ID: 682651
Sample Name:
ballfin,file,08.11.22.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:01:48
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

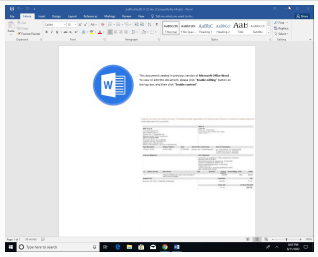
Windows Analysis Report

ballfin,file,08.11.22.doc

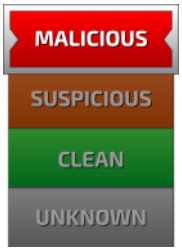
Overview

General Information

Sample Name:	ballfin,file,08.11.22.doc
Analysis ID:	682651
MD5:	75d17f46accbe9…
SHA1:	6ae88b35e85f6fb.
SHA256:	4f479dc5b981aa..
Tags:	doc IcedID
Infos:	



Detection

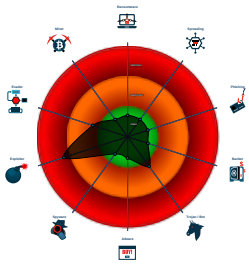


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 5268 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

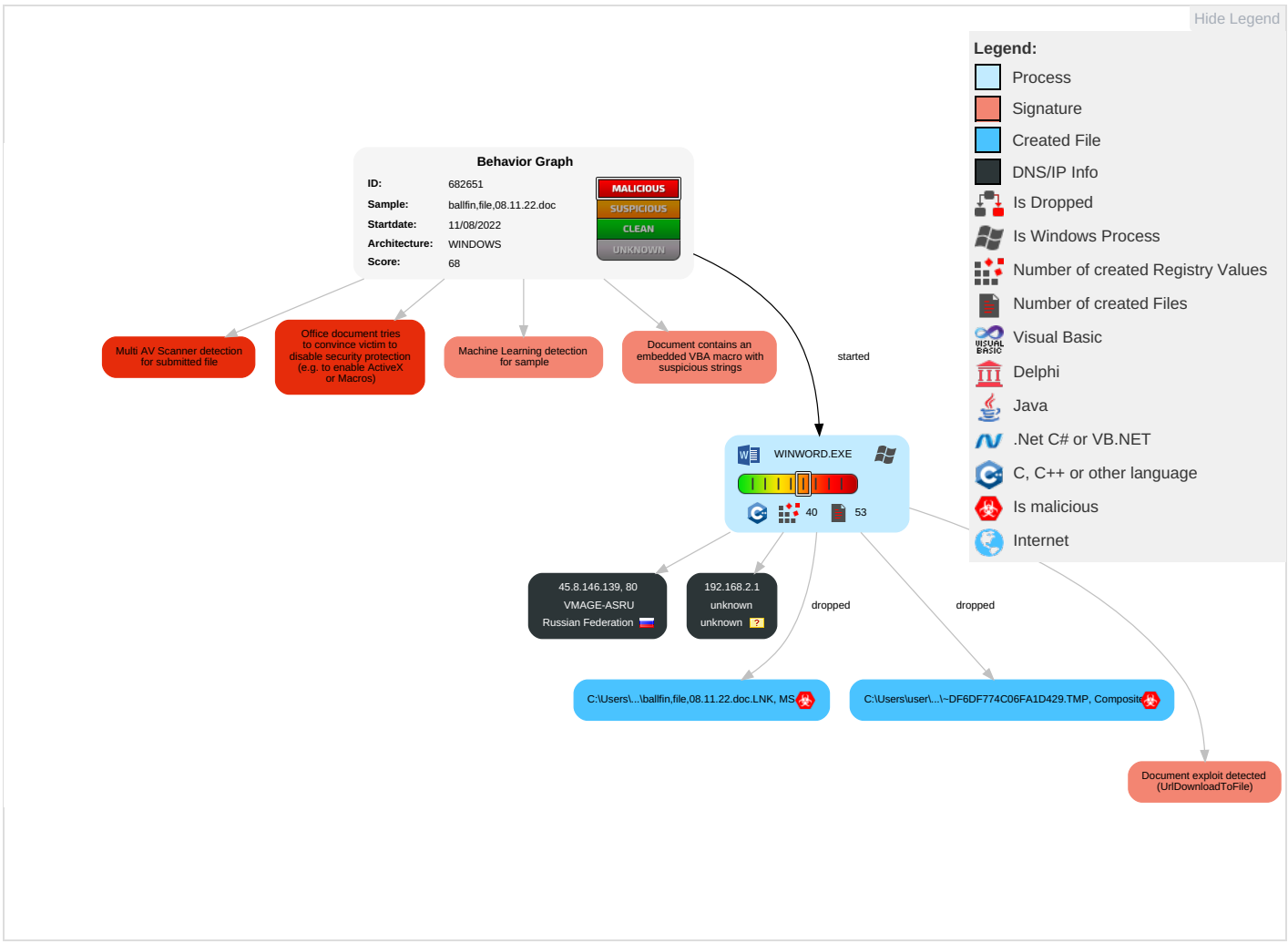
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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

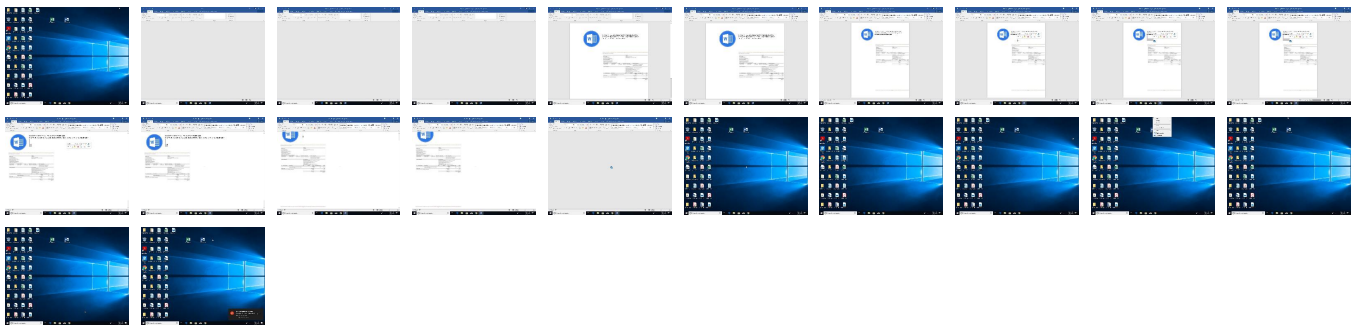
Behavior Graph

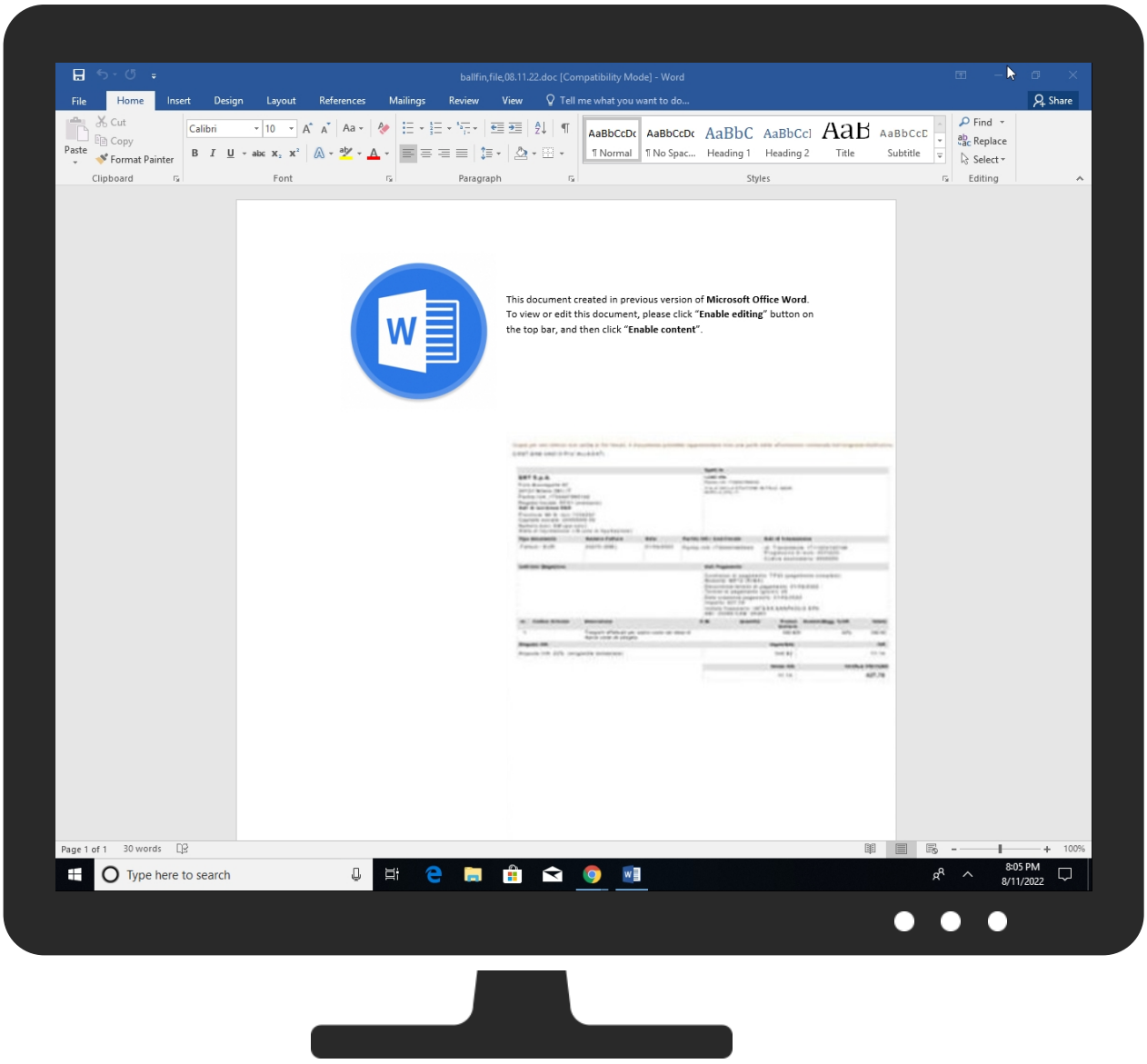


Screenshots

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
ballfin,file,08.11.22.doc	23%	Virustotal		Browse
ballfin,file,08.11.22.doc	16%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
ballfin,file,08.11.22.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF6DF774C06FA1D429.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

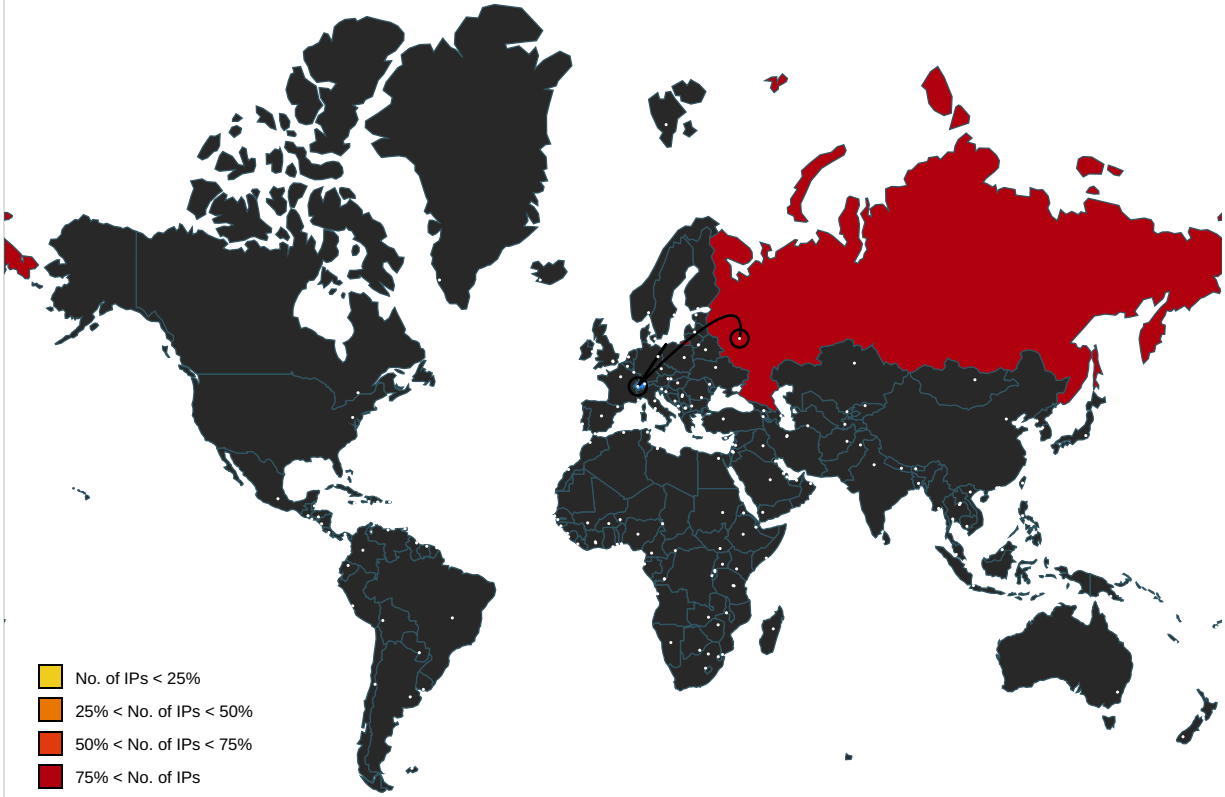
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://login.microsoftonline.com/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://shell.suite.office.com:1443	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://autodiscover-s.outlook.com/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://roaming.edog.	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://cdn.entity.	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://powerlift.acompli.net	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://cortana.ai	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://api.aadrm.com/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://api.microsoftstream.com/api/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://cr.office.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://graph.ppe.windows.net	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://my.microsoftpersonalcontent.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://messaging.engagement.office.com/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://web.microsoftstream.com/video/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://dataservice.o365filtering.com/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://ncus.contentsync.	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://weather.service.msn.com/data.aspx	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://apis.live.net/v5.0/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://messaging.lifecycle.office.com/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://management.azure.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://outlook.office365.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://wus2.contentsync.	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://api.office.net	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://entitlement.diagnostics.office.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://outlook.office.com/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://outlook.office365.com/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://webshell.suite.office.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://management.azure.com/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://devnull.onenote.com	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messaging.action.office.com/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://ncus.pagecontentsync.	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://messaging.office.com/	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E800CA17-2BDC-4C6B-AA67-6F2CC214AA5A.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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682651
Start date and time:	2022-08-11 20:01:48 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ballfin,file,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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.expl.winDOC@1/11@0/2
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, 52.109.88.191, 52.109.88.37, 52.109.88.38
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\E800CA17-2BDC-4C6B-AA67-6F2C C214AA5A

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):	5.358137913208185
Encrypted:	false
SSDEEP:	1536:PcQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:O1Q9DQe+zuXYr
MD5:	FF4B0DAD22556BB9B5AB982AE5B061DE
SHA1:	001ECC298FB9737DA50640081D6E6996D401CE47
SHA-256:	1BBEF9D214131D32B4B69665C2D19E524F42B06DDD1EEC7C3422C096C5C6E25C
SHA-512:	9C09A35CA8F82F3B69874363AA22104889D7CF8A183668DC17F27FBF5444A198D2EC7396E5225E9596E4A4CABBBFCC1873B2EDC7C5D6F77CC7B88BCBEB0CF CF
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="2022-08-11T18:04:22">.. Build: 16.0.15607.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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\856807D8.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:	58994BDC81FF937B05B307C161F852383DAA8504EA17522CD96CDE6EBF99E4992BA64DBEA532424AC16FBD8273999295DBBB74E48A77AAB2122C5701633DC7A 3
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.^|.....|.....I`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\FD8075F9.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):	256382
Entropy (8bit):	7.980585954508351
Encrypted:	false
SSDEEP:	6144:mCEm3Vq8LdNmYXjyTmRwYbWgGBtvnYA96+jNztlbEgM:pEmlvWwy2xbiBmb+Zztlbg
MD5:	7C4404A9A30A9E0DBC736DADB560C774

SHA1:	34122AE87D3DA63C05DB71E043BE6E5641D8F4ED
SHA-256:	964ADAD2626BEAE97F471D03E04D03D51C03551E69C803CDE0752478EE37EDC4
SHA-512:	176AAA14ABAA29353A3F5CD1EF8BE6725B60FF363A2F24619617D7BE13B4DBC4ACF74DE3559711068219BA3011DF265237EF64C58F79E6789C64C6454BBA1CA A
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!...!.....IDATx^.....Eu..u.O&.$..}g>..I..Q1.h...Kb.Jo..D.D....M[q...Wh...*.q.!:..D..C.Q.#.,...;.....w.s9]..... .S.N.SuNU=...}...B..F...A.t.....,Z.m.....j.B....=qI...m>..3....a.....ce..YU}.`..Hz...o.@.Z<..._a.?...U...t.Ihyz...{.....,y.....<.....R|..O<.'iU...BK..kh.\.}P..i.5.d.....Cx...,3V....4.' /...d>.Z6e'.c...B....TYm....m...b. .=.LU..^yk>.....v..K..-O.#.z..@...i.Pa.....ph.*...p-T\K..jH..1H..gHhqm.....'Tz..*.....o.R.u.rf.....6.....K}H.....B.W:qmSB..*.t...N...1.1\|.m.2.*>! q._*...z.@M'.|K...s....L/.....4q.s.JL8.a.1\../.m.B..E.t.ii..o.P....I\B.K|..m'W..M....p..N.....[\...2.A..5...O\.V.-..._.3.t..2...|...@..m..J..3.0... c...'..2.....Z|.....3.....^..1.'....I..-.....7.V. ..K'.xj....t.@..m~...K.!_q-..h..Kh.&..Y....g.M.q.....-.....'..5..1....Z|...Oh..!.....T.L.....\....A....m...p=|..^...Vn....[.....2$.|...p.=|..1\./5^*..+=a..B..t.W..oqm;*=...'m..3.->e.x.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{134F09C7-3DAB-4618-911F-C15286BF82DA}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.1316685601583454
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82l0kwkvEz6l6pO3lb3lHll83lwZZ08/vlk:4LG1ND9Pxn82GkotpO1rqP5
MD5:	C24B69D1C5A5F5ACA66FB51A33AB5DF5
SHA1:	80EC61BF4DB7EA7E426E7CBA909A00991F411709
SHA-256:	8FECDA67A00B81A9AD0E9EF33408E33C02E66CE5E401552258F5EEC2139E4333
SHA-512:	901B0FB29D6F67B585CC7242F8424C84390A6FC87F7FA9BDDCF6B6FB58DC8BB1714B81A24CF00BB4CEA362ABCC744364B179E93F2B92431615828A4AD374665 9
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{EB0BA440-0E83-4F25-A0A6-6F8E4E68B6EE}.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\Temp\~DF6DF774C06FA1D429.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):	4.4320002925704225
Encrypted:	false
SSDEEP:	768:03WGJMlamI4Y6um5kgJl8HLP4CYzxMb3998h5WmXjm:21JMlamIiAP8Mb3n8h5WmXj
MD5:	C3739E595DC7BCF7D1CE574F30061EAB
SHA1:	2DEC35E8EA72D190E70B5745F75EB3FFADC96488

SHA-256:	794A9ECCF1520193E2E0342EFBAADC5C0EF084647CD60786EFC8E420982F32E9
SHA-512:	696B03E2CFAE9ADF4D731C5458498022C69461E12A67F8FFD9053CFE2E1EA8C39669594A6D2F68671BAC1E1292371C5C039EABA9C4E47271BFE8D01C63F6C24 7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
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\ballfin,file,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 15:31:49 2022, mtime=Fri Aug 12 02:04:24 2022, atime=Fri Aug 12 02:04:18 2022, length=2203323, window=hide
Category:	dropped
Size (bytes):	1110
Entropy (8bit):	4.716196721152369
Encrypted:	false
SSDEEP:	24:8nZwjopPWslcLcmIETyAPtUtDqy7aB6m:8WkpPWsu7HtPtUwjB6
MD5:	E8B69A71879269605C2332DE03D8C00F
SHA1:	8B23F8A6C9AC272657660FEB5B6381FA4DA43087
SHA-256:	77105B4AE8DAD775A0E1230D3EAED4EEBE1849A88A50F9025B59B6F76E5E07AF
SHA-512:	08A5835F769497379C8617DE5ED5EAE99289104AB1AE9B528516A4FD66231862732775646B7584A02619C4460FDBB259286F68FF260EA86F9E5F08488EE9B6FB
Malicious:	**true**
Preview:	L.....F.... .....3..F.1:....j.6.....!.....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.....]...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...!..U.. .BALLFI~1.DOC..d.....hT...U.....h.....b.a.l.l.f.i.n.,.f.i.l.e.,.0.8...1.1...2.2...d.o.c.....:.._.....-.....^.....>.S.....C:\Users\user\Desktop\ballfin,file ,08.11.22.doc..0.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.b.a.l.l.f.i.n.,.f.i.l.e.,.0.8...1.1...2.2...d.o.c.....:.,.LB.)...As...`.....X.....093954.....!a..%.H.VZAj...7.....-..!a..%.H. VZAj...7.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2

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):	4.686856508512727
Encrypted:	false
SSDEEP:	3:bDuMJlfgJobbBCmX1bbbBCv:bCUgJobbBNbbBs
MD5:	EDB8EF121D6546C78A3F28C32E5601DC
SHA1:	8ACD48E663847EB20244E22B46883FF11F56890A
SHA-256:	D9A74503B42E6A029AAE4755B7D382590A15C3DC531E43A9E6A1D68669EEB567
SHA-512:	CF520B9F811054860B12EDA93CB692156376C454F78AB371DC9C5FCC06DB8CBBFAD601E66877D8B30316DD3E9973CD2E4C5503452FF516ACF177AEFB675C8D A
Malicious:	false
Preview:	[folders]..Templates.LNK=0..ballfin,file,08.11.22.doc.LNK=0..[doc]..ballfin,file,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):	2.2688869265568865
Encrypted:	false
SSDEEP:	3:Rl/ZdB79h/5lFl37Dlszl/lBlqKI59pXf:RtZDhrl/3lsztcF9pP
MD5:	4AB2D73AC87761DA56077441185F525B
SHA1:	8F5571916CF9F63CDB4251B66B84DC80875B591E
SHA-256:	CB11187839DA41BFA1DC16978B19189ADD160B3A442CFACCBBC4A0A620CEBE53
SHA-512:	18F298E2E0278A7B6C3B5B041A1359E0A3CF405EA61BFAB6375F1BC84C0273E096B7102CFA8E22EF4B5889625487AC750B437761893FAFF46CD66A49C19DE6D
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....u.....x).....i.....H.....6C.....m.....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\~$llfin,file,08.11.22.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.2688869265568865
Encrypted:	false
SSDEEP:	3:Rl/ZdB79h/5lFl37DlszI/lBlqKI59pXf:RtZDhrl/3lsztcF9pP
MD5:	4AB2D73AC87761DA56077441185F525B
SHA1:	8F5571916CF9F63CDB4251B66B84DC80875B591E
SHA-256:	CB11187839DA41BFA1DC16978B19189ADD160B3A442CFACCBBC4A0A620CEBE53
SHA-512:	18F298E2E0278A7B6C3B5B041A1359E0A3CF405EA61BFAB6375F1BC84C0273E096B7102CFA8E22EF4B5889625487AC750B437761893FAFF46CD66A49C19DE6D
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....u.....x).....i.....H.....6C.....m.....H...

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.9931718162127225
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:	ballfin,file,08.11.22.doc
File size:	2298562
MD5:	75d17f46accbe980e1deb28dd7513085
SHA1:	6ae88b35e85f6fbb55584893f696f859dccfedc2
SHA256:	4f479dc5b981aadc01b1f245d8694b1ad043247f04148bbb78a86c8ed530b777
SHA512:	e9959f74b0c4cb34c1167eb622fbdd8ae8bbeb808ca8d6680bc82f22c9d0566b6dac30b1376837fd54a4b21bac7af414bccc90e849ec32b2f78564d98bf5674f
SSDEEP:	49152:NOUM0iO62qwcjsAGQnvISJw3zMtsqF+MhVo6H8LvdQ7yh4SbCu+o:gUmXIA+SJw3z++CcyM4yb
TLSH:	75B53393D127F54CDD4616AD638825F65FF10327189EE9AB03BA2606D38F1BF0C9958C
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.....hl.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/682651/sample/ballfin,file,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: 2769	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2769
Data ASCII:	...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.$CustomlizC.P.... .D.? PtrSa.fe Funct@ion .... Li.b "user3.2" Alias. "KillTi.mer" (By0Val ... A@s Long.., ..$'...
Data Raw:	01 d6 b4 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 44 6f 63 75 6d 65 6e 10 74 22 0d 0a 0a 8c 42 61 73 01 02 8c 31 4e 6f 72 6d 61 6c 02 2e 19 56 47 6c 6f 62 61 6c 21 01 aa 53 70 61 63 01 6c 46 61 08 6c 73 65 0c 4a 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72 75 0d 22 45 78 70 08 6f 73 65 14 1c 54

VBA Code

Streams	
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 369	
General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	369
Entropy:	5.253715637016501
Base64 Encoded:	True
Data ASCII:	ID="{F718A541-6FAD-499A-B2A3-854E068A76A8}"..Document=ThisDocument/&H00000000..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="FDFF151AEF13F313F313F313F3"..DPB="FAF8121D0E1E0E1E0E"..GC="F7F51F20E1E0DFE1DFE120"....[Host Extender Inf
Data Raw:	49 44 3d 22 7b 46 37 31 38 41 35 34 31 2d 36 46 41 44 2d 34 39 39 41 2d 42 32 41 33 2d 38 35 34 45 30 36 38 41 37 36 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
Data ASCII:	a . . .
Data Raw:	cc 61 ff ff 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 5116	
General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	5116
Entropy:	1.9292601170451005
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 00 11 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 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 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:	2.696829186323428
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . P . . . . . p . . . . . ! . . . . . ` . . . . . , . . p . . . . . a . . . . . Q . ` . . . . . \\ . . 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 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 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:	6.294817845464784
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 0e 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 20:04:29.819391012 CEST	49736	80	192.168.2.3	45.8.146.139
Aug 11, 2022 20:04:32.903865099 CEST	49736	80	192.168.2.3	45.8.146.139
Aug 11, 2022 20:04:38.904438019 CEST	49736	80	192.168.2.3	45.8.146.139

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 5268, Parent PID: 756

General

Target ID:	0
Start time:	20:04:19
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:	0x1240000
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\tstE366.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\tstE367.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\tstE396.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\tstE397.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\yF914.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	142F46AB	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	142F6626	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	142F6626	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	142F6626	URLDownloadToFileA

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	142F6626	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	142F6626	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	142F6626	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	142F6626	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	142F6626	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	142F6626	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	142F6626	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	142F6626	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	142F6626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\856807D8.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\FD8075F9.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\~DF6DF774C06FA1D429.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\tstE366.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstE367.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstE396.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstE397.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\yF914.tmp	success or wait	1	142F4702	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DF6DF774C06FA1D429.TMP	success or wait	1	65925805	unknown
C:\Users\user\Desktop\~$llfin,file,08.11.22.doc	success or wait	1	65925805	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\856807D8.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$a<>"=X11^|.|!|`Ec#T"	success or wait	1	65925805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FD8075F9.png	0	65536	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 fd 00 00 01 fd 08 06 00 00 00 37 fd fd 00 00 00 01 73 52 47 42 00 fd fd 1c fd 00 00 00 04 67 41 4d 41 00 00 fd fd 0b fd 61 05 00 00 00 09 70 48 59 73 00 00 21 fd 00 00 21 fd 01 04 fd fd fd 00 00 fd fd 49 44 41 54 78 5e fd fd 09 fd fd 45 75 fd 06 75 fd 4f 26 fd 24 fd fd 7d 67 3e fd fd 49 04 04 51 31 fd 68 fd fd fd 4b 62 fd 4a 6f fd fd 44 fd 44 fd fd 05 fd 4d 5b 71 03 11 fd 57 68 16 15 0c 2a fd 71 0b 21 3a fd fd 44 fd 06 43 fd 51 13 23 2e 2c fd fd fd 3b fd fd fd fd fd fd fd fd 77 fd 73 39 5d fd fd fd 07 fd fd fd 53 fd 4e fd 53 75 4e 55 3d fd 7f fd 7d 04 fd 1d 42 0f fd 46 fd 1f 08 41 fd 74 fd fd 03 fd fd 2c 5a fd 6d 00 fd 0e fd 03 6a fd 42 fd fd fd 18 3d 71 49 fd fd 0a 6d 3e fd fd	PNGIHDR7sRGBgAMAapHYs!!IDATx^E uuO&$}g>IQ1hKbJoDDM[qWh*q!:DCQ #.,;ws9]SNSuNU=}BFAt,ZmjB=qIm>	success or wait	4	65925805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ballfin,file,08.11.22.doc	unknown	14	success or wait	2	65B82FF3	unknown
C:\Users\user\Desktop\ballfin,file,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\ballfin,file,08.11.22.doc	1871618	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

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	65938A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	65938A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2D856	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\2D856	2D856	binary	04 00 00 00 94 14 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 A2 8E 54 5D F8 AD D8 01 56 D8 02 00 56 D8 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	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	File Path	unicode	C:\Users\user\AppData\Local\Temp\imgs.htm	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2022-08-11T20:05	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

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\00006109F100A0C00000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1358364678	1426784263	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100C040000000000F01FEC\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\00006109F100C040000000000F01FEC\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\00006109F100904000000000F01FEC\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\00006109F100904000000000F01FEC\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\2D856	2D856	binary	04 00 00 00 94 14 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 A2 8E 54 5D F8 AD D8 01 56 D8 02 00 56 D8 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	04 00 00 00 94 14 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 00 00 00 56 D8 02 00 56 D8 02 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 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 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				

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

Disassembly

No disassembly