ID: 682695
Sample Name:
bergo.document.08.11.2022.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:57:50
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

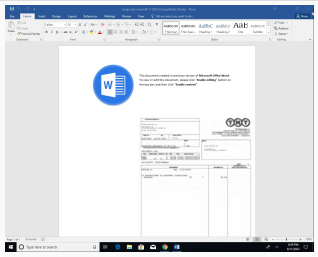
Windows Analysis Report

bergo.document.08.11.2022.doc

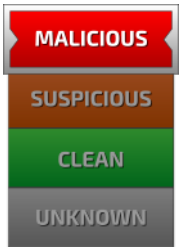
Overview

General Information

Sample Name:	bergo.document.08.11.2022.doc
Analysis ID:	682695
MD5:	228c063e5ce747..
SHA1:	e13b37423003eb.
SHA256:	025d824f7fd0627.
Tags:	doc IcedID
Infos:	



Detection

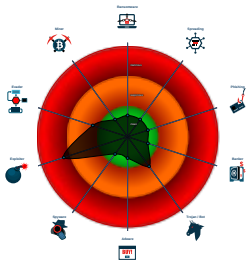


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 5512 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

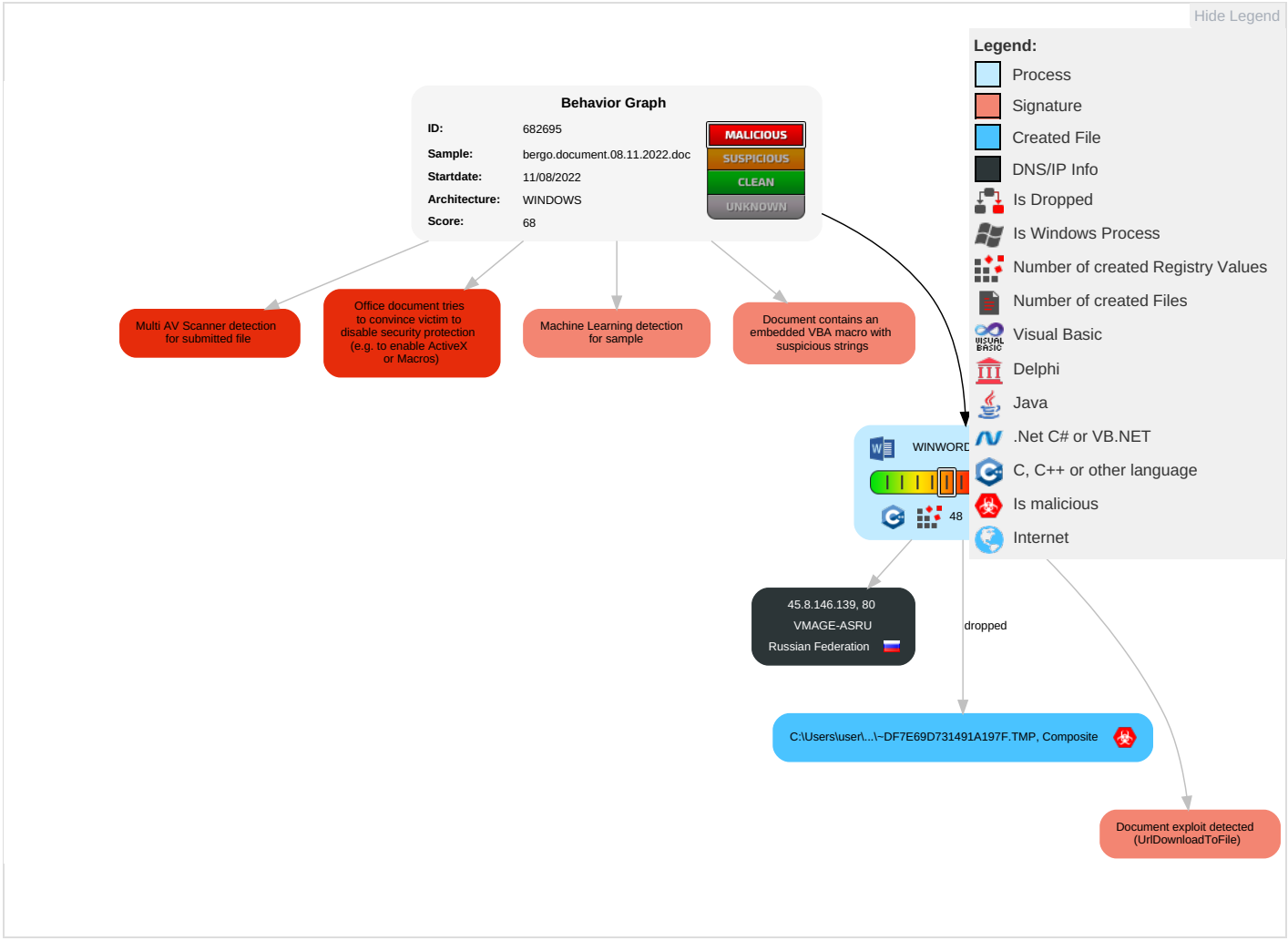
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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	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 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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Extra Window Memory Injection	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

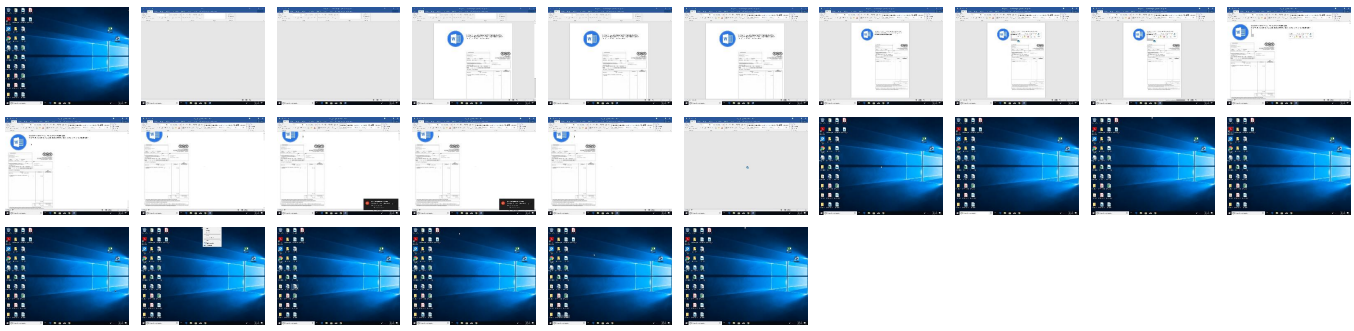
Behavior Graph

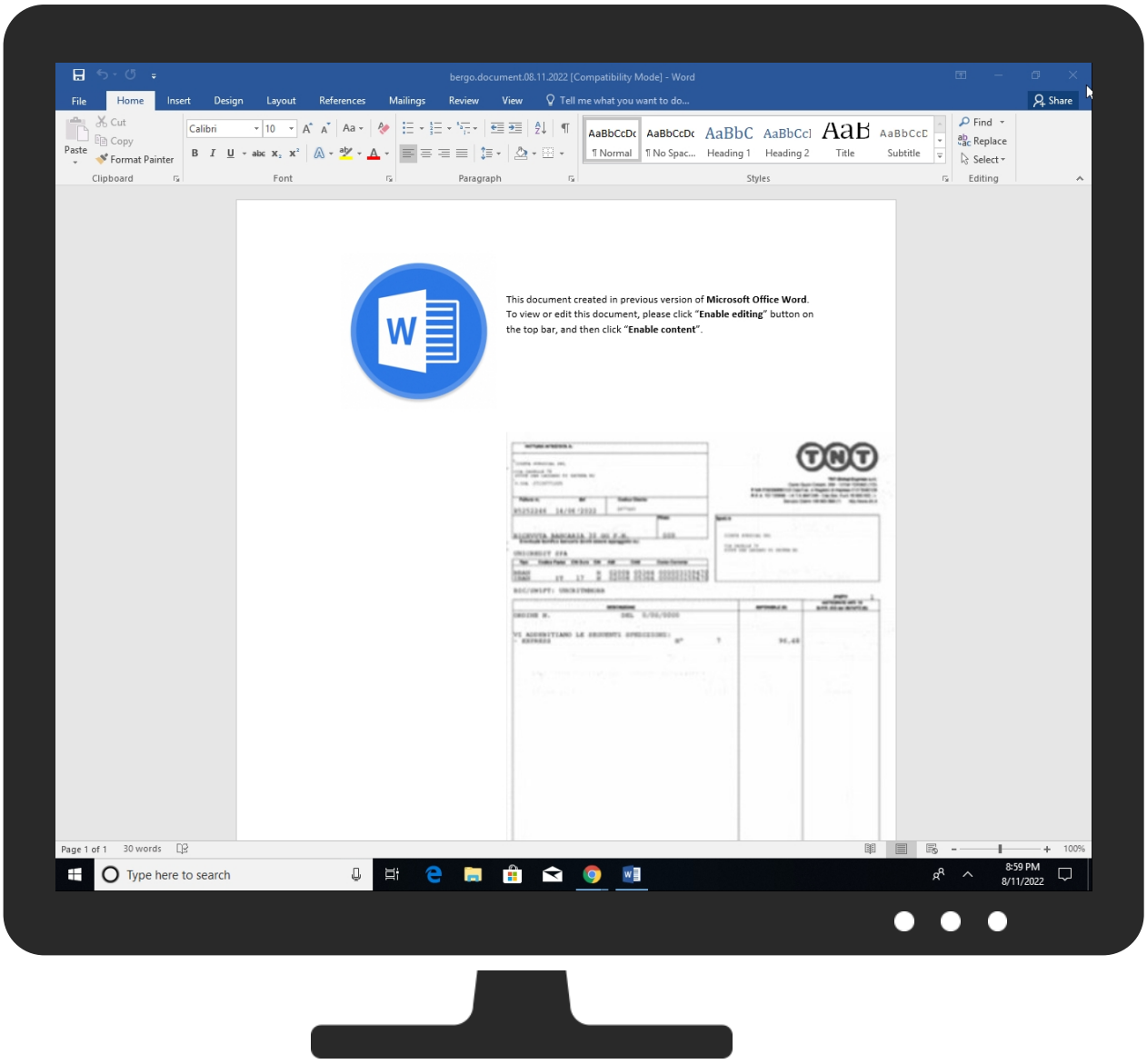


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
bergo.document.08.11.2022.doc	25%	Virustotal		Browse
bergo.document.08.11.2022.doc	18%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
bergo.document.08.11.2022.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF7E69D731491A197F.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

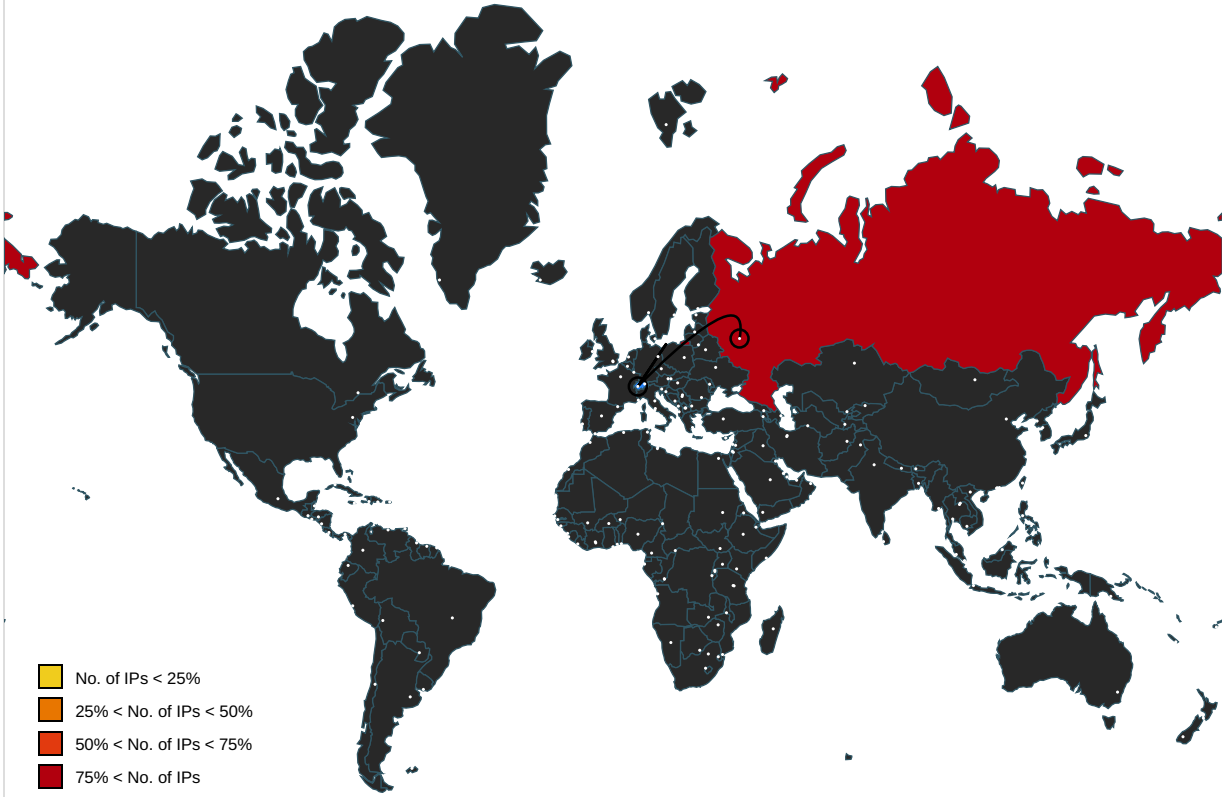
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://login.microsoftonline.com/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://shell.suite.office.com:1443	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://autodiscover-s.outlook.com/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://roaming.edog.	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://cdn.entity.	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://powerlift.acompli.net	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://cortana.ai	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://api.aadrm.com/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://api.microsoftstream.com/api/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://cr.office.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://graph.ppe.windows.net	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://my.microsoftpersonalcontent.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://messaging.engagement.office.com/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://web.microsoftstream.com/video/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://dataservice.o365filtering.com/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://ncus.contentsync.	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://weather.service.msn.com/data.aspx	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://apis.live.net/v5.0/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://messaging.lifecycle.office.com/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://management.azure.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://outlook.office365.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://wus2.contentsync.	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://api.office.net	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://entitlement.diagnostics.office.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://outlook.office.com/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://outlook.office365.com/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://webshell.suite.office.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://management.azure.com/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://devnull.onenote.com	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messaging.action.office.com/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://ncus.pagecontentsync.	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://messaging.office.com/	95309DC2-B687-4A1D-B357-9791BF084621.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	95309DC2-B687-4A1D-B357-9791BF084621.0.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:	682695
Start date and time:	2022-08-11 20:57:50 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bergo.document.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:	21
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@1/12@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, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.76.141, 52.109.76.35, 52.109.76.33, 52.109.88.39
- 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, licensing.mp.microsoft.com, 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\95309DC2-B687-4A1D-B357-9791BF084621

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):	5.358166691498604
Encrypted:	false
SSDEEP:	1536:GcQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:Z1Q9DQe+zuXYr
MD5:	E03E33AF89F97DC5B25DDD82F5850D04
SHA1:	B893DA24D9796D1E0F4FEDA83CC217C4D5B8199F
SHA-256:	E4492B3860EFFB5E622595DACA757C8AF0391BB2474DFB1A98E74639CB9E232D
SHA-512:	41E8C8D655E5F1791DDD48652EAC3520F097D196A3D9297A56B5C1F19A0FFE57D3C75F1A40A715EE80CDEB70D4E631EAC3D375D3665A263D654C6CC18790FF1
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="2022-08-11T18:58:53">.. 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\1AA1F65.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):	256277
Entropy (8bit):	7.980105068490826
Encrypted:	false
SSDEEP:	6144:Iqua1wNXfdpQfqpdHWbjGadcQ4Lv8zhP9BXWZ:ZuaizWqpd0HdkyVBXu
MD5:	CF4AB970C74E474774B60BF03CFDC3CE
SHA1:	2E78C30BF4B9D673EEECED99009F69FE8F525A06
SHA-256:	716D8319B106C690F8CD67E5611792FA7E7999FF0270CFE366DA3A02F815BE19
SHA-512:	1B7278E6ED4E548EA43B79483EDCEEA550AC0A73EC072577480AA07687CBA873BEBB1648303468323A24CEC8AE5C35ABC9F7B6C1440AFFE2E6A0660B57F10F91
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!...!.....IDATx^....Eu..=..L.&..y..$...h.....,.Dz.q..2F.4.....- .A..h...$..I...7..g..~.....u.N.u.O;..AuU.:uj.....9l.....0..6..rm..O:....J..^.Y.Z..lCK.~.x...C.....[...6.. .e... ...gZ..m.....;H..dez...|.s...E.i...m.6/.E.i-.Wn[f...N....z..Z^.i.|5....e...+{...L...+.0i.....C...5.HZ...w"y.....3..TT..g,..... ./..o..m..z40K~.<..Kk.5.z..m:..q.4.i5.TZ.....6-.%f..m..=...L.<....!.[..1..D...x....*2....p....*oE.{.E..}...p.....p}&mZ..e.@.k.5...9..W..'j...-o...M...I..".oy*...o...{>..V...+....#.z.DOH..K.<.o.&h.U.6-..U....WW.Syzh...+-...i.H..IO$-y@..6.~K.....h.U...J...jZK...%2-.[..mz.....2\...z<.Pe..5..!<...7tP.=zMO.....g.....5=...D.'.hm.Z.D..{..Z.....A/-i5.....hyZ$-....g..S.T.....".P.*j|...L.....OZ.3..8...<-f...*.. .-O..g.....g.f..\.P...e.>+=.6....|...%...%=.Z.V.hy2.....3.l.....=.D.'...M..'.*.P. .....@.W..=.=...|.c.^.:.2-].....A.3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\723487F4.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.$..\...@0....I.ZqB.+?_...fR}....%.\.....Y,.\|A..r..Z..B~8..t.P.~.Cc[p.D.W.INn...f....5....c.If.V....Oh$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{366CD27B-2A62-41B6-93DB-1F7B697094DD}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.123533094102747
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82lSkwkvrl3vlVvlHllgvlwZZZ/vlk:4LG1ND9Pxn824krbzCD
MD5:	2C60317F4137C93B1BBBF0B29D73E874
SHA1:	0D4C57CFFF33DABE22C395315DAB436A64AEBD43
SHA-256:	DB44CD349A5CA5942CF678E03EB69D4F65CF3AAFA29F087DB9761F174CCEDBB9
SHA-512:	911B78500883894F7DA6FA4979DEE509A51107B0D8E538EE1E759FF4910EDF31C55E972BA43E50528DA6507065122EC7995156AE1DE5CDABB1E71B60848BDCE5
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\Microsoft\Windows\INetCache\Content.Word\~WRS{62B53BDA-0627-4E63-9488-8A3BDB0E682E}.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\Temp\~DF7E69D731491A197F.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):	4.470554556820957
Encrypted:	false
SSDEEP:	384:YMF8VwyzFWNgoYUS2ru2ZXNe2+Oqy2fQPk4fZonyByKE9r7D6AblN25wYkpet0db:YuDyzcnPHUXtmsptc0zo5W2QP
MD5:	342C3838A5E66097A21DF18DCC6A9B9F
SHA1:	C827094599144193 57C2EB8E0B3F5F0F0B3903A7
SHA-256:	6694349AF68E7894C10E3842098B52188DE8299FA7B30633851C3B25DA070FBB
SHA-512:	7204F8D9A95CA52BA7D7C65BAF4C5E074876AD9FB6CFE0564603CCCCC57D39EAAE515379367BB28ADE4E3F7493425339BEA846D9D0D4A9C2EF8D22CE2F03F833
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\bergo.document.08.11.2022.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 15:28:51 2022, mtime=Fri Aug 12 02:58:55 2022, atime=Fri Aug 12 02:58:49 2022, length=2221899, window=hide
Category:	dropped
Size (bytes):	1135
Entropy (8bit):	4.694746211785935
Encrypted:	false
SSDEEP:	12:8VOU5fc6CHivEZuWcGX+Dr+W4Lc1wjGjA+/yQ9LRmEIDyvzJ+J04t2Y+xIBjKZm:8lSZuWRAv1JA+KQ9lcDyv97aB6m
MD5:	DE8ECDD6894F3A72FC2BA53710C7F56B
SHA1:	E9A56536053DE521D7C2BCB03D6471A532C2B96B
SHA-256:	A29E5FBD4E2090439476ABE0E1742015C74281E1677F3C70D4247796FAB7E587
SHA-512:	01754942F706126EA0373D4F0D9F35430F9C6F9E7046FF140AD79A6BD2D3FB3A059FD10C89084E7876210F350A188630EE831C1F6A183E5CABAD5BCA16317FEE
Malicious:	false
Preview:	L.....F.... .....i..3..:~.....K.!.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...UR.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....T.1.....hT....user..>.....NM..UR.....S.....x6.a.l.f.o.n.s.....~.1.....hT....Desktop.h.....NM..UR.....Y.....>.....L. .D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....2.K.!..UY. .BERGOD~1.DOC..l.....hT...UY.....e[.b.e.r.g.o...d.o.c.u.m.e.n.t...0.8...1.1...2.0.2.2...d.o.c.....d.....-.....c.....>.S.....C :\Users\user\Desktop\bergo.document.08.11.2022.doc..4.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.b.e.r.g.o...d.o.c.u.m.e.n.t...0.8...1.1...2.0.2.2...d.o.c.....:..,LB.)...Aw..`..... .X.....103386.....!a..%.H.VZAj.....s.....W...!a..%.H.VZAj.....s.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.

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):	101
Entropy (8bit):	4.642026852171083
Encrypted:	false
SSDEEP:	3:bDuMJlfyF8oALRlj9omX1xQ8oALRlj9ov:bCUyFtALr9itALr9y
MD5:	B2F218041B0F211C03F9CDAD574B84F9
SHA1:	24EAA43E1E915A6459650FBC65DCE94339079CC1
SHA-256:	EB84EE53E0ABF646203578F381883080960072CFE3F0462A3FBD7BB7EE36D66B
SHA-512:	1C8B4DF8649F493B35FD4B8EE262FBB28904B43F6F20A081E59110EDF2CA0C34E72770B874D91487FD92A7495A241AACB838924C337D449329842BA6F5DF22A3
Malicious:	false
Preview:	[folders]..Templates.LNK=0..bergo.document.08.11.2022.LNK=0..[doc]..bergo.document.08.11.2022.LNK=0..

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.1126747774478654
Encrypted:	false
SSDEEP:	3:Rl/ZdUx3lklTa9hnsH2xZ+xXlqSdEST:RtZ2Vk8DPZ2YFW
MD5:	1849C6ECEEDC70C326156A171E48044E
SHA1:	1F6EAB5EC51C725D3D21CE7576F730ADC5A92C22
SHA-256:	072BC80C9B39571A09BE4EC421CDE2914046D553008DEF5F23FDFD5E69ABC222
SHA-512:	1EBBF1F1B80441BD94A7A8B3055F0E731C18F8EC25E39CB2D8FADCDE8CCD08139E7CA5E3211706E623C5EF181D9D6ADEAF80BB35C2846E41290972FE70D62 07
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....`.E.....^Ij@.HjT.Hj`.HjDBIjZRIjI.Y.....T.....6C..8.j.h.].....$...

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	20

Entropy (8bit):	2.8954618442383215
Encrypted:	false
SSDEEP:	3:QVNliGn:Q9rn
MD5:	C4F79900719F08A6F11287E3C7991493
SHA1:	754325A769BE6ECCC664002CD8F6BDB0D0B8CA4D
SHA-256:	625CA96CCA65A363CC76429804FF47520B103D2044BA559B11EB02AB7B4D79A8
SHA-512:	0F3C498BC7680B4C9167F790CC0BE6C889354AF703ABF0547F87B78FEB0BAA9F5220691DF511192B36AD9F3F69E547E6D382833E6BC25CDB4CD2191920970C5
Malicious:	false
Preview:	..p.r.a.t.e.s.h.....

C:\Users\user\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\~$rgo.document.08.11.2022.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.1126747774478654
Encrypted:	false
SSDEEP:	3:Rl/ZdUx3lklTa9hnsH2xZ+xXlqSdEST:RtZ2Vk8DPZ2YFW
MD5:	1849C6ECEEDC70C326156A171E48044E
SHA1:	1F6EAB5EC51C725D3D21CE7576F730ADC5A92C22
SHA-256:	072BC80C9B39571A09BE4EC421CDE2914046D553008DEF5F23FDFD5E69ABC222
SHA-512:	1EBBF1F1B80441BD94A7A8B3055F0E731C18F8EC25E39CB2D8FADCDE8CCD08139E7CA5E3211706E623C5EF181D9D6ADEAF80BB35C2846E41290972FE70D6207
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....`.E.....^Ij@.HjT.Hj`.HjDBIjZRIjI.Y.....T.....6C..8.j.h.].....$...

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.99348706678991
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:	bergo.document.08.11.2022.doc
File size:	2316883
MD5:	228c063e5ce747dd51ffbbdf31dcc1f9
SHA1:	e13b37423003ebf1aacc898435607dc471ae0bd6
SHA256:	025d824f7fd062715efe4914065eb6026a0f1720256f03e18c652978ec9d6844
SHA512:	0f6c3c0f467c1d6f6b8915fd93a9034ea87bddc4b95225c444cd48f2f735f2e09b379febf2951b7ce76ceee9f61191f61bcf6c299d28f974825e6e425ee2159a
SSDEEP:	49152:FNbf0FGXHT9mAt0LoXOx1dPtHdSBEPd2rB9:F5f0F2HECAndXKEM
TLSH:	CCB533BF0CC46EF4D6A7C931261C30AE5C9361925D0E5B6EF1F1DB0AD668C8D0DA198B

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/682695/sample/bergo.document.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: 2868

General

Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2868
Data ASCII:	. . 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 l . . . . . A s L o n r g . 0 , ...) . .
Data Raw:	01 87 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: 357

General

Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	357
Entropy:	5.292924656590583
Base64 Encoded:	True
Data ASCII:	I D = " { 0 D A 1 E 0 6 5 - B 0 B 9 - 4 5 A 3 - A 4 8 7 - E 3 C 9 8 D D C 0 1 8 2 } " . . 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 = " 1 8 1 A F A F 8 F E F 8 F E F 8 F E F 8 F E " . . D P B = " 3 0 3 2 D 2 1 5 D 3 1 5 D 3 1 5 " . . G C = " 4 8 4 A A A 2 D A B 2 D A B D 2 " . . . . [H o s t E x t e n d e r I n f o] . . & H 0 0 0 0 0 0
Data Raw:	49 44 3d 22 7b 30 44 41 31 45 30 36 35 2d 42 30 42 39 2d 34 35 41 33 2d 41 34 38 37 2d 45 33 43 39 38 44 44 43 30 31 38 32 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
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: 5108	
General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	5108
Entropy:	1.923404837779589
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . P . . . . . " . . . . . q . . . . . A . . . . . ` . . . . . ` i . . . . .
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 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 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:	2.6997184068499265
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . P . . . . . p . . . . . ! . . . . . ` . ! . . . . . , . . p . . . . . A . . . . . q . . . . . ` . . . . . 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 ff 00 00 00 00 78 00 00 00 08 00 50 00 c1 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 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:	6.316355165237147
Base64 Encoded:	True
Data ASCII:	. . . . . 0 . . . . . H . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . Z 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 f8 5a 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 20:58:59.697133064 CEST	49765	80	192.168.2.5	45.8.146.139
Aug 11, 2022 20:59:02.840079069 CEST	49765	80	192.168.2.5	45.8.146.139
Aug 11, 2022 20:59:08.840548038 CEST	49765	80	192.168.2.5	45.8.146.139

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 5512, Parent PID: 812

General

Target ID:	0
Start time:	20:58:50
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:	0x930000
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\tstEFB5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	66412F42	unknown
C:\Users\user\AppData\Local\Temp\tstEFB6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	66412F42	unknown
C:\Users\user\AppData\Local\Temp\tstEFE6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	66412F42	unknown
C:\Users\user\AppData\Local\Temp\tstEFE7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	66412F42	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	6628977C	unknown
C:\Users\user\AppData\Local\Temp\yB1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F246AB	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	13F26626	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	13F26626	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	13F26626	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	13F26626	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	13F26626	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	13F26626	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	13F26626	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	13F26626	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	13F26626	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	13F26626	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	13F26626	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	13F26626	URLDownloadToFileA
C:\Users\user\AppData\Roaming\Microsoft\Proof	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6618765D	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6618765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6618765D	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\723487F4.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	661B5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1AA1F65.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	661B5805	unknown
C:\Users\user\AppData\Local\Temp\~DF7E69D731491A197F.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	661B5805	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstEFB5.tmp	success or wait	1	66412F42	unknown
C:\Users\user\AppData\Local\Temp\tstEFB6.tmp	success or wait	1	66412F42	unknown
C:\Users\user\AppData\Local\Temp\tstEFE6.tmp	success or wait	1	66412F42	unknown
C:\Users\user\AppData\Local\Temp\tstEFE7.tmp	success or wait	1	66412F42	unknown
C:\Users\user\AppData\Local\Temp\yB1.tmp	success or wait	1	13F24702	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DF7E69D731491A197F.TMP	success or wait	1	661B5805	unknown
C:\Users\user\Desktop\~$rgo.document.08.11.2022.doc	success or wait	1	661B5805	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	0	2	fd fd		success or wait	1	6618765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	0	2	fd fd		success or wait	1	6618765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	2	14	70 00 72 00 61 00 74 00 65 00 73 00 68 00	pratesh	success or wait	1	6618765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	16	4	0d 00 0a 00		success or wait	1	6618765D	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\723487F4.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 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	661B5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1AA1F65.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 26 45 75 fd fd 3d fd fd 4c fd 26 fd fd 79 d9 fd 24 02 fd fd 68 38 fd fd fd 2c fd 44 7a 03 71 fd 11 32 46 62 34 fd fd fd 02 fd fd fd 1b 0d 2d 20 fd 41 05 86 68 fd fd fd 24 1a 0d 49 0c fd 10 37 fd fd 67 fd 5d 7e fd fd fd fd fd 75 1e 4e 17 75 fd 4f 3b fd fd 41 75 55 fd 3a 75 6a fd fd a9 fd fd fd fd 39 6c fd fd 06 1f fd 30 20 fd fd 36 fd fd 72 6d fd fd 4f 3a fd fd fd fd 4a fd fd 5e 8a 59 fd 5a 06 fd 6c 43 4b fd 7e fd 78 fd fd fd 43	PNGIHDR7sRGBgAMAapHYs!!IDATx^Eu=L&y$h,Dzq2F4-Ah$I7g~uNuO;AuU:uj9l06rmO:J^YZlCK~xC	success or wait	4	661B5805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\bergo.document.08.11.2022.doc	unknown	14	success or wait	2	66412FF3	unknown
C:\Users\user\Desktop\bergo.document.08.11.2022.doc	unknown	4	success or wait	16	6641253D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	end of file	1	6618765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	6618765D	unknown
C:\Users\user\Desktop\bergo.document.08.11.2022.doc	1872093	184	success or wait	2	661B5805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	661C8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	661C8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	661C8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools	success or wait	1	6618765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\1.0	success or wait	1	6618765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom Dictionaries	success or wait	1	6618765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	661B5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	661B5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\3DBBC	success or wait	1	661B5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	661B5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	661B5805	unknown

Key Value Created

Key Path	Name	Type	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	1426784257	success or wait	1	6618765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C0000000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784257	success or wait	1	6618765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom Dictionaries	1	unicode	CUSTOM.DIC	success or wait	1	6618765D	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom Dictionaries	UpdateComplete	dword	1	success or wait	1	6618765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	661B5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\3DBBC	3DBBC	binary	04 00 00 00 88 15 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 9E A2 52 FA FF AD D8 01 BC DB 03 00 BC DB 03 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	661B5805	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 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	661B5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2022-08-11T20:59	success or wait	1	661B5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	661B5805	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\00006109F1009040000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358626817	1426784258	success or wait	1	6618765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784257	1426784258	success or wait	1	6618765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784258	1426784259	success or wait	1	6618765D	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\00006109F1009040000000 0000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784258	1426784259	success or wait	1	6618765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F1009040000000 0000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784259	1426784260	success or wait	1	6618765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C0000000 0000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784257	1426784258	success or wait	1	6618765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C0000000 0000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784258	1426784259	success or wait	1	6618765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\3DBBC	3DBBC	binary	04 00 00 00 88 15 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 9E A2 52 FA FF AD D8 01 BC DB 03 00 BC DB 03 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	04 00 00 00 88 15 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 BC DB 03 00 BC DB 03 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 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	success or wait	1	661B5805	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 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 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 FF FF FF FF 00 00 00 00 00 00 00 00				

Disassembly

⊘ **No disassembly**