ID: 682653
Sample Name:
airdynefile08.11.22.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:06:37
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

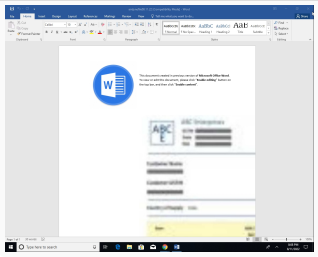
Windows Analysis Report

airdynefile08.11.22.doc

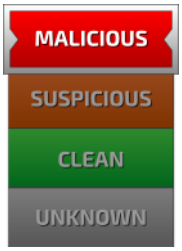
Overview

General Information

Sample Name:	airdynefile08.11.22.doc
Analysis ID:	682653
MD5:	9cbf5c3239d290…
SHA1:	e0fab1bc0137f94..
SHA256:	3c59aab375e8eb..
Tags:	doc IcedID
Infos:	



Detection

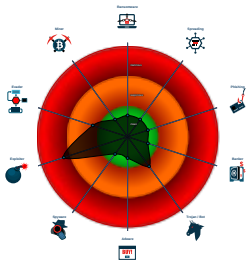


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 2508 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Software Vulnerabilities

Document exploit detected (UrlDownloadToFile)

System Summary

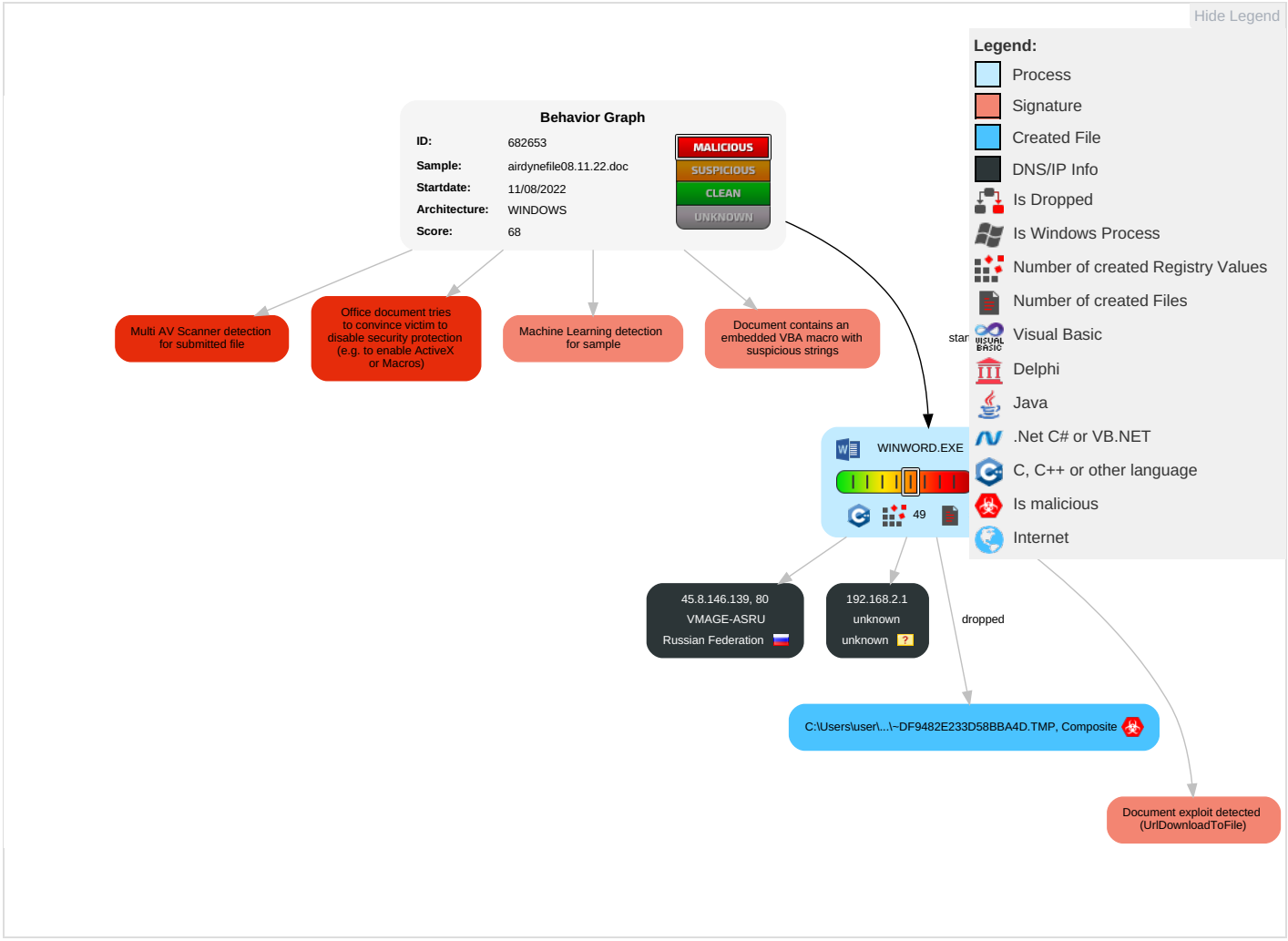
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains an embedded VBA macro with suspicious strings

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 Scripting	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 1 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 2 Scripting	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

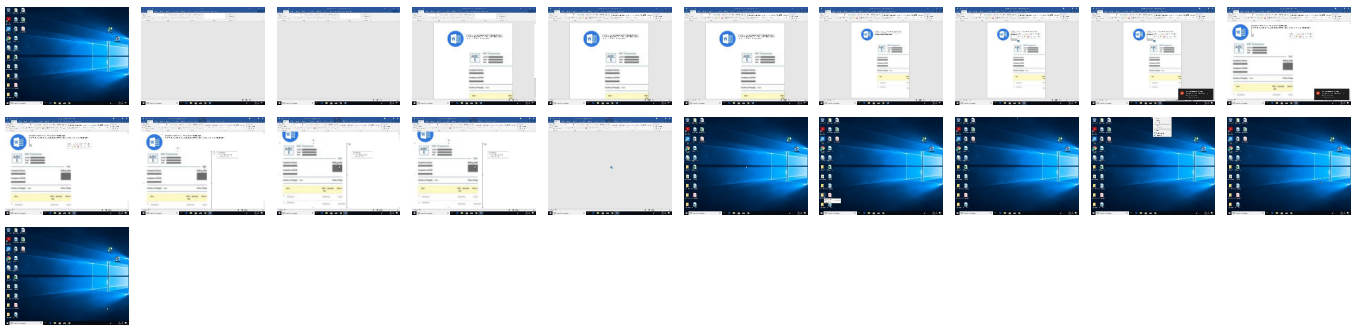
Behavior Graph

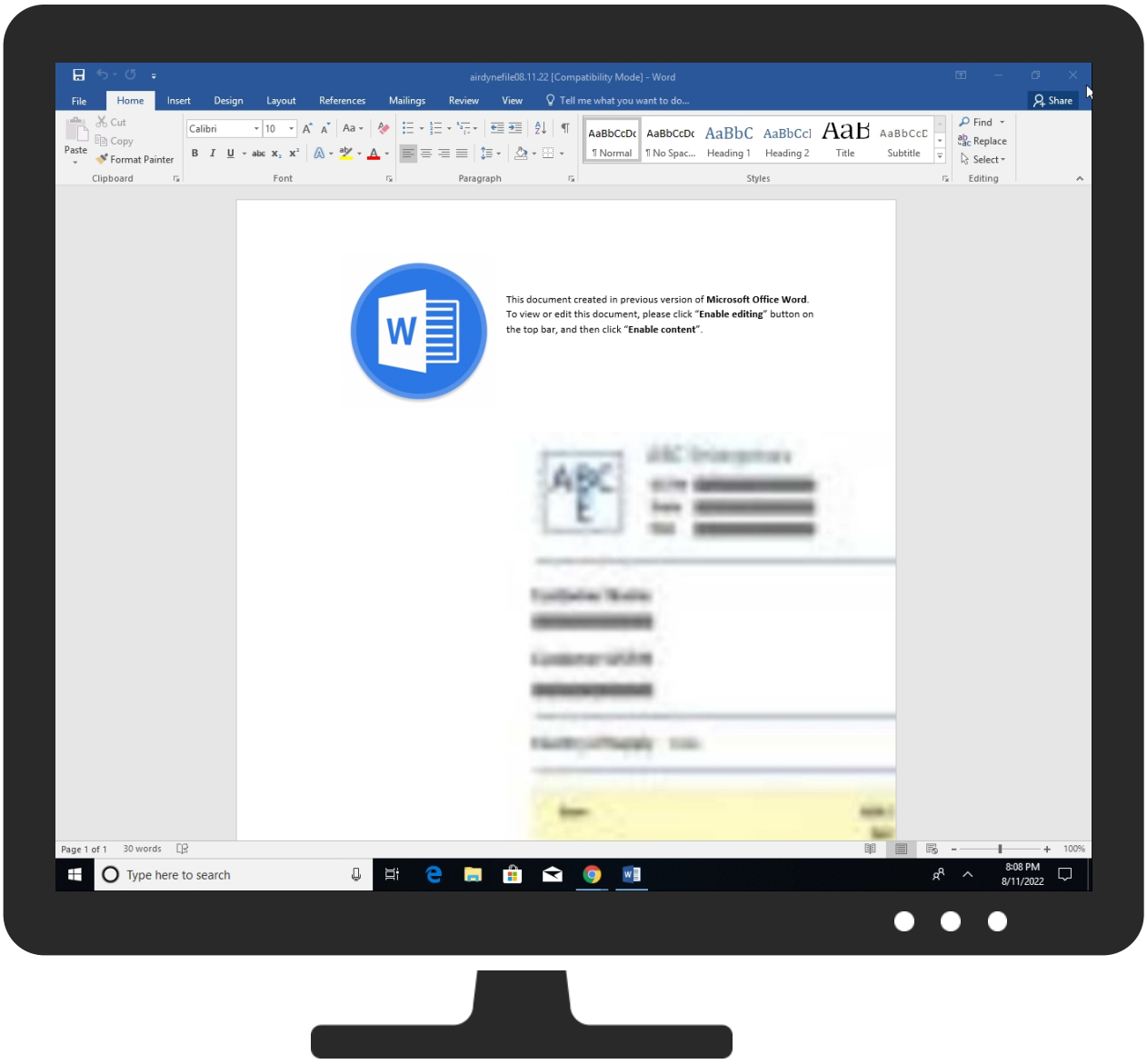


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
airdynefile08.11.22.doc	27%	Virustotal		Browse
airdynefile08.11.22.doc	15%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
airdynefile08.11.22.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF9482E233D58BBA4D.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

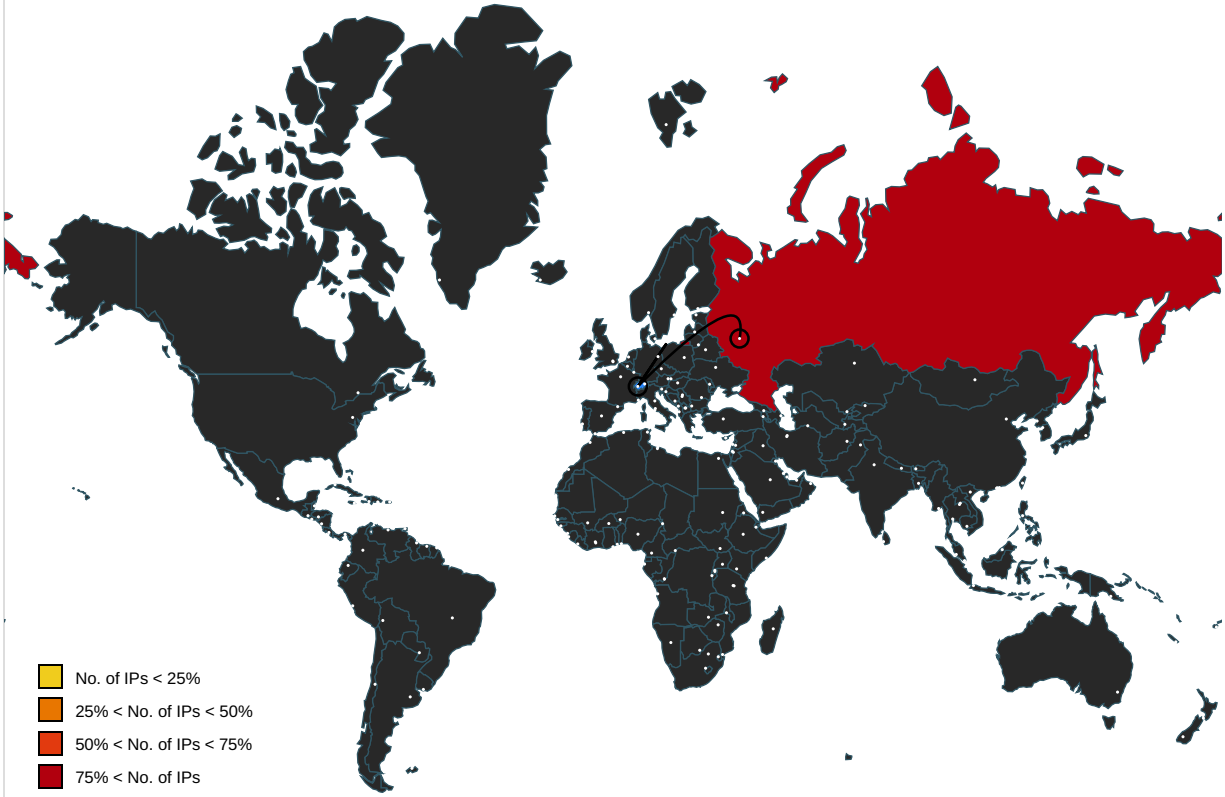
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://login.microsoftonline.com/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://shell.suite.office.com:1443	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://autodiscover-s.outlook.com/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://roaming.edog.	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://cdn.entity.	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://powerlift.acompli.net	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://cortana.ai	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://api.aadrm.com/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://api.microsoftstream.com/api/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://cr.office.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://graph.ppe.windows.net	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://my.microsoftpersonalcontent.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://messaging.engagement.office.com/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://web.microsoftstream.com/video/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://dataservice.o365filtering.com/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://ncus.contentsync.	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://weather.service.msn.com/data.aspx	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://apis.live.net/v5.0/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://messaging.lifecycle.office.com/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://management.azure.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://outlook.office365.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://wus2.contentsync.	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://api.office.net	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://entitlement.diagnostics.office.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://outlook.office.com/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://outlook.office365.com/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://webshell.suite.office.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://management.azure.com/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://devnull.onenote.com	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messaging.action.office.com/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://ncus.pagecontentsync.	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://messaging.office.com/	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	5BCCED0D-6489-4D58-8030-93DECA1D9495.0.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:	682653
Start date and time:	2022-08-11 20:06:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	airdynefile08.11.22.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:	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@0/2
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, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.32.24, 52.109.88.37, 52.109.88.38
- 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, tile-service.weather.microsoft.com, 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\5BCCED0D-6489-4D58-8030-93DE CA1D9495

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):	5.35816368801646
Encrypted:	false
SSDEEP:	1536:VcQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:01Q9DQe+zuXYr
MD5:	D5B4F12484FE8D4AB745F9103E07F8E9
SHA1:	60E132B6DFEAAC1DC0290943AF59A39CB66D075C
SHA-256:	6A095196A214FDC98FE432A5F0DE5491F65B9D5A56E5CE82B67D375FC052C337
SHA-512:	A84FD823A8F3DCA2C297426FBA48A094AAD4CCDA4194C3DDC8E4C313A834379744B3542562EF7E8B0D5244119C269EEA50BCD42E36FD951276C90A3CBEB35(8D
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="2022-08-11T18:07:47">.. 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\30A5DA22.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 636 x 613, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	113730
Entropy (8bit):	**7.990292786537194**
Encrypted:	**true**
SSDEEP:	3072:ShIiMUFV26oUc72Dl+oj/Yc6oGqdxVJw0c8N2mirB0VZp:ShMggmEceUi8N2miK/
MD5:	E0B30095BE35E9494E5073277D4FC1A1
SHA1:	19D39B036989A331F5389E377FBE565436599894
SHA-256:	EA952A68D25232D981CDBE0CD6DA947A9386D4BFFD5D1BE2EF80C4A1246AC3E2
SHA-512:	A524907D5D60AA77DB0BA3A3BF114EA7F8AEA9190ADAA84A0C78F96EC8E333AB124D68C84863E83E735D602117B0F3422746C9C4A0D6823CC8B51B652C4197 E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...|...e.....V.R.. .IDATx.....4.....~.:..t."...$.....d..+...%Y.,V.(...7...03""""..O.....?>..y.}.v.&u.....?0.....g.NH.....F...$..H.....km.%"D .=.f;.....A....O..w ..,"n...U....N~?".....'...7w)A..l.+.....7....q|..q.7?.....v.f...6....x._<.On.WLm..>s<.-....."....."_..~a....f=..7.....P.~...,gD..:.P...,*.....c...;.B...q..1.>|.....R.7m...7.....,".p7%. M."::...9..P.8.!..?.... .)".....A..Z..rA.).g.7..'QD.....@$.....*..oC. .6w...lP...lN..1X...H.....q....X{.s..A.....w..I....l`..t.C87.p.k...H>r...),.,..n...Dd.R.c..xHs.nWv.....>.j.WCi.. .....a...}.t\_....A.q..t..^A..Q..g.,..P.h.n.nm....7....YYT.....jl.....yR>s...w.....|.z..L.....\.FP.....QG...0.....2...@T.*....C.....M...;...i....Y8...R.Y*....~.;.CA.....q....6`.....~.....2.g."... ../..{x.(...o..p...YW&+//[.....].....h....s....&...m_.)tG...s....<...].R..w..!.....A;.....I.,\.I@...&.....0[.\a?..`.#2upVW.4.{..c.JMZ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\DAA79FBB.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):	255895
Entropy (8bit):	7.979759984902193
Encrypted:	false
SSDEEP:	6144:P5rAVWEVTBoN+zhOdTeH3/kldpFO23BgSD5rPnuV0UJc4:P5jkTB26Olev0T3v9jUJb
MD5:	9B32A04B89F73BF2C6DB5756158B35B5

SHA1:	3389E751C09D18696F2BCD1C54E8AA5931066760
SHA-256:	337CA9401C94826508B2E027E35C63D60B05821AEFF587388E6F11A2B12ADA0A
SHA-512:	A14901247DE770DCEDAB27DA14A05A9F11B588396C78E8405F2BDC6421B80F8CA1C5F61DA629F62B83489E63DF2BC74E11B36A49F05096FE60DD038A1E2DDDF
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!...!.....IDATx^....fEu.;...7.....7.V[L0&11dTo4...4.qLL4...b;!("..4...`4.....W..D.....>C...G..<...[{..E..4...P]Uk.Z5.]kU...>.(...W.K.z.z2IC.E.....cr.W.Yg.T9...-.g..u.h."eZ...W.....w.A..O.5..r.Un.Y.....V..4.NZ.....L.HT^.+.....\.+..e>..^. ....."e.m}cHyP.....o.$Zz..r...,?..[T~/]..{2-..m #.?...Uz...p.r...H~-SA..HS&..Z.D[.'.bE&.w.`/.Hzv...Z...5..\..I.vPk..l"i-/.=Z.\|....O.4.r.6.j..Y.. ...n.6.q. .....]?@:...;.T...m....:j.5]...\|.....'Z..g..Zw.z"....[...:ZT~+...0..V..oy.....O...1 .U...m..Kz.....L...8.2-=1...oeW.=..s.{t0F....M.!.y..j\.I.zf..2I....L.....h....%z..4q....-_eZ^..W^....m..d..3.b.....i...T.....k.R..J..V.o..+o,.....'....+.*.'...g...z-{Hz...j~.....mh1&.3.....D..}.. cPiU&.M...m...,.\|.e...B...B.g..@..PIo....s..1]..+.MW9Pi.x..m..U>...'z...oc...6..^H.4.....L.U....l{.....*z.*_..6.r..g.5]1...1:.....5.....c.{.I.!..J..D..^.1.d{:..)Se3.-?.,$.'{8<0.O....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{3C465CDC-CAEF-4249-848A-53A66E3988F8}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.1363686128594344
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82lkYkwkvLTlB9nlqnnlHlllnlwZZw/vlk:4LG1ND9Pxn82yYkNr2u
MD5:	0D05048999F4DFFFF86BF6035C83ACDC
SHA1:	61E16DFF058C675F17E6AF5799B086728953A419
SHA-256:	C654F1B18F50F559AB5B2AFB8CD9D6F450E06A6A9A7CDE63883255C7BA3B3936
SHA-512:	54E4957355BACDFDFA18440E6AE9EBF7013FA7B22EDED6483B629EEA836125F48158AB3B56235F1BBF8826FB13064E9FD3D5AE1E3D4756908B931E6E4C76FEA5
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{E918CB2E-5D62-4B18-96C2-226D6B9031C2}.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\~DF9482E233D58BBA4D.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	4.467449547221044
Encrypted:	false
SSDEEP:	768:uNH75HYm9Shja2qHTVg1ofDo2jA1gaPHjg:uNH7im9Yj7L1EWV
MD5:	930D49442E2C117351865C372FCF6786
SHA1:	380AAED68CDCE678AA00C2D3F2DEA18DA892E26D

SHA-256:	D82B3799870D02F90FDB229C30701C8AD0C1FAB9BD6A9D3A9919E37E0B9A8AB7
SHA-512:	08DAB42356F6A9D7714B2C111D376051F96B51845CE53FDC2240092B8D8CF0477502CC8AE845AC61952EDAD5044ABA4125EA94AC50D7FAC12C6CE83E78C622E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	.....>.....G.....&.....!..."..#...$...%.....'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8.....:...;...<...=...>.....@...A...B...C...D...E...F...9...^...I...J...K...O...M...N.....P...Q...Z...S...T...U...V...W...X...Y...L...[...\...]..._.....`...a...b.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\airdynefile08.11.22.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 15:28:57 2022, mtime=Fri Aug 12 02:07:50 2022, atime=Fri Aug 12 02:07:44 2022, length=2255369, window=hide
Category:	dropped
Size (bytes):	1105
Entropy (8bit):	4.718682500961763
Encrypted:	false
SSDEEP:	12:8yFkYEY0Uip6CHi3FTiDGXNDTl8+W2p/486hjAM/yhG4wfjLR4VxDywJp4t2Y+x4:8ZYt6EFTiqxTjZOAMKhSSDy27aB6m
MD5:	30C51846FA0F1A68A450B6203090733A
SHA1:	F512288DF48501D4AFF544CD48DF2505564C29E1
SHA-256:	0B0881800A32B472FAA2A95D9D119116A19A5EDC528F714D2577D665E7B057F2
SHA-512:	D821C44BC710EE63034076EA89C95D1C74A5A727B2DCA2A0CCFF2AE4AA6F987D704271755960A2DD85BF808843395D9E6B5564CE8AF21EF8146CCAB84DC7709
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....)..3...+.....E.....j".....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...U.....:.....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..U.....S.....%.a.l.f.o.n.s.....~.1.....hT....Desktop.h.....NM..U.....Y.....>.....5..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....|.2.j"..U.. .AIRDYN~1.DOC..`.....hT...U.....>g..a.i.r.d.y.n.e.f.i.l.e.0.8...1.1...2.2...d.o.c.....^.....-.....]..... .>.S.....C:\Users\user\Desktop\airdynefile08.11.22.doc.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.a.i.r.d.y.n.e.f.i.l.e.0.8...1.1...2.2...d.o.c.....:.,.LB.)...Aw...`.....X.....936905.....!a..%.H.VZAj.....s.....W...!a..%.H.VZAj.....s.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.

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):	89
Entropy (8bit):	4.66206935403088
Encrypted:	false
SSDEEP:	3:bDuMJlcMRXIwdRjbUmX1rIwdRjbUv:bC1wfjbwwfjb2
MD5:	768F6BDC43FCB0CE423AE169D54AB0FD
SHA1:	42B20BEA79CB7F30BA795B0F8D3DF6C7E76C54F2
SHA-256:	EA16E2892845962864B4F9AFB78244BC7180B5D322293359A682E8C5854E3615
SHA-512:	C738FA5E9CFE102852F658A960797D207B286246950941B71FB7F104263DE6C5B36A1B697450F43AEDDEB1F9CD204FBC78F4F17BF07555DF5DED1371DCA649AD
Malicious:	false
Preview:	[folders]..Templates.LNK=0..airdynefile08.11.22.LNK=0..[doc]..airdynefile08.11.22.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):	2.93777952317554
Encrypted:	false
SSDEEP:	3:Rl/Zds73xMXtNWTa9hnsH/xZlptl7:RtZMOPDQblpt5
MD5:	CB05A717E5BC31EF3523242FB57612D4
SHA1:	671D4C94ED08E906500B729A860245DA914DC373
SHA-256:	19198A1C210522CB73D44C6D6E85C87EA67699CB292ED655FD1A37F292A2C395
SHA-512:	95D3F5631AC9D5E2B025881612A1D02680225FFB9B143298477B373F1CF272A664BCFA37C64571FE4D1EC16A300CA22C5EEDB88923A142C721D6B415E831132C
Malicious:	false

Preview:	.pratesh.....p.r.a.t.e.s.h.....}... .....y.....^lj@.HjT.Hj`.HjDBIjZRIje.....$...

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\~$rdynefile08.11.22.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.93777952317554
Encrypted:	false
SSDEEP:	3:Rl/Zds73xMXtNWTa9hnsH/xZlptl7:RtZMOPDQblpt5
MD5:	CB05A717E5BC31EF3523242FB57612D4
SHA1:	671D4C94ED08E906500B729A860245DA914DC373
SHA-256:	19198A1C210522CB73D44C6D6E85C87EA67699CB292ED655FD1A37F292A2C395
SHA-512:	95D3F5631AC9D5E2B025881612A1D02680225FFB9B143298477B373F1CF272A664BCFA37C64571FE4D1EC16A300CA22C5EEDB88923A142C721D6B415E831132C
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....}... .....y.....^lj@.HjT.Hj`.HjDBIjZRIje.....$...

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993763586131025
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:	airdynefile08.11.22.doc

File size:	2349614
MD5:	9cbf5c3239d290b08ba1f0d8617b6802
SHA1:	e0fab1bc0137f946134c22f27bd9f1bb9484c785
SHA256:	3c59aab375e8ebf7a3da914e7f1f38c6c54947b4c27c73c5c591ab27152dfe4d
SHA512:	8042fb552648d95ef3fd785e0d3c2b9efdcdb62ec81012e6d3369e923425948cebed2fc9b4fd165170319f9253bf46156eccfe3822d6959d892dd44725e17b3c
SSDEEP:	49152:QSbTwbt983aPk2JHFeqvFOpJNWqsMxhAyjMuBBcRVOl/9wE:lMYkvs7bx0yQWBO45
TLSH:	5FB5330906A1A68F4D64F430376A5B187E612FFB17859F0AA3061D7DE1FDB637A0F0A4
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/682653/sample/airdynefile08.11.22.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: 2860

General

Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2860
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 8 . . . . . L . i b " k e r n . e l 3 2 " A l . i a s " V i r . t u a l P r o t . e c t " (B y V a l . . . . . A s L o n g . 8 ,
Data Raw:	01 ba b4 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 44 6f 63 75 6d 65 6e 10 74 22 0d 0a 0a 8c 42 61 73 01 02 8c 31 4e 6f 72 6d 61 6c 02 2e 19 56 47 6c 6f 62 61 6c 21 01 aa 53 70 61 63 01 6c 46 61 08 6c 73 65 0c 4a 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72 75 0d 22 45 78 70 08 6f 73 65 14 1c 54

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365

General

Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	365
Entropy:	5.268842495589465
Base64 Encoded:	True

General	
Data ASCII:	I D = " { 0 9 5 0 3 B 1 F - A 2 8 D - 4 6 8 B - 9 5 E 9 - C F 2 6 4 8 9 D F 7 A 5 } " . . 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 = " A C A E 5 E 0 C A 6 B C A A B C A A B C A A B C A A " . . D P B = " 5 8 5 A A A 4 D A B 4 D A B 4 D " . . G C = " 0 4 0 6 F 6 5 4 0 E 0 1 0 F 0 1 0 F F E " . . . . [H o s t E x t e n d e r I n f o] . .
Data Raw:	49 44 3d 22 7b 30 39 35 30 33 42 31 46 2d 41 32 38 44 2d 34 36 38 42 2d 39 35 45 39 2d 43 46 32 36 34 38 39 44 46 37 41 35 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:	1.9217258555644907
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . 8 . . . . P . . . . " . . . . q . . . . A . . . . ` . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . `) . . . .
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 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 38 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 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 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:	2.708973861727282
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . . ` . . . . . . . . . . . . . . p . . . . . . . . . . . . . . . . . A . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . Q . P . . . . . . . . . . . . . 0 . . p . . . . . . ! . . . . . . . . . . . q . . . . . . . . . . . . . . . . . . . . . ` . q . . . . \\ . . p . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 11 00 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 60 00 d1 08 00 00 00 00 00 00 00 00 00 00 00 00 00 04 70 10 00 fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 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:	6.288212539715818
Base64 Encoded:	True

General	
Data ASCII:	. . . . . 0 . . . . . H . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . S 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 06 53 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 20:07:55.576704025 CEST	49767	80	192.168.2.5	45.8.146.139
Aug 11, 2022 20:07:58.671518087 CEST	49767	80	192.168.2.5	45.8.146.139
Aug 11, 2022 20:08:04.672071934 CEST	49767	80	192.168.2.5	45.8.146.139

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2508, Parent PID: 812

General

Target ID:	0
Start time:	20:07:45
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:	0x1080000
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\tstBC9.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\tstBF8.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\tstBF9.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\tstBFA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	66412F42	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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\y211A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	151B46AB	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	151B6626	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	151B6626	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	151B6626	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	151B6626	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	151B6626	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	151B6626	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	151B6626	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	151B6626	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	151B6626	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	151B6626	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	151B6626	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	151B6626	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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
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\30A5DA22.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\DAA79FBB.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\~DF9482E233D58BBA4D.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\tstBC9.tmp	success or wait	1	66412F42	unknown
C:\Users\user\AppData\Local\Temp\tstBF8.tmp	success or wait	1	66412F42	unknown
C:\Users\user\AppData\Local\Temp\tstBF9.tmp	success or wait	1	66412F42	unknown
C:\Users\user\AppData\Local\Temp\tstBFA.tmp	success or wait	1	66412F42	unknown
C:\Users\user\AppData\Local\Temp\y211A.tmp	success or wait	1	151B4702	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DF9482E233D58BBA4D.TMP	success or wait	1	661B5805	unknown
C:\Users\user\Desktop\~$rdynefile08.11.22.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\30A5DA22.png	0	65536	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 7c 00 00 02 65 08 02 00 00 00 fd 56 fd 52 00 00 20 00 49 44 41 54 78 fd fd fd fd fd 34 0a fd fd fd fd fd fd 7e fd fd 3a fd fd 74 fd 22 fd fd 03 24 04 fd fd fd fd fd 64 fd fd 2b fd fd fd 25 59 1f 2c 56 01 28 fd fd fd 37 0d 54 fd 30 33 22 22 22 00 fd 4f fd fd fd fd fd fd 3f 3e fd fd 79 fd 7d fd 76 fd 26 75 fd 0f 1e fd ff fd 3f 30 fd fd fd 0d fd 67 fd 4e 48 fd fd fd fd fd db fd 0a fd fd 2e 1e 1c 46 fd fd fd 24 00 00 48 1e 7f 18 fd fd 06 fd fd fd 6b 6d fd 25 22 44 20 fd 3d fd 66 3b fd fd 16 11 fd fd 06 fd ec fd 41 fd 1d fd fd 4f fd fd 77 fd fd 2c 22 6e a7 fd fd 55 fd fd 19 fd 4e 7e 3f 22 fd fd 0b fd fd 27 fd fd fd 37 77 29 41 fd fd 6c fd 2b fd fd fd 01 fd 37	PNGIHDR|eVR IDATx4~:t"$d+%Y,V(703"""'O?>y}v&u? 0gNH.F$Hkm%"D = f;AOw,"nUN~?"'7w)Al+7	success or wait	2	661B5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\DAA79FBB.png	0	65536	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 fd 00 00 01 fd 08 06 00 00 00 37 fd fd 00 00 00 01 73 52 47 42 00 fd fd 1c fd 00 00 00 04 67 41 4d 41 00 00 fd fd 0b fd 61 05 00 00 00 09 70 48 59 73 00 00 21 fd 00 00 21 fd 01 04 fd fd fd 00 00 fd fd 49 44 41 54 78 5e fd fd 09 fd 66 45 75 fd 3b fd fd fd 37 fd fd fd fd fd fd fd 37 fd 56 5b 4c 30 26 31 31 64 54 6f 34 1a fd 09 34 0e 71 4c 4c 34 0e fd 0c 62 3b 21 28 22 fd 04 34 fd 08 fd 60 34 fd 18 fd 12 fd fd 57 fd fd 44 fd 10 15 07 fd fd 3e 43 fd 1e 00 47 fd fd 3c fd fd fd 5b 7b 1d 16 45 fd fd 34 fd fd 7f 50 5d 55 6b fd 5a 35 fd 5d 6b 55 fd fd fd 3e fd 28 fd fd 10 57 fd 4b 01 7a fd 7a 32 49 43 fd 45 fd fd fd fd 00 63 72 15 57 fd 59 67 fd 54 39 2b fd fd 2d e6 67 fd fd 75 fd 68 fd 22	PNGIHDR7sRGBgAMAa pHYs!!IDATx^f Eu;77V[L0&11dTo44qLL4 b;!("4`4W D>CG<[{E4P]UkZ5]kU> (WKzz2ICEcrWYgT9- guh"	success or wait	4	661B5805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\airdynefile08.11.22.doc	unknown	14	success or wait	2	66412FF3	unknown
C:\Users\user\Desktop\airdynefile08.11.22.doc	unknown	4	success or wait	15	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\desktop.ini	unknown	176	success or wait	1	661B5805	unknown
C:\Users\user\Desktop\airdynefile08.11.22.doc	1871238	333	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

Key Path	Completion	Count	Source Address	Symbol
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\408C7	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\00006109F100A0C00000000000F01FEC\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
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\408C7	408C7	binary	04 00 00 00 CC 09 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 1E 7B 7A D9 F8 AD D8 01 C7 08 04 00 C7 08 04 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 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	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	2022-08-11T20:08	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\00006109F100C040000000000F01FEC\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\00006109F100C040000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784258	1426784259	success or wait	1	6618765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F1009040000000000F01FEC\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\00006109F1009040000000000F01FEC\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\00006109F100A0C0000000000F01FEC\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\00006109F100A0C0000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784258	1426784259	success or wait	1	6618765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\408C7	408C7	binary	04 00 00 00 CC 09 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 1E 7B 7A D9 F8 AD D8 01 C7 08 04 00 C7 08 04 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	04 00 00 00 CC 09 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 00 00 00 00 C7 08 04 00 C7 08 04 00 00 00 00 00 DB 04 00 00 00	success or wait	1	661B5805	unknown

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

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

Disassembly

No disassembly