ID: 682661
Sample Name: cis-broadband invoice 08.11.22.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:16:10
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

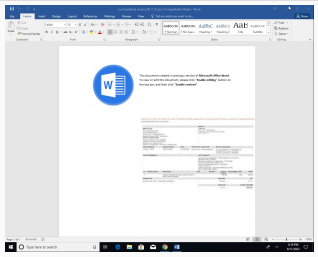
Windows Analysis Report

cis-broadband invoice 08.11.22.doc

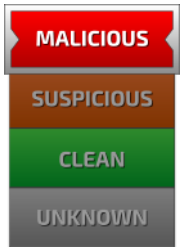
Overview

General Information

Sample Name:	cis-broadband invoice 08.11.22.doc
Analysis ID:	682661
MD5:	91ca71d98c0e42..
SHA1:	b8b01ee5940864.
SHA256:	373856a75b7840.
Tags:	doc IcedID
Infos:	



Detection

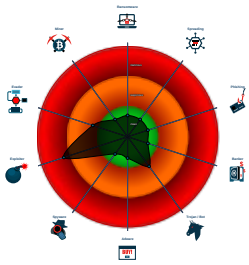


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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: 1868 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)

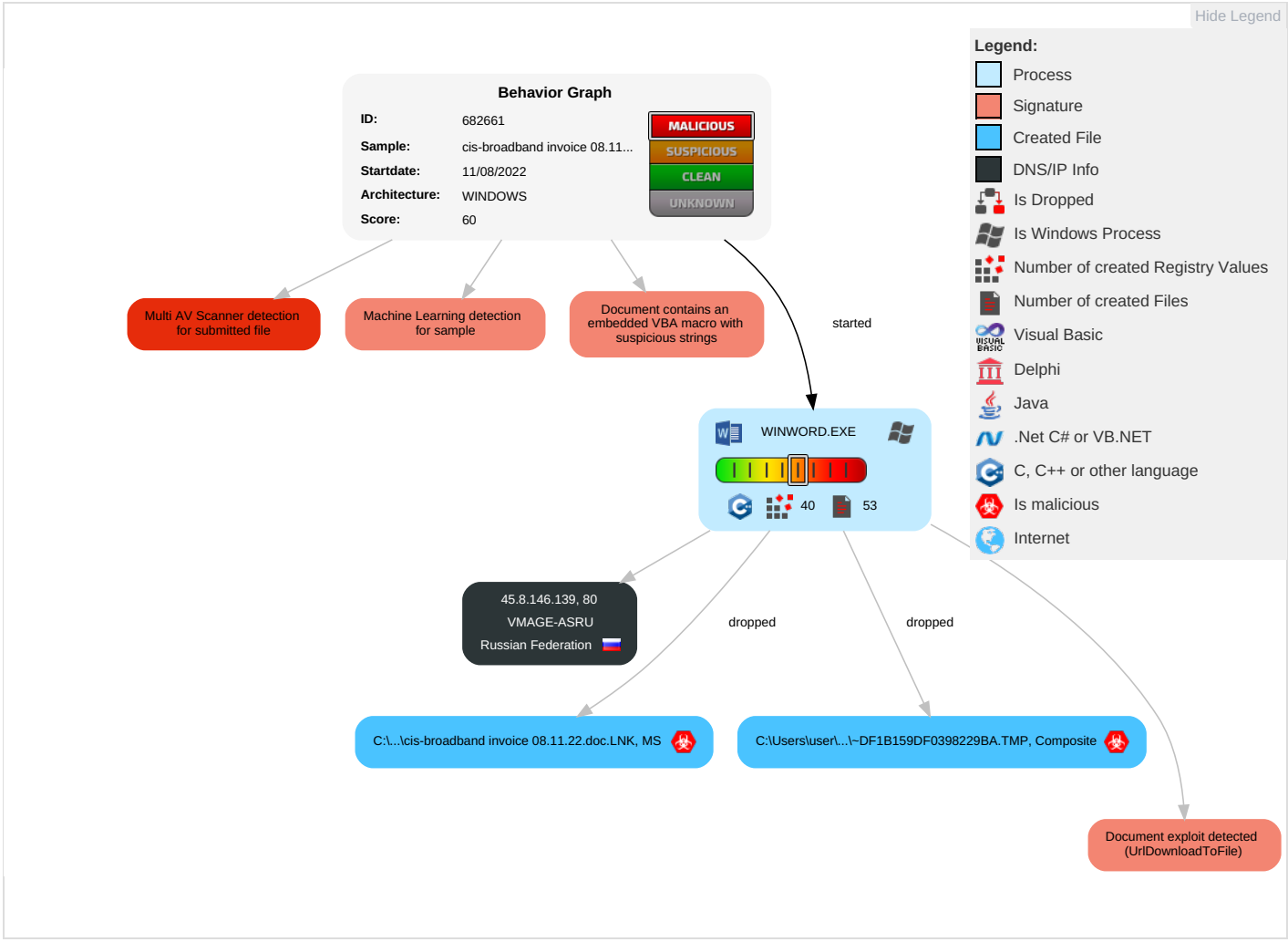
System Summary

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	1 Extra Window Memory Injection	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 2 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Extra Window Memory Injection	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

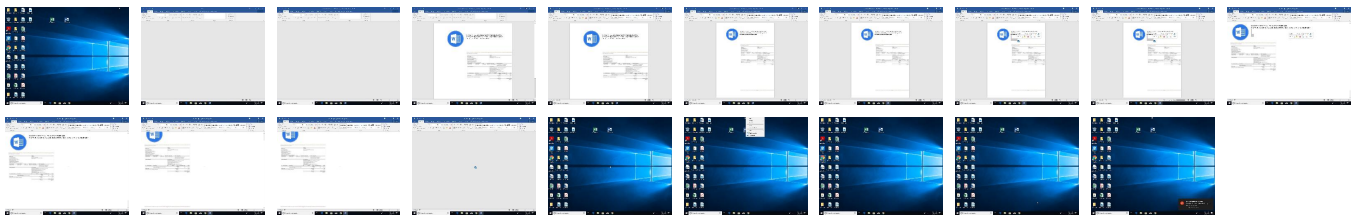
Behavior Graph

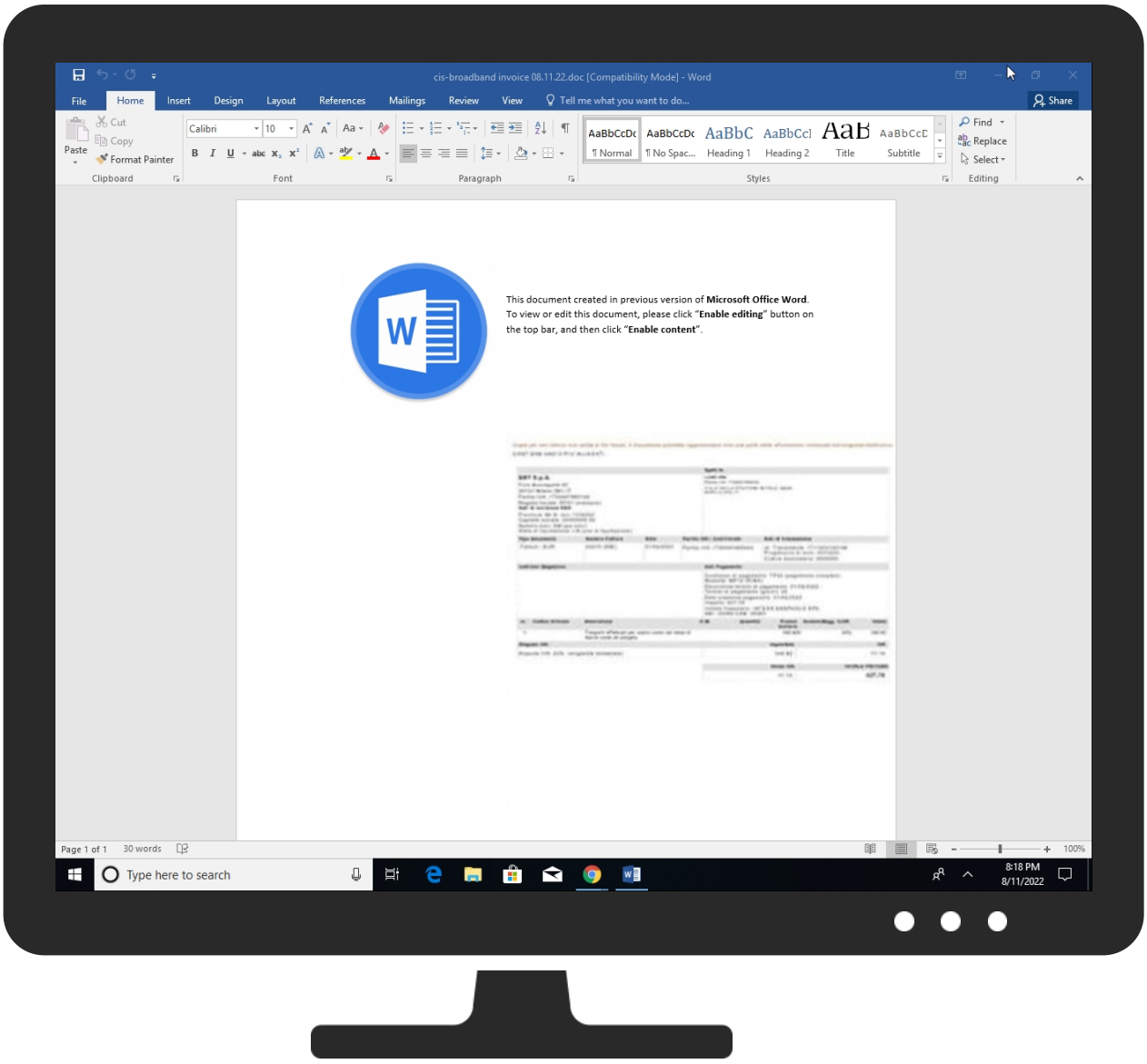


Screenshots

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
cis-broadband invoice 08.11.22.doc	25%	Virustotal		Browse
cis-broadband invoice 08.11.22.doc	15%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
cis-broadband invoice 08.11.22.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF1B159DF0398229BA.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

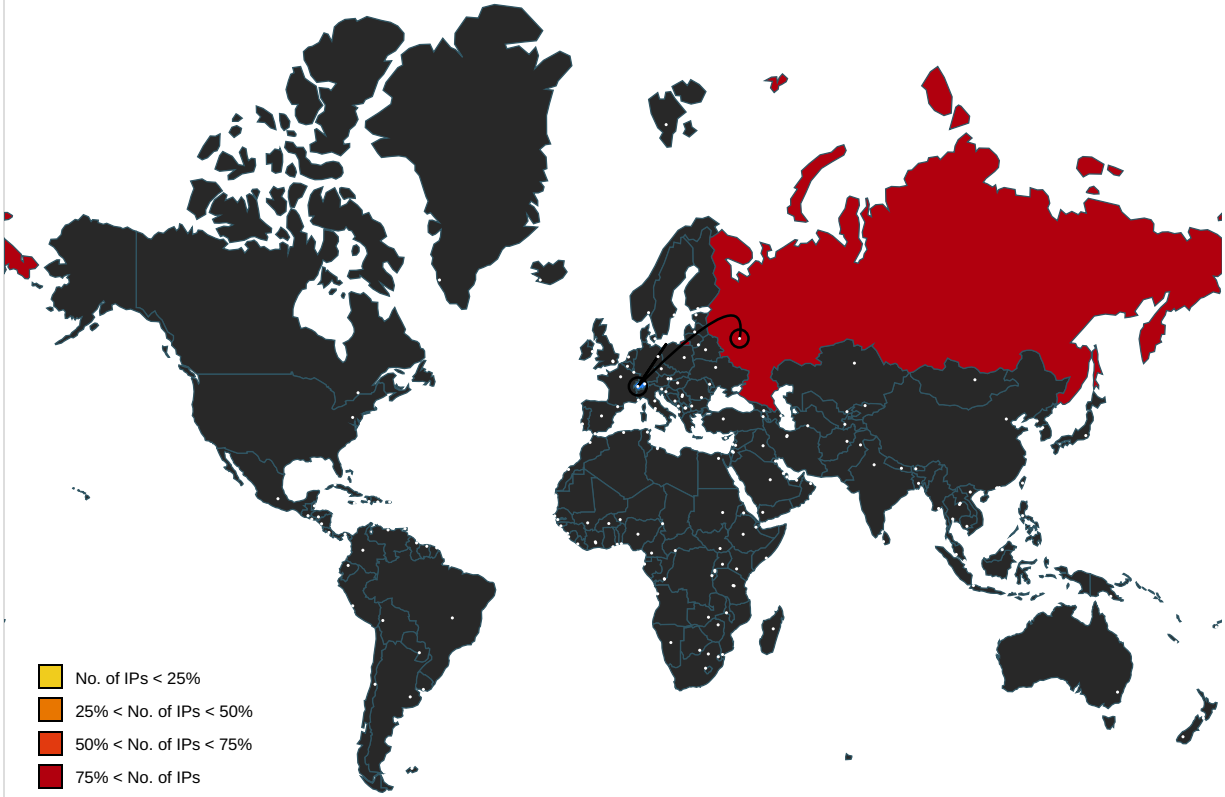
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://login.microsoftonline.com/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://shell.suite.office.com:1443	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://autodiscover-s.outlook.com/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://roaming.edog.	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://cdn.entity.	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://powerlift.acompli.net	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://cortana.ai	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://api.aadrm.com/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://api.microsoftstream.com/api/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://cr.office.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://graph.ppe.windows.net	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://my.microsoftpersonalcontent.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://messaging.engagement.office.com/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://web.microsoftstream.com/video/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://dataservice.o365filtering.com/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://ncus.contentsync.	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://weather.service.msn.com/data.aspx	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://apis.live.net/v5.0/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://messaging.lifecycle.office.com/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://management.azure.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://outlook.office365.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://wus2.contentsync.	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://api.office.net	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://entitlement.diagnostics.office.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://outlook.office.com/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://outlook.office365.com/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://webshell.suite.office.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://management.azure.com/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://devnull.onenote.com	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messaging.action.office.com/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://ncus.pagecontentsync.	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://messaging.office.com/	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	C0AEEC49-6B3D-4037-965A-40C5DB21F9AC.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:	682661
Start date and time:	2022-08-11 20:16:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cis-broadband invoice 08.11.22.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:	mal60.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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.76.141, 52.109.88.37, 52.109.76.34
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.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\C0AEEC49-6B3D-4037-965A-40C5DB21F9AC

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):	5.358151187659545
Encrypted:	false
SSDEEP:	1536:DcQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:a1Q9DQe+zuXYr
MD5:	4535D15B864E4FCE74BC9E58C3ACB1AF
SHA1:	57C32FE73D39C65B5092860D18D3D106AE264063
SHA-256:	0208448D5B9D24C385319DFE51BB32CD3C29E5E500F9F52E88BB6DF93F1B1B69
SHA-512:	713CE648B783F49604B4C7F4004E498E737B093FBBFE43B76ED85DE1170AA2DF4CBC59ADDC0AC2752824B6D7C033062804CF432C07CDBA3D01F7011A818F66A
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="2022-08-11T18:17:17">.. 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\7CD912C7.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 410 x 568, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	61935
Entropy (8bit):	7.988218918927523
Encrypted:	false
SSDEEP:	1536:vFo53cC4vJ7Y8qgUmqhIIPI2MM+ikJU78DPaFx:vy53qv6nmII0I2ngJAEan
MD5:	4800E90C87A78932178C7D338BA32F43
SHA1:	8006244EDAFF9A31546A17FCF99CB61DA4F69417
SHA-256:	8CD11EB654C64C7315F7B2904D123532F7993FAF2F210B250C4C4D670200FF73
SHA-512:	58994BDC81FF937B05B307C161F852383DAA8504EA17522CD96CDE6EBF99E4992BA64DBEA532424AC16FBD8273999295DBBB74E48A77AAB2122C5701633DC7A3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....8.....X.L.. .IDATx..}i..F.-..\r.E.l..u..3....L....^TR-.....DF...*I.e;i.:U.L&...pq.p.1.HD.Z.@.6.._cc.....>.n....2v..c.%...)..G.?|...>k...bf.....c0.sy..$...a....<.....>".=X1.....1.^|.....|.....|`E..c.#.T.....'.'.....$6&L1.0.H...X&".cp.l...p.>..?.@?.1.Tp.....Y...=D.]....).w=...~..yp...{x/.....d}1.G.h..b."1..-}.0x...O.....<. &n...0.1...el...."". ....C<t..A.H..4O.L.G....v...6Bd....W{..>..;W.....E.#<..s.^...Q...B.o.=l.lB{...1.ab.$D..:WB$O..V..>..k...y~.w".....A...-.D..;.I.4b.D..E".3...1...f....J.~xv.35G&&....?.acR...P.N....)...U.J....F.I...c$... ....a..z&...1..I...D...b.A4.....U.._.D.Z...E.6.G9t..=..qj...^L.$.;...>..S&dD.X... 1...0.{~.w..P.....1.U(.....j.PM.....9J..[.O2...).12swy%.3..M?NGt_.....Z.....?F..+.....[4@.=.....;.".6..i.c..qH4...Ll...8.kl....=""".!..h.g7.\'.....Bb.A...f..o).+..`..++..?u..<.i.M..Gvs..@w.$.2X..'.[.h.8h.3..G.g.E...3..d.)..V*../$)...."%...F....~...s.1@|.....dE.8D|..d.....N.z..(...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A9F03E1C.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):	256229
Entropy (8bit):	7.979121196288089
Encrypted:	false
SSDEEP:	6144:xcZ1/hftNLDurggURJVg/41g/U14PThyg2vnHkX005Pk:xcZ15ftNLy5MJMM4Ff2vHI00y
MD5:	9D69322290350F00911BF601D1EB0548
SHA1:	2CC5B16D959BCCF6457C881EC3106EDD846E77E6
SHA-256:	4B4AA777CC69D3E05C61AA4F57475E1F41B4AA8DA40463AD4EBF2CA98AD5A927
SHA-512:	C7CC06DCDD2E9DA32FBDC0BD4B5F5CFBC937C980CBB66DDFD2953DFC7DD4EB9D69E19EA72BF3D291D4F229CAE015A9C83040AA5DE23563B1D28BDF0E9875CCD
Malicious:	false
Reputation:	low

Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!...!.....IDATx^....fEu..;..&..&.....c....Fc.....b41q`FlAQ....44 8+m....CL'.!...!*Q..>.g.!H...?.g.uzuQ.=....TW. Z.V..j.]....?. .V1...P.JO.K.h..IO.*7.oi...=:.i.l.'oV.V7.K@..6.%j."....I....[..5Td= yI.....P.....d>Q..ke....I9.H^...\....h.cm....'1.....+.$.....S.....J...g....U.8..:....3.h.ni5...'Z^.'..j...&..- 3.....8Q...j..[Y...t..^..zh..#_.E-W.5...r!Q..U..V...*..Z..|.[.....m.=z;.2.5....8./.,K.u...U~L.i-oV.t...A.!.{;.k.1z-..+....[> _.S.\-.l.W.D...Nz..^..`.r.,...b..z.^>..{.Te..2N..~.....T=..4... he&....X.m..V.....D..5]...j...%.L.....F=YW.3..Z..*..h.S..e..).jz9...IK~O.E.L.@..Z~E.z.D..I....B..#$.|...u.^....t.c.d..{2.#.h.W...U. _.=.PudH.*....'2?FK:q[~....aL.Mg..J..+/..*Z=.'N .h..D..t...G..m..@hL..3..Zz.3.b.....ze.LO>..q.5.5.=...m..[^..8.....c.6.5..gh1F_n.U^.n.%.G.....N.*....eA-..X:..}..|.Y..6.^....[[.e@.'..-..%..g.Z...t...L..R&.5..j:Q.IE...uI.....D.W~..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{9343E1C6-3507-4871-9EDD-1A22949243C5}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{BBC4E15D-9EE8-46CF-A28B-0D2AE4D0041E}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.1256146146486787
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82lrBkwkvGtklT3ls3lHll/3lwZZ6/vlk:4LG1ND9Pxn82TkIgKrhc
MD5:	A6C46D28C8F9D02A012AAA25896630B8
SHA1:	7A1DB7B158DF32B3D8EC3656FA4C08D07B20EC98
SHA-256:	04A5BDBB912F30C24E48817448574D6B3DE5E5F61354B329B98D1B1C8D6B9586
SHA-512:	1250F816535DA5B58CC0788EBA4E076DFAAF74CBAD332D057C7A96E45BD47D55E4B775331ED4E3B7328103A576FCD1999259CC28F23BAF3E312E4983C3C256 5
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\~DF1B159DF0398229BA.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):	50688
Entropy (8bit):	4.446604929324278
Encrypted:	false
SSDEEP:	768:rajpiVUVvpRoBIY0DH5fZaYw6tHRtyb2:raliVUZpRvHGkH
MD5:	C520FE2725CF6BA67E5EA4781911910D
SHA1:	277D17A5DEB768540F22E814DE0D69C6A9261C07
SHA-256:	1996A41078B6D525183688EFA0402F61FF70B22858F875C997DE07127155BF6D
SHA-512:	5496DBB5271D37308B65077C33A2CB47ECF70D5BC2205EC329E9E5100DBDE925E72186BFB4BE565D6C64F4AE27BE62CCD023F70307334723F992A0E1375377D
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...N...M.....O...P...Q...Z...S...T...U...V...W...X...Y...L...[...\...^....._...`...a.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\cis-broadband invoice 08.11.22.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 15:31:46 2022, mtime=Fri Aug 12 02:17:18 2022, atime=Fri Aug 12 02:17:13 2022, length=2203257, window=hide
Category:	dropped
Size (bytes):	1155
Entropy (8bit):	4.708831443860152
Encrypted:	false
SSDEEP:	12:8p3C0UfhuElPCH2K0jAYIyWA+WvpKf+79zijAy/TXLDq9zwDVRG35Gp4t2Y+xIBx:8puW4nkfaBeAy7XiBwDse7aB6m
MD5:	474B37F558E14925F9B1212D25DBD614
SHA1:	4377AA6CA78D766CAAFE8BFC961BC3524CB38938
SHA-256:	1ED97E92781C95B6271A3201F64E4D1DDDAF5D671B2B77E430E903437931A08C
SHA-512:	1690743B65F867487BA59E98DD8C18F0E7978661AA7164FE9F8D39E75E66F098196EB8F451275B4455BAE646A94CA6D528A91720DF720E983DA3E55EB5BA0163
Malicious:	**true**
Preview:	L.....F.... ...51...3..,....._`.....y.!.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...U .....:.....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..U .....S.....J=2.h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..U .....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.y.!..U'. .CIS-BR~1.DOC..v.....hT...U'.....h.....\9W.c.i.s.-.b.r.o.a.d.b.a.n.d. .i.n.v.o.i.c.e. .0.8...1.1...2.2...d.o.c.....h.....-.....g.....>.S.....C:\Users\user\Desktop\cis-broadband invoice 08.11.22.doc..9....\....\....\....\....\.D.e.s.k.t.o.p.\.c.i.s.-.b.r.o.a.d.b.a.n.d. .i.n.v.o.i.c.e. .0.8...1.1...2.2...d.o.c.....:.,.LB.)...As...`....X.....377142.....!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):	4.764454533436411
Encrypted:	false
SSDEEP:	3:bDuMJleUHELgLplbbBCmX1bWEHELgLplbbBCv:bCU7DbbBsu7DbbBs
MD5:	88B2B35166DDB96A4C8E5C35506C4D74
SHA1:	219395A96048D3375C111B5D6398AE08B39698FB
SHA-256:	F2EB906A7F898C6D0BD9BB810C148AEA114FC666EDC42C919ED4756972682B29
SHA-512:	951B95945B07B1D905C5FBAB8606CC9B9211BD94ED1391F010C4963089B774727FD16851BCB5F482A2C39DF9469FCE65B81008E1C06E9EC43D29A012169EBF3
Malicious:	false
Preview:	[folders]..Templates.LNK=0..cis-broadband invoice 08.11.22.doc.LNK=0..[doc]..cis-broadband invoice 08.11.22.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):	2.1633835850239973
Encrypted:	false
SSDEEP:	3:Rl/Zdy6bttt7MsXcJ/lBlqK7+X1tln:RtZThXcJ/cg+1
MD5:	7B8282E0ABFEABA447F740463AF49C87
SHA1:	2EC7CF9497B7F66A5DBD8F1B73D8139B0AC9540C
SHA-256:	B4F4AA389E94E835FB0CF860BD05356282C64D8969097764C3944C35B5B992C8
SHA-512:	5DE382D69575F0BC030513A7B654D6C8B337EA5C4D62D5E0BBA39B485794DD5BE838F7CF82B9F6C95B92FEBF49F2B725F8CEE043C0CCDD94020E4843EE8B5A6E
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....8.....".9.....H.....6C.....&.:.....

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\~$s-broadband invoice 08.11.22.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1633835850239973
Encrypted:	false
SSDEEP:	3:Rl/Zdy6bttt7MsXcJ/lBlqK7+X1tln:RtZThXcJ/cg+1
MD5:	7B8282E0ABFEABA447F740463AF49C87
SHA1:	2EC7CF9497B7F66A5DBD8F1B73D8139B0AC9540C
SHA-256:	B4F4AA389E94E835FB0CF860BD05356282C64D8969097764C3944C35B5B992C8
SHA-512:	5DE382D69575F0BC030513A7B654D6C8B337EA5C4D62D5E0BBA39B485794DD5BE838F7CF82B9F6C95B92FEBF49F2B725F8CEE043C0CCDD94020E4843EE8B5A6E
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....8.....".."..9.....H.....6C.....&..:.....

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993383170496904
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:	cis-broadband invoice 08.11.22.doc
File size:	2298962
MD5:	91ca71d98c0e42e0446e9157fc83e1f2
SHA1:	b8b01ee5940864817c670187dfc1cb9a663c79a8
SHA256:	373856a75b78406d26cfbb41cbbba7041bad1e56a3304ba17376b294bc773eee
SHA512:	f5ca7cb3645558bd8e390d34721ce9abfd93912c56a9470e7f2e5ebab52bcdf82c5740e90e3d0f8d0710fdc313cd9570e3fee05f897d1883af04df2773740717
SSDEEP:	49152:l5cNRR+7lr64bJwEeTVzVSqJI4VBnLiiYRCcuaNTSIY:l5cbR+7bmEcVQ4VBnOiYGCTG
TLSH:	FAB53374A4EC9D32EA4FA3B1D78634E5F6C97C8D30B84657671F1902D0AAA1E03E21F5
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/682661/sample/cis-broadband invoice 08.11.22.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: 2837	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2837
Data ASCII:	.h.Attribut.e VB_Nam.e = "Thi.sDocumen.t"...Bas..1Normal...VGlobal!.Spac.lFa.lse.JCrea.tabl. .Pre decla..Id..#Tru."Exp.ose..Temp.lateDeri.v.$CustomlizC.P.... .D.? PtrSa.fe Function .... Lib ".user32" .Alias "S.etTimer" (ByVal..... As Long.1, ..*.....
Data Raw:	01 68 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: 365	
General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	365
Entropy:	5.3000173575513605
Base64 Encoded:	True
Data ASCII:	ID="{4ACDA209-D3D8-436D-A5D9-6DA204CC3EA8}"..Document=ThisDocument/&H00000000..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="EBE9F817E71BE71BE71BE71B"..DPB="D6D4C50C5B1C471D471D47"..GC="C1C3D2D7D3D7D328"....[Host Extender Info]..
Data Raw:	49 44 3d 22 7b 34 41 43 44 41 32 30 39 2d 44 33 44 38 2d 34 33 36 44 2d 41 35 44 39 2d 36 44 41 32 30 34 43 43 33 45 41 38 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:	ThisDocument.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
Entropy:	1.8423709931771088
Base64 Encoded:	False

General	
Data ASCII:	a . . .
Data Raw:	cc 61 ff ff 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 5108	
General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	5108
Entropy:	1.936648264793182
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . 8 . . . . P . . . . " . . . . q . . . . A . . . . ` . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . ` i 8 . . . .
Data Raw:	72 55 40 04 00 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 38 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 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 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:	2.691025655888252
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . . ` . . . . . . . . . . . . . . p . . . . . . . . . . . . . . . . . 1 . . . . . . . . Q . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . P . 1 . . . . . . . . . . . , . . p . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . ` . 1 . . . . X . . p . . . . Q . . . .
Data Raw:	72 55 40 00 00 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 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 60 00 b1 08 00 00 00 00 00 00 00 00 00 00 00 00 00 04 70 10 00 fe ff ff ff 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:	6.307455107707739
Base64 Encoded:	True
Data ASCII:	. . . . 0 . . . . . . H . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . J 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 b9 4a 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 11, 2022 20:17:23.791425943 CEST	49744	80	192.168.2.3	45.8.146.139
Aug 11, 2022 20:17:26.798727036 CEST	49744	80	192.168.2.3	45.8.146.139
Aug 11, 2022 20:17:32.798871994 CEST	49744	80	192.168.2.3	45.8.146.139

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: **1868**, Parent PID: **756**

General

Target ID:	0
Start time:	20:17:14
Start date:	11/08/2022
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:	0xfd0000
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\tstD491.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\tstD492.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\tstD493.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\tstD4C3.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\yE686.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	145D46AB	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	145D6626	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	145D6626	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	145D6626	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	145D6626	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	145D6626	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	145D6626	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	145D6626	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	145D6626	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	145D6626	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	145D6626	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	145D6626	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	145D6626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7CD912C7.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\A9F03E1C.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\~DF1B159DF0398229BA.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\tstD491.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstD492.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstD493.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstD4C3.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\yE686.tmp	success or wait	1	145D4702	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DF1B159DF0398229BA.TMP	success or wait	1	65925805	unknown
C:\Users\user\Desktop\~$s-broadband invoice 08.11.22.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\7CD912C7.png	0	61935	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 fd 00 00 02 38 08 02 00 00 00 fd 58 fd 4c 00 00 20 00 49 44 41 54 78 fd fd 7d 69 fd fd 46 fd 2d 10 11 5c 72 fd 45 fd 6c fd fd 75 fd fd 33 fd fd 07 fd 4c fd fd fd fd 5e 54 52 2d fd fd fd 08 fd 0f fd 44 46 fd fd fd 2a 49 fd 65 3b 69 fd 3a 55 fd 4c 26 17 fd 06 70 71 01 70 fd 31 fd 48 44 fd 5a fd 40 fd 36 11 fd 5f 63 63 fd fd 00 fd fd fd fd fd e0 3e 3e fd 6e 07 0e 1b fd 32 76 7f fd 63 fd 25 07 fd fd 29 fd fd 47 fd 3f 7c fd fd 5c 3e 6b 11 fd fd 62 66 fd fd fd fd fd fd 63 30 1f 73 79 ef fd 24 fd fd fd 61 fd fd fd fd 3c fd 0b fd fd 1f fd 0e 3e 22 fd 3d 58 31 10 11 0b fd fd 31 fd 5e 49 7c 2e fd fd fd fd 15 7c 21 0b 09 fd fd 19 49 60 45 fd fd 63 fd 23 fd 54 0f fd 7f fd 15 fd 27 fd 27 13 fd 18 fd	PNGIHDR8XL IDATx}iF-\rElu3L^TR-DF*Ie;i:UL&pqp1HDZ@6_cc>n2vc%)G?|>kbfc0sy$a<>"=X11^|.|!|`Ec#T"	success or wait	1	65925805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A9F03E1C.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 45 75 fd 0f 3b 8c fd 26 fd fd 26 fd fd fd fd 1a 01 fd 09 63 fd fd fd fd 46 63 fd fd 09 1c 20 62 34 31 71 60 46 6c 41 51 11 10 fd fd 34 34 20 38 2b 6d fd fd 18 13 43 4c 27 fd 21 18 fd fd 21 2a 51 fd fd 3e fd 67 fd 21 48 fd fd fd 3f fd 67 fd 75 7a 75 51 fd 3d fd fd 7f 0f 54 57 fd 5a fd 56 0d fd 6a fd 5d fd fd fd fd fd 0a fd 3f fd 20 d5 56 31 fd fd 06 50 fd 4a 4f 12 4b 1a 68 fd 15 49 4f fd 2a 37 fd 6f 69 fd 01 0a 3d 3a fd 69 fd 6c fd 27 6f 56 fd 56 37 fd	PNGIHDR7sRGBgAMAapHYs!!IDATx^f Eu;&&cFcb41q`FlAQ448+mCL'!!*Q>g!H?guzuQ=TWZVj]?V1PJOKhlO*7oi=:il'oVV7	success or wait	4	65925805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\cis-broadband invoice 08.11.22.doc	unknown	14	success or wait	2	65B82FF3	unknown
C:\Users\user\Desktop\cis-broadband invoice 08.11.22.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\cis-broadband invoice 08.11.22.doc	1871659	184	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

Key Path	Completion	Count	Source Address	Symbol
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\2C4DD	success or wait	1	65925805	unknown
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\2C4DD	2C4DD	binary	04 00 00 00 4C 07 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 48 A6 F3 2A FA AD D8 01 DD C4 02 00 DD C4 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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				
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	2022-08-11T20:18	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	1426784263	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	1426784268	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	1426784263	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	1426784263	1426784264	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	1426784264	1426784265	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	1426784268	1426784269	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	1426784269	1426784270	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	1426784263	1426784264	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	1426784264	1426784265	success or wait	1	658F765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2C4DD	2C4DD	binary	04 00 00 00 4C 07 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 48 A6 F3 2A FA AD D8 01 DD C4 02 00 DD C4 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	04 00 00 00 4C 07 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 DD C4 02 00 DD C4 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 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	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