805	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	651A5805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	651A5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2BC81	2BC81	binary	04 00 00 00 1C 1D 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 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 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 68 EE 2C 39 E5 DF D9 01 81 BC 02 00 81 BC 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	651A5805	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 FF FF FF FF 00 00 00 00 00 00 00 00				
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	651A5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2023-09-05T12:39	success or wait	1	651A5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	651A5805	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\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1462042637	1462042638	success or wait	1	651A5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1462042638	1462042639	success or wait	1	651A5805	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	651A5805	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	651A5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	651A5805	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
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	651A5805	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	651A5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	doc	wpd doc	success or wait	1	651A5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2BC81	2BC81	binary	04 00 00 00 1C 1D 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 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 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 68 EE 2C 39 E5 DF D9 01 81 BC 02 00 81 BC 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 00 00 00 00 00 00	04 00 00 00 1C 1D 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 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 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 81 BC 02 00 81 BC 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 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	success or wait	1	651A5805	unknown

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				

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 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 FF FF FF FF 00 00 00 00 00 00 00 00				

Disassembly

No disassembly