ID: 682773
Sample Name: [name removed]
file 08.11.2022.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 00:24:59
Date: 12/08/2022
Version: 35.0.0 Citrine

Table of Contents

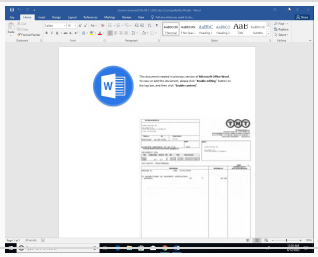
Windows Analysis Report

[name removed] file 08.11.2022.doc

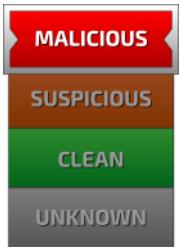
Overview

General Information

Sample Name:	[name removed] file 08.11.2022.doc
Analysis ID:	682773
MD5:	4f487d329bcf514..
SHA1:	52d9885233394a.
SHA256:	d66a64e64a1d1b.
Tags:	Bokbot, doc, IcedID, macros, MonsterLibra, Shathak, TA551
Infos:	



Detection

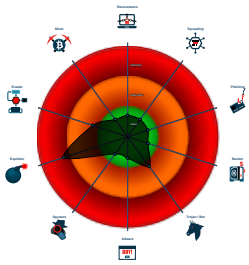


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince v…
- Multi AV Scanner detection for subm…
- Document contains an embedded V…
- Document exploit detected (UrlDown…
- Machine Learning detection for sam…
- Potential document exploit detected…
- Tries to connect to HTTP servers, b…
- Document contains an embedded V…
- Document contains embedded VBA…
- IP address seen in connection with …
- Document misses a certain OLE str…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 5636 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **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

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Software Vulnerabilities

Document exploit detected (UrlDownloadToFile)

System Summary

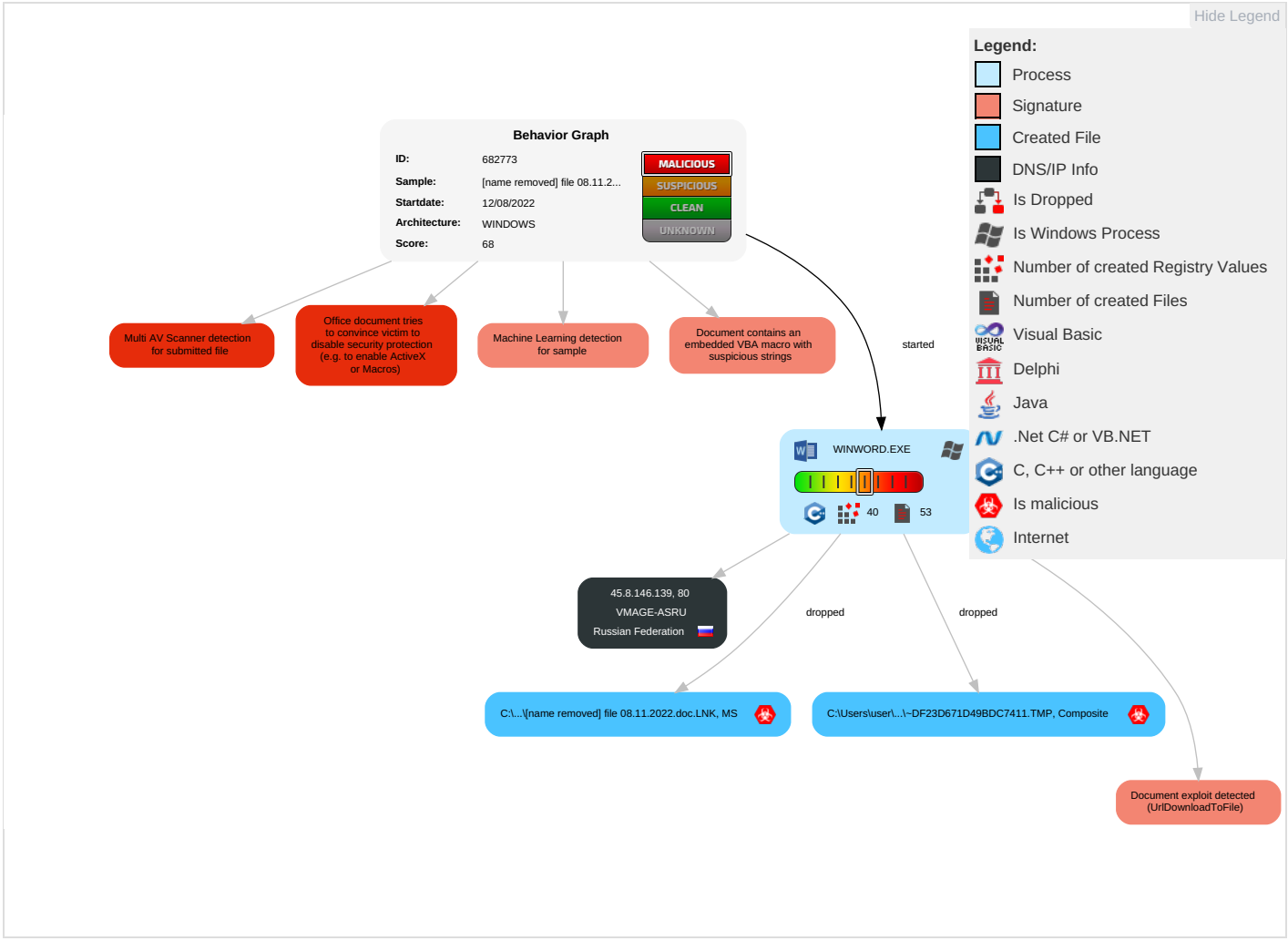
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains an embedded VBA macro with suspicious strings

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 2 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	1 1 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 2 Scripting	Security Account Manager	Query Registry	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

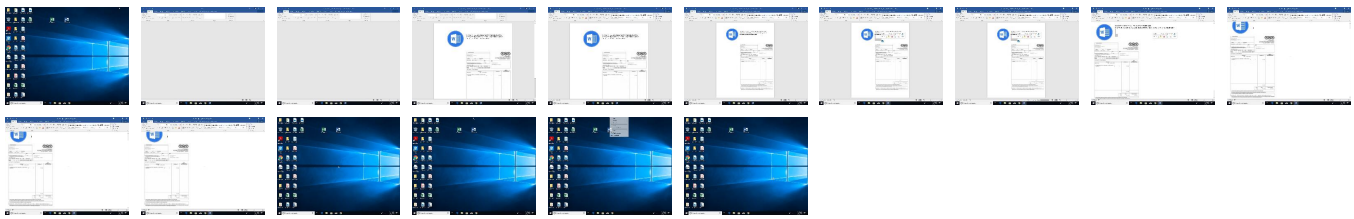
Behavior Graph

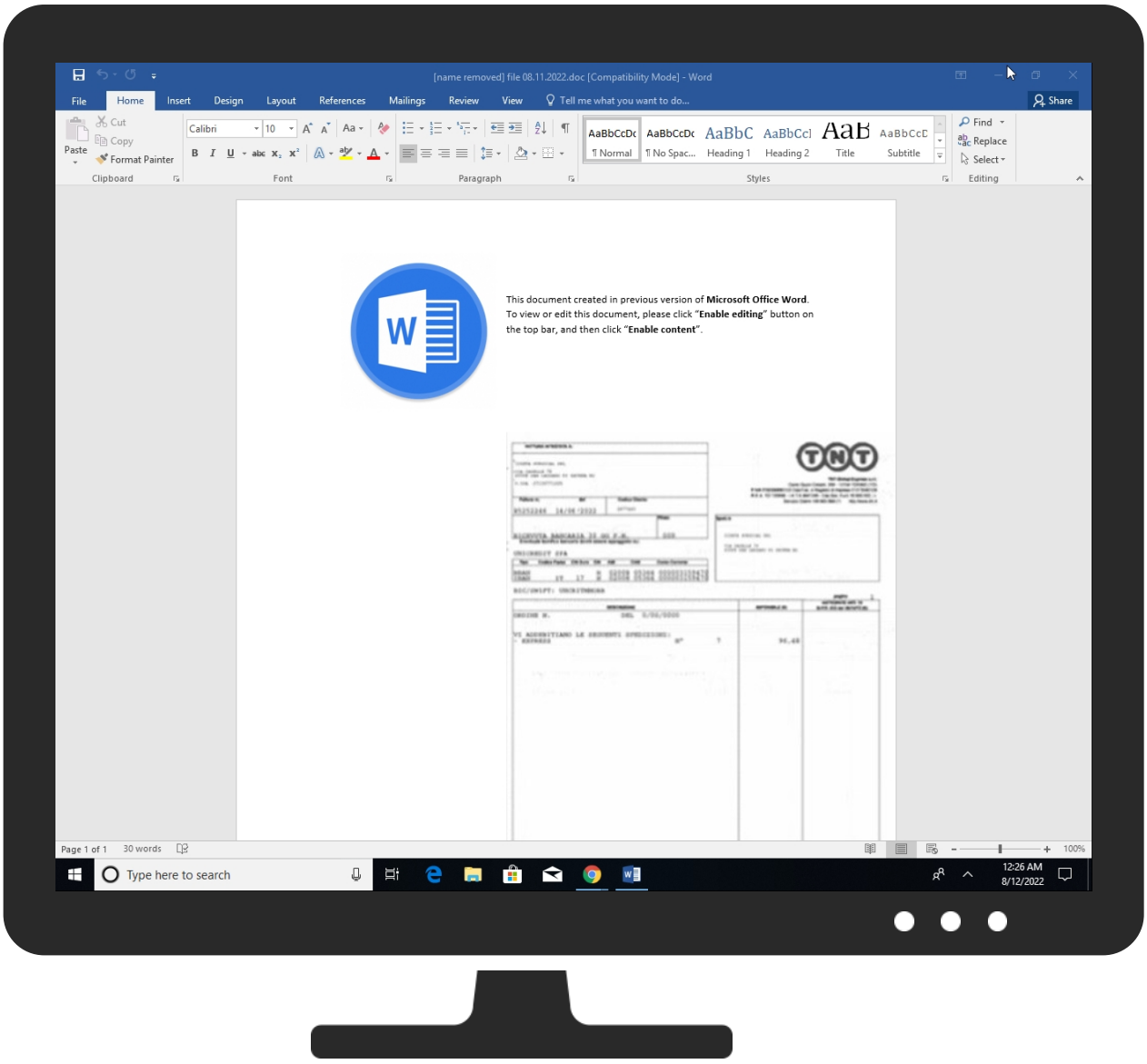


Screenshots

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
[name removed] file 08.11.2022.doc	27%	Virustotal		Browse
[name removed] file 08.11.2022.doc	20%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
[name removed] file 08.11.2022.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF23D671D49BDC7411.TMP	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
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://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	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://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://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://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

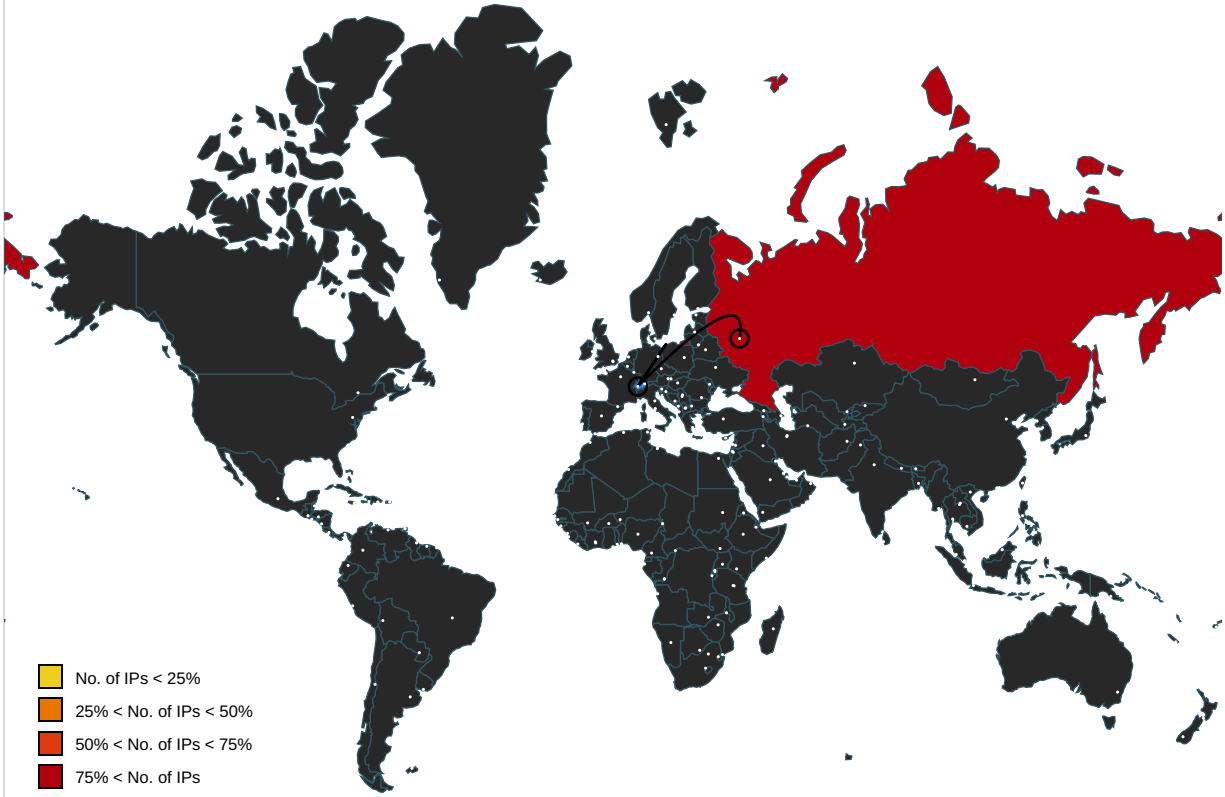
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://login.microsoftonline.com/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://shell.suite.office.com:1443	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://autodiscover-s.outlook.com/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://roaming.edog.	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://cdn.entity.	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://powerlift.acompli.net	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://cortana.ai	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://api.aadrm.com/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://api.microsoftstream.com/api/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://cr.office.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://graph.ppe.windows.net	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://my.microsoftpersonalcontent.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://messaging.engagement.office.com/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://web.microsoftstream.com/video/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://dataservice.o365filtering.com/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://ncus.contentsync.	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://weather.service.msn.com/data.aspx	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://apis.live.net/v5.0/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://messaging.lifecycle.office.com/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://management.azure.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://outlook.office365.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://wus2.contentsync.	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://api.office.net	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://entitlement.diagnostics.office.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://outlook.office.com/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://outlook.office365.com/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://webshell.suite.office.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://management.azure.com/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://devnull.onenote.com	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messaging.action.office.com/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://ncus.pagecontentsync.	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://messaging.office.com/	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	DF273B98-9C51-4F12-BC5B-F382F2EC592E.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.8.146.139	unknown	Russian Federation		44676	VMAGE-ASRU	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682773
Start date and time:	2022-08-12 00:24:59 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	[name removed] file 08.11.2022.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.expl.winDOC@1/11@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Adjust boot time • Enable AMSI • 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, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.88.191, 52.109.76.35
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information

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\DF273B98-9C51-4F12-BC5B-F382F2EC592E

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	148061
Entropy (8bit):	5.358149896701831
Encrypted:	false
SSDEEP:	1536:icQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:d1Q9DQe+zuXYr
MD5:	DDE67BDFA5CC860258898381F8D47561
SHA1:	0EE7608FFBC9D1CF2F9CC68A18ABD9A79F60203E
SHA-256:	5A86A94E467321B63B2C72476067DB8FB70B1B8057E8B7004555E30DDA7CC31E
SHA-512:	7FE35CD1788843BE52A9461DCEF40AEDD4F665886E6AB5524344BFDE0400BAAF2B980C141DBB3B8EB069463DC166E70DC4E5A99BE016621A7D7E6B6F074E6867
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="2022-08-11T22:25:58">.. Build: 16.0.15607.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\515DF229.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 440 x 440, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	256215
Entropy (8bit):	7.978353630345434
Encrypted:	false
SSDEEP:	6144:eAJt7vvFhw7UBHzZiKVixZs+63Jby+hvEaAWirPosx4gR:eAzDfhH1nVWh63J9mbxnR
MD5:	C46CBD511D9669284EA364D93575B594
SHA1:	3754D9E8FE6F6D2B9946215D7EAB1F27AFCF55DE
SHA-256:	C79BCF4CCCFCAC32F26C892F6196BE3D299CEAA4DC157E633F73E470534B9F90
SHA-512:	2D3FE353D3D3DBBF5671DD780E4B2ADD4E62F32291091CDBD3757DE3F2665A69A99CDD6987368DE1271A14BA3432B853D4A1B55226B07CABDB06AF31D4A307A3
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!...!.....IDATx^....fGU..3.W...}.....*$.a..1... .)aT.(*...h.....tw..!.!. F....p..Q&....s.O.I..>.....Ju..4..'.U..U..VU. s...9.-.~.!..+.R.8..2.S..2=..U..j[.g>..<....@....l..q.W....m..h.UO..+....,.q.c.....+.....r-f.....=z..J.t...f]....n....'*..{.c.:@/.PQ.....A....6.C.I=..R.mo.W9.....OT.,....c1h.-5M..VT...2.q.. .to\Lk.k.E..6]c.....lE-..g.....*..z..Zz...e@/.qMg.R..'..m\..UZ..]..P.1Z.[..T...^..k.._..'.h.W...=...*2..U.m.6].5n...|.Y..=.7.WT..zeg.....h.|.r..he.B".m\Qy=>H^....=z..0....5..>.....J.t..-.t$2.:2O..@.'z40K...5..r.o.....k....ek.him...I....2...*..'...Z.^>C..+...%P.X..o....K.1 .a.=.^.3.....3.Bo<.m[..6.Z~.h..+.....w...>..+.[$o.L..9>I.U...,.6.P.y_.I-...^N4Hz.e....+-.he..-Z... .....|.L.....Iz.z.4.. ...g\...Lb.|E.S....ZT~O6i..'.\..|K.q".9.....V...gHTZ..h.J.hice.W..^?k.D...2...h.=.I_.....*V..W.6]...'.I.\.....mj..D+.....^.0&.i.^uW~...k.....%.J...2.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7B8918C8.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 380 x 526, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	79862
Entropy (8bit):	7.9850226558494
Encrypted:	false
SSDEEP:	1536:3oqyPqib6IbiXmcfDBFdEU8yslk2ZGBlGUCk4+:3yqtImXmcbBFopLwlGDkH
MD5:	F673388F14A0B0E6160D7E31FB8B27A7
SHA1:	792480CA5B43D57E2A0A65466D77A294DA9D55C3
SHA-256:	0D79507FBC5D3C1843F0584E92FFD8B8F2862B4AE569BEB934963B30185E6489
SHA-512:	957C95FE8ED7DC213F027C59952F3F2AB5DFE6ED91944880D230AFC7B2B9EFFD812000FBF26CD6948DD3C478CB9B049C97405F6EBD4A86E3D10241DA3A0B692A
Malicious:	false
Reputation:	moderate, very likely benign file

Preview:	.PNG.....IHDR...|.....4.!... .IDATx...{#...9g...p...l.+....^x..[..'.....9...g.K.t7.0#...Ca....S..[o.:.N:.v.'.....r...W...q.....!.....q.CF.g..._.c.y.....,.;9....6.._z...,./.....nt.../..g.t..._....._./.-.....F.....+mt.X.../...+...0:....../.^.{...b.}.`0.X,....V..|.8N0.$..\...@0....l.ZqB.+?_...fR}....%.\.....Y,.\|A..r..Z..B~8..t.P.~.Cc[p.D.W.INn...f....5....c.If.V....Oh$Y...|....GI.....q... .....u..../..b.`.0.L.@ 0.L..@(.....Ac..Rd...o.....6~x..v..t._...Ph6.E"..... .T.._,..p..e.1.o.....qf.uk/.km/w.Z..<...9.'.|>..B.PH.....K.J.8...$.;.\|>g...A..3\..'._e....pX6x..(..m....Kc6...a.By;.P..R..M.u..p2.\|....7..0V.kO..n...v#..\|>.....pm.....B..$..-..h4:.N#..r..D"|n<...ak..`0.k.g....d@q..Cf<wk..oW.....5.....V.U.+$.*...?.2..r..6...}:=.e.j.l.)/....*....Y..t:.L.....vG.H...t.j....:..`0..FL.H$....d.P(..DB...j%.....g.Y..<??o.Z...t.....l.P(.r.X,&k..._.Fm>..Z....^.7...)...8.X.X,...t:..Dd-.{%.....y.8.x<...h6..H$.H.\..`;[..O....(.....B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{AB7DD05B-CB79-4DB6-ACB7-3D8144095A6D}.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\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{D24A98BC-5D49-42B4-8DB0-23D79BB38FC4}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.1334198335541092
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82l2kwkvOqnlAenltnlHllQnlwZZx/vlk:4LG1ND9Pxn820kT37uH
MD5:	960AF49AF35F5728FF363D731F3C56D6
SHA1:	BB885B3B081EC820C8DD0D5DFE7185922742BF3D
SHA-256:	B895D345BF6216675EFC3C62F59AD7274EE3C82498AE3894795BE317C646DA58
SHA-512:	73A21B290304FA38710D4E1B7052D3BED76DF76A14E6B654D5949B28E949417A86F820A64CFCEB7F8B630C96740FC322890AAB2822395EA309AA9A38B29A81C8
Malicious:	false
Reputation:	low
Preview:	../../...T.h.i.s. .d.o.c.u.m.e.n.t. .c.r.e.a.t.e.d. .i.n. .p.r.e.v.i.o.u.s. .v.e.r.s.i.o.n. .o.f. .M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .W.o.r.d.....T.o. .v.i.e.w. .o.r. .e.d.i.t. .t.h.i.s. .d.o.c.u.m.e.n.t.,. .p.l.e.a.s.e. .c.l.i.c.k. .. E.n.a.b.l.e. .e.d.i.t.i.n.g.. .b.u.t.t.o.n. .o.n. .t.h.e. .t.o.p. .b.a.r.,. .a.n.d. .t.h.e.n. .c.l.i.c.k. .. E.n.a.b.l.e. .c.o.n.t.e.n.t. ....z..... ....

C:\Users\user\AppData\Local\Temp\~DF23D671D49BDC7411.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):	51200
Entropy (8bit):	4.456057133152078
Encrypted:	false
SSDEEP:	768:ZvFAIt3/zpsfHPCOVkZ35GE28fUmtq5rOtKZ:1F13/zpsvPVkHGn5y
MD5:	DEA93C9085C03BC699E591BC9662178B
SHA1:	168DBFF17F04CA13E5DEB769718A64F1CBB748D6
SHA-256:	3A1F13C329E3EAFDD96FFE33F91DE2DBF4C7754963C09AFE78A0FEDB0D0048BA
SHA-512:	28DBE35EE65F499F5E9E568A5A7D736C83AC52FE6FF6E1273583C686865CA541F734E81FEC246731B9E23DF11B10CC9870705654325F1FD00F1E330C0BA46A8F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

Preview:	.....>..... .....G.....&... .....!..."..#...$...%.....'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8.....:...;...<...=...>.....@...A... B...C...D...E...F...9...^...I...J...K...O...M...N.....P...Q...Z...S...T...U...V...W...X...Y...L...[...\...]..._.....`...a...b.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\[name removed] file 08.11.2022.doc.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 Mar 8 15:31:41 2022, mtime=Fri Aug 12 06:26:00 2022, atime=Fri Aug 12 06:25:55 2022, length=2221308, window=hide
Category:	dropped
Size (bytes):	1155
Entropy (8bit):	4.721233857156778
Encrypted:	false
SSDEEP:	12:8uNX0k/E0UuuElPCH2JL9Y05X+WchKfQgxjAy/Ip9LDe3DPD594t2Y+xIBjKZm:8uRbLUcfTFAyo9W3Drd7aB6m
MD5:	BB5746020CD194A6240EB2FD830E7869
SHA1:	D1AAA9E017D887440AA7C1B471B3C1A1E96BFBB3
SHA-256:	CE6D1812CAA6E088678D1C3FF83D5284F8CAFA867AFC326BDCB84AB8A6D948A6
SHA-512:	03785B9091413EDD4B5B22C1F36E3618990F8D05B60687B70B069793763E9C5B255D0C6FD1D0C8F0EFED42F7D45901E777D14ABB7D4C9528795F90A0671B32AE
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ...y....3..7._.....!.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...U6;.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....P.1.....hT....user.<.....Ny..U6;.....S.....c9.h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..U6;.....Y.....>.....f.@.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....2...!..U<; ._NAMER~1.DOC..v.....hT...U<;....h.....f.[.n.a.m.e. .r.e.m.o.v.e.d.]. .f.i.l.e. .0.8...1.1...2.0.2.2...d.o.c.....h.....-.....g.....>.S .....C:\Users\user\Desktop\[name removed] file 08.11.2022.doc..9.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.[.n.a.m.e. .r.e.m.o.v.e.d.]. .f.i.l.e. .0.8...1.1...2.0.2.2...d.o.c.....:..,.LB.)... As...`.....X.....216041.....!a..%.H.VZAj.....-..!a..%.H.VZAj.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.

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):	119
Entropy (8bit):	4.683543152128782
Encrypted:	false
SSDEEP:	3:bDuMJlmZMY9TLBCmX10EIDMY9TLBCv:bC/p9HB6tp9HBs
MD5:	6B8D275C117744818A489CC600AFCDBA
SHA1:	7DEDC3D62242EFFD8D3FF966E38DBA73139BEC08
SHA-256:	C7045A392BBA803ABB7AFC176E0E157422B8112BDAFD2A916A798BD69F123FB1
SHA-512:	D4A20369BC2CDDF78C296113420F5BEDB88B904311A0978B7E1138F964588CBCD814F5DDDEFE4D2409D11ED30DD028658156E270089680B3784D42FBB6BF81F
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..[name removed] file 08.11.2022.doc.LNK=0..[doc]..[name removed] file 08.11.2022.doc.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):	1.98277332707181
Encrypted:	false
SSDEEP:	3:Rl/Zd/PpX/tHPA7v7PbFlt/Xtln:RtZ9hXt47TjftP
MD5:	086BAEDFC7E8E7C15516F206F258374C
SHA1:	B079E2AE29E62D0EB7B14FF6A209D859276232AB
SHA-256:	779145B8EEB92B7F3937BFE9A2F61BF4BB0C970F6FBD8A4D9D1EC0D4B370CFE5
SHA-512:	B14EE5EAB294ACE9780C58C9C717BDF6451EE3FD029600417F5614A69A7FB43985D7EDAA07466A190262D64F7BDB02B1CF274A3C9F5B79904FE9C5E0409696A 1
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....Kj..8.....Oj..9.....j..:.....

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators

Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$ame removed] file 08.11.2022.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	1.98277332707181
Encrypted:	false
SSDEEP:	3:Rl/Zd/PpX/tHPA7v7PbFlt/Xtln:RtZ9hXt47TjftP
MD5:	086BAEDFC7E8E7C15516F206F258374C
SHA1:	B079E2AE29E62D0EB7B14FF6A209D859276232AB
SHA-256:	779145B8EEB92B7F3937BFE9A2F61BF4BB0C970F6FBD8A4D9D1EC0D4B370CFE5
SHA-512:	B14EE5EAB294ACE9780C58C9C717BDF6451EE3FD029600417F5614A69A7FB43985D7EDAA07466A190262D64F7BDB02B1CF274A3C9F5B79904FE9C5E0409696A1
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....Kj..8.....Oj..9.....j..:.....

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993668516736907
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	[name removed] file 08.11.2022.doc
File size:	2316250
MD5:	4f487d329bcf514575a0c8e5a4dcb53f
SHA1:	52d9885233394acffdda1ea3a40989a8b47e9e34
SHA256:	d66a64e64a1d1b44ebcc854f04b1e175ccc93b61fff0f093394f6dcdcd785d82
SHA512:	2fbe8609658dc2caa3a9e74227b69e1fd52fb86482794881d4f61cb635536f961f78b93cf73d4d387c8717e10d1232aa6ceac68c0d7a7f8de190743ebf832b1e
SSDEEP:	49152:TnxBpMvUTIyOgNz8bc10IsulzqMy44elEAU33SapcOnaT54Z1+bBOz:TxBpMavFNzUculsul+d44e1y3VlV4rY2
TLSH:	36B533B0C86EBA19CA01AD3389D3546E35ABD427FB3D5C478053890B76DB558FEE2881
File Content Preview:	PK.....!..U~....._rels/.rels...J.@.....4.E..D.....$....T..w-..j.....|.zs..z..z.*X.%(v.....6O.{PI.....`S__._x .C..CR....:....t..R.....hI.3..H.Q..*.;..=..y... n.....yo.....[vrf..A..6..3[.>_...-K....\NH!....<..r...E.B..P...<_.

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/682773/sample/[name removed] file 08.11.2022.doc"	
Indicators	
Has Summary Info:	
Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

Streams with VBA	
VBA File Name: ThisDocument.cls, Stream Size: 2846	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2846
Data ASCII:	. n . A t t r i b u t . e V B _ N a m . e = " T h i . s D o c u m e n . t " . . . B a s . . 1 N o r m a l . . . V G l o b a l ! . S p a c . l F a . l s e . J C r e a . t a b l . . P r e d e c l a . . I d . . # T r u . " E x p . o s e . . T e m p . l a t e D e r i . v . $ C u s t o m l i z C . P . . . . . D . ? P t r S a . f e F u n c t . i o n . . L i b . " u s e r 3 2 " . A l i a s " . K i l l T i m e . r " (B y V a x l . . . . . A s L o n g , , ... / . . .
Data Raw:	01 6e b4 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 44 6f 63 75 6d 65 6e 10 74 22 0d 0a 0a 8c 42 61 73 01 02 8c 31 4e 6f 72 6d 61 6c 02 2e 19 56 47 6c 6f 62 61 6c 21 01 aa 53 70 61 63 01 6c 46 61 08 6c 73 65 0c 4a 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72 75 0d 22 45 78 70 08 6f 73 65 14 1c 54

VBA Code

Streams	
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 369	
General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	369
Entropy:	5.262779644813546
Base64 Encoded:	True
Data ASCII:	I D = " { B 3 5 A B 5 D 0 - 1 5 B 8 - 4 F 3 3 - 8 D A 0 - 8 E D B C A 2 B 4 B 0 A } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 8 5 8 7 9 4 1 D 9 C A 6 A 0 A 6 A 0 A 6 A 0 A 6 A 0 " . . D P B = " 0 A 0 8 1 B 9 C A 1 9 D A 1 9 D A 1 " . . G C = " 8 F 8 D 9 E 1 B A 6 2 5 2 A 2 6 2 A 2 6 D 5 " . . . . [H o s t E x t e n d e r I n f
Data Raw:	49 44 3d 22 7b 42 33 35 41 42 35 44 30 2d 31 35 42 38 2d 34 46 33 33 2d 38 44 41 30 2d 38 45 44 42 43 41 32 42 34 42 30 41 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: PROJECTwm, File Type: data, Stream Size: 41	
General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.0773844850752607
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7	
General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	ISO-8859 text, with no line terminators
Stream Size:	7

General	
Entropy:	1.8423709931771088
Base64 Encoded:	False
Data ASCII:	a . . .
Data Raw:	cc 61 ff ff 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 5116	
General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	5116
Entropy:	1.9231245259582155
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . P . . . . . " . . . . . q . . . . . A . . . . . ` . . . . . `) " . . . . .
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 22 00 1f 00 00 00 00 00 01 00 01 00 00 00 01 00 71 07 00 00 00 00 00 00 00 00 00 00 a1 07 00 00 00 00 00 00 00 00 00 00 d1 07

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 2724	
General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	2724
Entropy:	2.6915430960066646
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . P . . . . . p . . . . . 1 . . . . . ` . 1 . . . . . , . . p . . . . . q . . . . . a . . . . . ` . . . . . X . . p . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 50 00 b1 08 00 00 00 00 00 00 00 00 00 00 00 04 70 08 00 fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 486	
General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	486
Entropy:	6.292426243264921
Base64 Encoded:	True
Data ASCII:	. . . . . 0 . . . . . H . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . A P d - . . . " . < . . . r s t d o . l e > . . s . t . . d . o . l . e . (. . h . . * \ \ . G { 0 0 0 2 0 4 3 0 - . . . . C . . . . . 4 6 } # 2 . 0 # . 0 # C : \ \ W i n . d o w s \ \ s y s @ t e m 3 2 \ \ . e 2 . . t l b # O L E . A u t o m a t . i o n . E N o r (m a l E N C r . m . a F . . c E C . . . . > m . ! O f f i c g O . f . i . c g . . g 2 D F 8 D 0 . 4 C - 5 B F A
Data Raw:	01 e2 b1 80 01 00 04 00 00 00 03 00 30 aa 02 02 90 09 00 20 14 06 48 03 00 a8 80 00 00 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 00 08 06 12 09 02 12 80 41 50 f4 64 2d 00 0c 02 22 0a 3c 02 0a 16 02 72 73 74 64 6f 08 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 00 28 0d 00 68 00 11 5e 00 03 2a 5c 00 47 7b 30 30 30

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 12, 2022 00:26:03.640768051 CEST	49742	80	192.168.2.3	45.8.146.139
Aug 12, 2022 00:26:06.760776997 CEST	49742	80	192.168.2.3	45.8.146.139
Aug 12, 2022 00:26:12.761372089 CEST	49742	80	192.168.2.3	45.8.146.139

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: **5636**, Parent PID: **756**

General

Target ID:	0
Start time:	00:25:56
Start date:	12/08/2022
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:	0x11a0000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstB6E7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstB6E8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstB718.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstB748.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	659F977C	unknown
C:\Users\user\AppData\Local\Temp\yC6BA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	142046AB	GetTempFileNameA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14206626	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14206626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14206626	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14206626	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14206626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14206626	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14206626	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14206626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14206626	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14206626	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14206626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14206626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7B8918C8.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	65925805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\515DF229.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	65925805	unknown
C:\Users\user\AppData\Local\Temp\~DF23D671D49BDC7411.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	65925805	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstB6E7.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstB6E8.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstB718.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstB748.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\yC6BA.tmp	success or wait	1	14204702	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DF23D671D49BDC7411.TMP	success or wait	1	65925805	unknown
C:\Users\user\Desktop\~$ame removed] file 08.11.2022.doc	success or wait	1	65925805	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7B8918C8.png	0	65536	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 7c 00 00 02 0e 08 02 00 00 00 34 fd 21 fd 00 00 20 00 49 44 41 54 78 fd fd fd 7b 23 d1 fd 1b 39 67 10 04 fd 70 fd fd fd 6c fd 2b fb fd fd fd 5e 78 fd fd 5b fd fd 27 07 0e 13 08 10 39 fd fd fd 67 fd 4b fd 74 37 fd 30 23 da fd fd 43 61 fd 0e fd e9 53 fd fd 5b 6f 05 3a fd 4e 3a fd 76 1c 27 10 08 04 02 fd fd 72 19 0c 06 57 fd fd fd 71 04 02 fd fd fd 21 fd 04 02 01 fd fd 71 fd 43 46 fd 67 fd fd 1c 5f 0e 63 fd 79 fd fd fd 11 fd fd 0f fd 2c fd 3b 39 fd 0c fd fd 36 13 fd 5f 7a fd 04 fd 2c fd 2f d7 fd fd fd fd 6e 74 fd fd fd 2f d7 fd 67 fd 74 fd fd fd 5f 14 fd 08 fd fd fd 1c 5f fd 2f fd 2d fd fd fd fd fd fd 46 fd fd fd fd fd 2b 6d 74 fd 58 fd fd 79 2f fd fd fd 2b fd	PNGIHDR|4! IDATx{#9gpl+^x['9gK t70#CaS[o:N:v'rWq!qCFg _cy,;96_z,/nt/gt__/- F+mtX/+	success or wait	2	65925805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\515DF229.png	0	65536	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 fd 00 00 01 fd 08 06 00 00 00 37 fd fd 00 00 00 01 73 52 47 42 00 fd fd 1c fd 00 00 00 04 67 41 4d 41 00 00 fd fd 0b fd 61 05 00 00 00 09 70 48 59 73 00 00 21 fd 00 00 21 fd 01 04 fd fd fd 00 00 fd fd 49 44 41 54 78 5e fd fd 09 fd 66 47 55 fd 0d 33 fd 57 1c fd fd 7d fd fd fd fd fd fd 2a 24 fd 61 fd 01 31 fd fd fd 20 fd 29 61 54 fd 28 2a 90 fd 09 68 fd 10 fd fd fd fd 74 77 fd 19 21 08 21 fd 20 20 46 10 fd fd fd 70 48 fd 51 26 fd fd fd fd 73 fd 4f 0f 49 18 fd 3e fd fd fd 7f fd fd fd fd 4a 75 fd fd 34 fd fd 27 fd 55 fd aa 55 fd b5 56 55 fd 73 fd 0e fd 39 fd 2d fd 7e fd 21 fd 18 2b 03 52 fd 38 fd fd 32 fd 53 fd fd 32 3d fd 07 55 fd fd 6a 5b fd 67 3e fd fd 3c 38 fd fd fd 40 fd	PNGIHDR7sRGBgAMAapHYs!!IDATx^f GU3W}*$a1)aT(*htw!! FpQ&sOl>Ju4'UUVUs9-~!+R82S2=Uj[g><@	success or wait	4	65925805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\[name removed] file 08.11.2022.doc	unknown	14	success or wait	2	65B82FF3	unknown
C:\Users\user\Desktop\[name removed] file 08.11.2022.doc	unknown	4	success or wait	16	65B8253D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	658F765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	658F765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	end of file	1	658F765D	unknown
C:\Users\user\Desktop\[name removed] file 08.11.2022.doc	1871139	333	success or wait	2	65925805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	65938A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	65938A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	65938A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\29532	success or wait	1	65925805	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	65925805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\29532	29532	binary	04 00 00 00 04 16 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 85 47 68 E6 1C AE D8 01 32 95 02 00 32 95 02 00 00 00 00 00 DB 04 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	65925805	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 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	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2022-08-12T00:26	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	65925805	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\00006109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358364678	1426849799	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358364683	1426849804	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C00000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1358364678	1426849799	success or wait	1	658F765D	unknown

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\00006109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426849799	1426849800	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426849800	1426849801	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426849804	1426849805	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426849805	1426849806	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C00000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426849799	1426849800	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C00000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426849800	1426849801	success or wait	1	658F765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\29532	29532	binary	04 00 00 00 04 16 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 85 47 68 E6 1C AE D8 01 32 95 02 00 32 95 02 00 00 00 00 00 DB 04 00 00 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	04 00 00 00 04 16 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 00 32 95 02 00 32 95 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 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	success or wait	1	65925805	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 FF FF FF FF 00 00 00 00 00 00 00 00				

Disassembly

No disassembly