ID: 682720
Sample Name:
suddenlinkfile08.11.2022.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:33:58
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

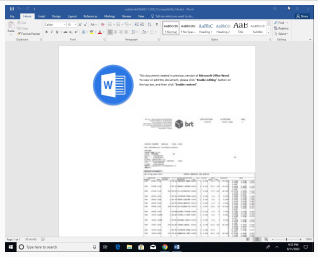
Windows Analysis Report

suddenlinkfile08.11.2022.doc

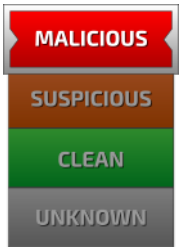
Overview

General Information

Sample Name:	suddenlinkfile08.11.2022.doc
Analysis ID:	682720
MD5:	3b6a5f7e4f048cb..
SHA1:	a2f68a276e0b18..
SHA256:	e9258541a5c96f..
Tags:	doc IcedID
Infos:	



Detection

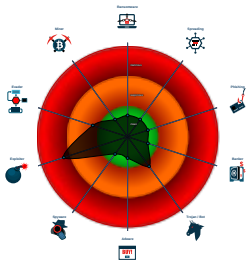


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 4928 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

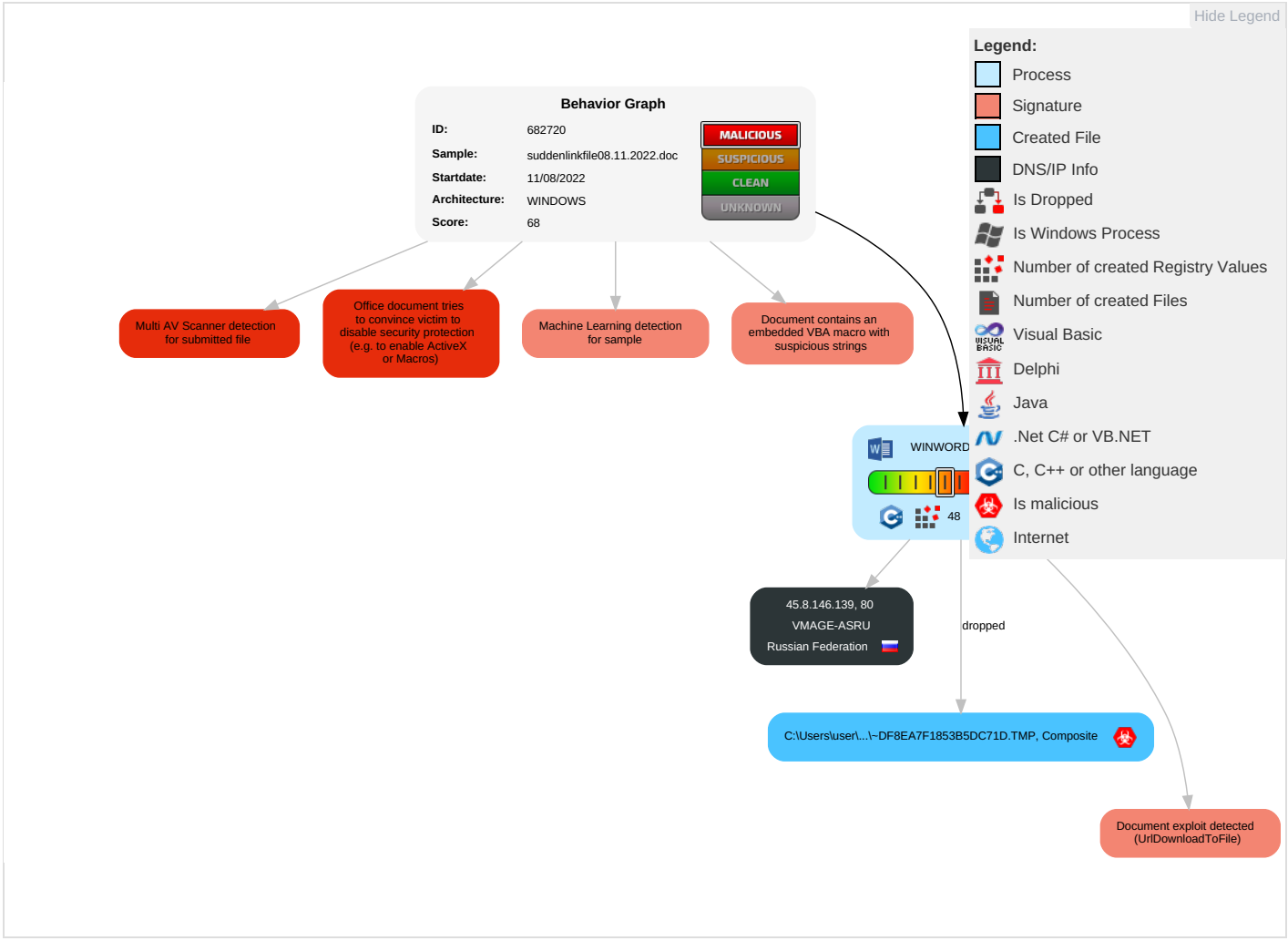
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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

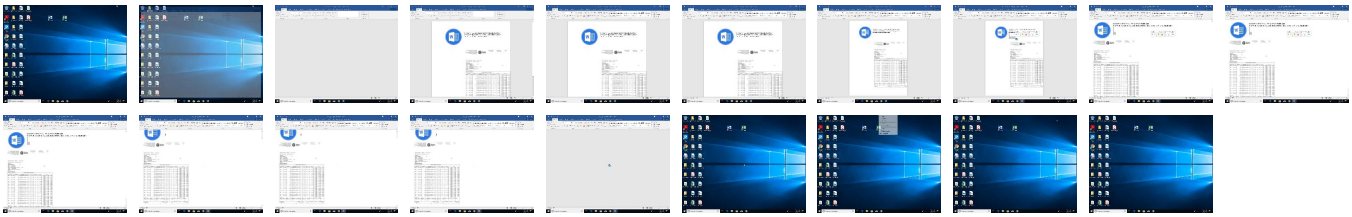
Behavior Graph

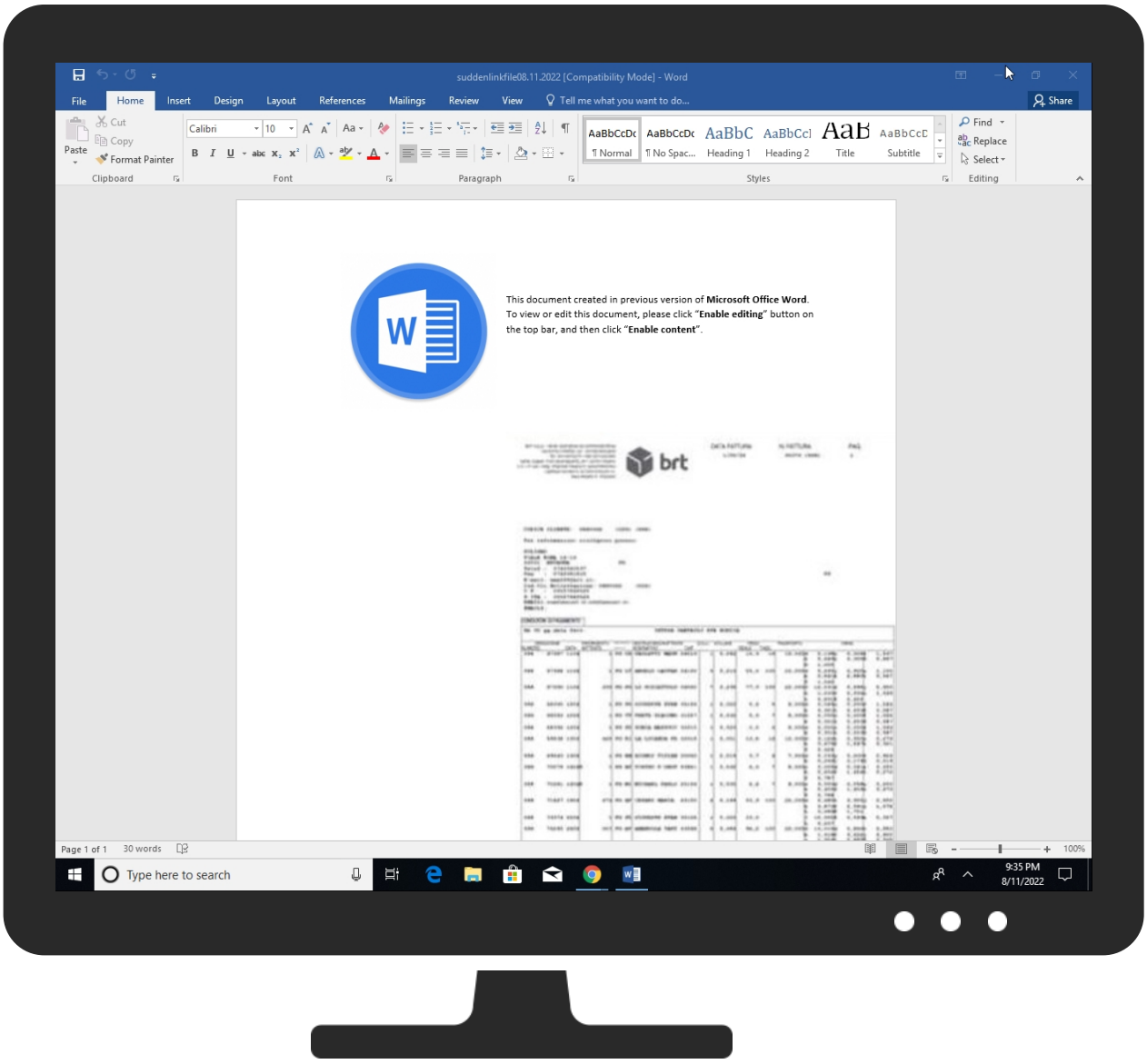


Screenshots

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
suddenlinkfile08.11.2022.doc	26%	Virustotal		Browse
suddenlinkfile08.11.2022.doc	18%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
suddenlinkfile08.11.2022.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF8EA7F1853B5DC71D.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

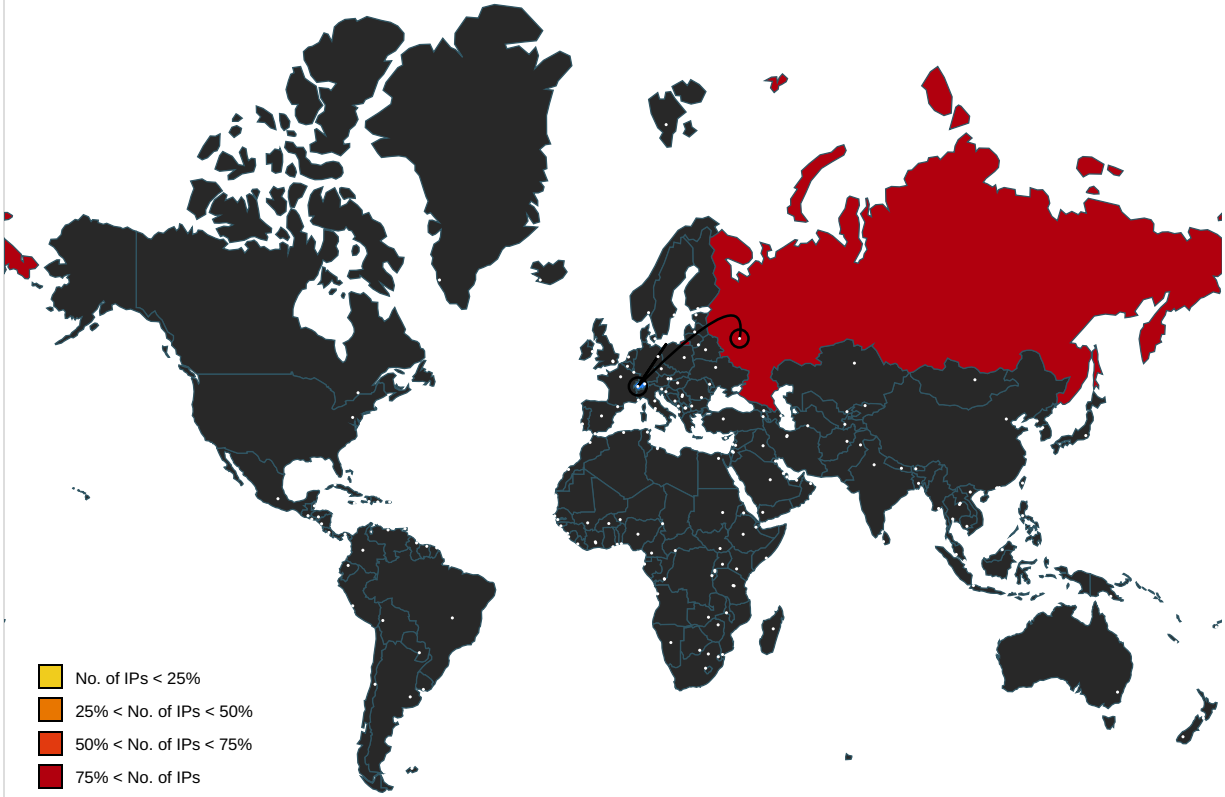
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://login.microsoftonline.com/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://shell.suite.office.com:1443	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://autodiscover-s.outlook.com/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://roaming.edog.	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://cdn.entity.	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://powerlift.acompli.net	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://cortana.ai	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://api.aadrm.com/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://api.microsoftstream.com/api/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://cr.office.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://graph.ppe.windows.net	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://my.microsoftpersonalcontent.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://messaging.engagement.office.com/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://web.microsoftstream.com/video/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://dataservice.o365filtering.com/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://ncus.contentsync.	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://weather.service.msn.com/data.aspx	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://apis.live.net/v5.0/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://messaging.lifecycle.office.com/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://management.azure.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://outlook.office365.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://wus2.contentsync.	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://api.office.net	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://entitlement.diagnostics.office.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://outlook.office.com/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://outlook.office365.com/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://webshell.suite.office.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://management.azure.com/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://devnull.onenote.com	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messaging.action.office.com/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://ncus.pagecontentsync.	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://messaging.office.com/	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	0ACDC8E2-D793-4ED8-82FA-6B88798FAB47.0.dr	false		high

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682720
Start date and time:	2022-08-11 21:33:58 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	suddenlinkfile08.11.2022.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Copyright Joe Security LLC 2022

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.expl.winDOC@1/12@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.32.24, 52.109.12.23, 52.109.12.24
- 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\0ACDC8E2-D793-4ED8-82FA-6B88798FAB47

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):	5.3581643098312
Encrypted:	false
SSDEEP:	1536:ZcQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:g1Q9DQe+zuXYr
MD5:	6AFC5F963B2BBE6E31A0353491A19032
SHA1:	3A59579AF39B80ADCC92FFDA974F26D7E43A1FC5
SHA-256:	CE2A1F5BE1BAFFD7D4A35FD903B8C038F7D920008D3AEC6274F6FFA35A1B8C33
SHA-512:	AC3B6AAA15C8A942AF54B572F18802F72D34783A62A642825948A35B26E6A56CDCFC075FAA542F9CE3A11FEB8D0FD4D8A728917ED986F4BCBD20A1E27FD6C6FB
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="2022-08-11T19:34:57">.. Build: 16.0.15607.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\75A754CF.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):	256096
Entropy (8bit):	7.979290280978911
Encrypted:	false
SSDEEP:	6144:M3Y5ZrfMaWvOqQjH5OHjYDoadLgGB7AgFMg9bdY5aD:MoLfmx8YjY3gk9bdSaD
MD5:	2B87DAB37C0E64FC69EF97114CD433AE
SHA1:	4277610AF912B13E6C5F79C1787E17512D3CB662
SHA-256:	11ED29EF2888F5D9F52BE4BB54EC2A3BAD6A6DA8CBC6A986ABFB960590D2AE30
SHA-512:	B1B9695E19A783B5A967884E72683412B819BA0E5CD48D9728601F83EF7164E8A7115AE509616B131AEDC1C5EF5792D4EB6AE575B2F031A107CF890DAE66E476
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!...!.....IDATx^....fGU..3*.W...z?....^?.I.....8....'.AI.Q.HBB..@ .B:=%...@.4.!F....0....L.}..1.0&}...}.k.....i... ....Z.j.....}.5..M. ?..w.H...i...=zO_.....1.}!Tz+[.1...r.).:,..k9..k.]Qu.....<.|.?U..6.g...|E.:nI...,G#...O$o.LEO?.mH...r=..F....tVyB....Z"y)..E.g..3..J....r..E.2c..WZ;&5.".).f.i.U...Q..-... .5..X.ce...^..z....k.\|....m\...W~.....qK...2..1^..-.....n.^.. =K.Z....D..5..L.ZZ.0...z2.6K....r.....-f.*/....z...].\|..A.k.....mh.U.n.^..z:r.R..i.+..r.1..t"...^..I.....-....A...D...h.m..... .up@O....S...=...1z....L'Z.0&.H.2-.qK$..D.oQ.m."e{.N..^.5.*...0h.....C..*f..2.l.z..v.T$..[Z.,...*?.^C..+.....=,....N>Qy5.%Sy=.L+[i..Md:...\|.V.....Pe...8..8....I..H^.3.j:QeZ.{.f.{ .Z.U..h.f.!e2.6.....2..S.3$z..+....*....n.\.O.3.j.E.7&..l.q..^..%.dkhq8.Z>...I.....[z.U...L"i5.r5..3.....ek..+.|...*j.....T^...g..Z..*7.2..6...o.g...-;...Z...7.@.YtB...*..zR.X

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A72B1286.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 404 x 560, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	129793
Entropy (8bit):	**7.991103599335203**
Encrypted:	**true**
SSDEEP:	1536:U4MtqqxENtB01ei3aAl/AKK/7zwFACKTMFIUSYEoa8aFSK0fLeCMrSQr4Ho0FK7T:vMIKWtY3ligvSiaYRLmQliHMlzTKI
MD5:	AF92425A49BAE0E026E6ED210EAD4FD2
SHA1:	1BE112AF7400BF91B305597286E3BA5BA54C8D2D
SHA-256:	2745C121B3DF782DFA4D684B264ED6BEC8303B3C85F695A268D633BB9756DAE0
SHA-512:	09638DB753DA0A3FF748217578EDD72F270917406F9786C14564C7A822B43D93084BA22B3E5EFA8523D6DB912CB4A1E0E84E0002D157AFC65A9B5D5B9B5E486
Malicious:	false
Reputation:	low

Preview:	.PNG.....IHDR.....0..... .IDATx...s....H....Q.%_.L235US.r....x^.....[....I..y.Y_....|K.TJ.H.....u...^.o3.x.1%...?g.)._....X.....s..|....lk...{{^..8N.....4..<.{wEY..2.x.1...c2]..y... ^.e.o..3.dv~.....wgX..|._.....T*.V...^.....{.....:..y...+..n.f&3^..y..g.....yf...x..y...m.....x>.1&.L..3..z..3..x...e.JzKfL.x.....v~G..M..{.>.....?x]..<v.....Q...7Y.}...uYm.. 6g.|.....}...^..S.._.g..r.....lP....q....7_x.C...b.%.7_..V....>..m~..<...=.s..m.v.../.}yY.~4..O6....3q....+u...x.v.=.M...s....z....}y..d.`.9b...=....x..4...G.&dY...o...+M..\.gYV*..$). J.R.wy...).. /.....N.^..[...s.....*K*^....)..P..n..,..E_y1.g.....p.....)./(^.}g..h.Fk..b._...<.{.I....._..?./..:.?J.(.H.lE.b.n.....v..<.{O....}@...\|..<.;.w...zvo..?.y....\|xt.!...R.jt....Rv~. .7.Oy..G.}.r..''..?.8E.P.....B.T....y.;.....U...!.....h.U.si..[w.}x.x..4M.\..\'ze.-F!.....5.)..@...}.2mD;.....I.;..n..2.u."..g..g$.6...`0_..M.uU6[.w.;]..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{24150DF6-1D3E-436F-806C-6601D0CF03F2}.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:DMlzfRLZRW4WZ1MFKuQ9cc3xn82l+akwkvFp/lt9lknlHll5xlwZZl8/vlk:4LG1ND9Pxn82UakZnUM5
MD5:	4DDA79371896BC810D837D816FB84168
SHA1:	9EC5A1C02624D480EF288C45E10B5B60F167E38E
SHA-256:	739D213BA26479353FC102B4735E315991A768B1B3593AB057B24A628D9D7935
SHA-512:	DE0D4F08F4BC4A629021193467865DCBDCD7305F803A3BAAB3CBB8DA58DA0975B1005090A0DC3176BB80DE4226E77432012C772DB691AF75B725B2248DCBB50
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{933789ED-2DBE-45E0-BC5D-68EAB1A560C7}.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\~DF8EA7F1853B5DC71D.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):	4.450047689856643
Encrypted:	false
SSDEEP:	768:qa9eGcbHfauzSDp2chKcrb6IGpg7t766D:qa9ZcrfaukpLru87
MD5:	C5968ADE1D73EA19E5F3FF6230E4D645
SHA1:	114A50D9F4F324B25C15C8F233E7A00B8D219070
SHA-256:	430F47D52F900DA3E105905A14EC7BBFB2F66C77B16A3B07583ECFBCB80EEC1B
SHA-512:	9D14623E6D19C4E8AA05A3BE7023972D387743F118465D7FD9A5499D5DC62AA7B3B5C6C9B26AB27E6A269782A7C7C83487A0F864172B66DCD3AEDF19F1BDDC7D
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.....

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):	99
Entropy (8bit):	4.644735439919192
Encrypted:	false
SSDEEP:	3:bDuMJlOUBA9MLsIYj9omX1Xw9MLsIYj9ov:bC6oK7Yj9OK7Yj9y
MD5:	6EF1C4B749DFF30D0B3C286D1DC65F3D
SHA1:	DBA1564C758F374CC424B56A0B94EFEF9207A926
SHA-256:	96616B6B94968109EC8B6F850C90192ACD4D4E7D943F3C3AEC152268B0C69736
SHA-512:	BB554EC4558B05FB85F82E5AE1EC51B4BF1D3D5A2126A19581B9F53873BA159446D60010D3ECBB95132909E204D8891518414BD1F5C069A97C0744975005D420
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..suddenlinkfile08.11.2022.LNK=0..[doc]..suddenlinkfile08.11.2022.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\suddenlinkfile08.11.2022.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 08:43:08 2022, mtime=Thu Aug 11 18:34:59 2022, atime=Thu Aug 11 18:34:53 2022, length=2271478, window=hide
Category:	dropped
Size (bytes):	1125
Entropy (8bit):	4.69205220940561
Encrypted:	false
SSDEEP:	12:8BGqBUhduCH2Tdx+8u3nCe+WKz2KfSIoajAw/DPvsj9LBn2Daru44t2Y+xIBjKZm:8OCdtcCn2KfJAwbM9ADo7aB6m
MD5:	5E422C1AA156407D8D162373FEE8A56B
SHA1:	0F4E9B48205F8919334AADFDA19C63CAF1DE881A
SHA-256:	AC07163A2673B4E11214E6F1FFDB37330FAA9715D5292FC893F3283D8B500572
SHA-512:	D336892E62DC9E989A558CE0A0181DD3F0DC8FAC38A2B0FB2DD453FF66E4110D9612E56D483BCE215A7DBB26940ECFDB9FCDFD2E5F0968FC1175EF3C38C28 9F
Malicious:	false
Preview:	L.....F.... ....^...2..3k.q.....Vcn.....".....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...UT.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....hTfM..user.<.....N...UT.....#J.....^ .j.o.n.e.s.....~.1.....hTgM..Desktop.h.....N...UU.....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[. .SUDDEN~1.DOC..j.....hTeM.U[.....V.....,..s.u.d.d.e.n.l.i.n.k.f.i.l.e.0.8...1.1...2.0.2.2...d.o.c.....b.....-.....a.....>.S.....C:\Use rs\user\Desktop\suddenlinkfile08.11.2022.doc..3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.s.u.d.d.e.n.l.i.n.k.f.i.l.e.0.8...1.1...2.0.2.2...d.o.c.....:..,.LB.)...As...`.....X.....675052... .....!a..%.H.VZAj...O%$.....!a..%.H.VZAj...O%$.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.

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):	2.1664096652442013
Encrypted:	false
SSDEEP:	3:Rl/ZdsIrOzlflqK5netlllt7eIRlllFr:RtZG6iylGJ
MD5:	B113B31E367A3D8E7B7532D76D841461
SHA1:	4C7EC260D1756A2601BE91C32E8C5A27AF566C06
SHA-256:	705C60A02938D7406698F208E4EFA2B564EC7CD056D20AAAB9C3AD4D0FEF9EBB
SHA-512:	5BD02250D8D5C037DDC90F7C81481B448FE5276542E59D02CD1CAA204B1A2020C3A563050F8C4C74A12B94ACBD7A0B18219EBAA8A632F88F757DA84497D694 4
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....X.{3.+.....$.....6C.....\..3.,.....P.s3.-.....

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\~$ddenlinkfile08.11.2022.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1664096652442013
Encrypted:	false
SSDEEP:	3:Rl/ZdsIrOzlflqK5netlllt7eIRlllFr:RtZG6iylGJ
MD5:	B113B31E367A3D8E7B7532D76D841461
SHA1:	4C7EC260D1756A2601BE91C32E8C5A27AF566C06
SHA-256:	705C60A02938D7406698F208E4EFA2B564EC7CD056D20AAAB9C3AD4D0FEF9EBB
SHA-512:	5BD02250D8D5C037DDC90F7C81481B448FE5276542E59D02CD1CAA204B1A2020C3A563050F8C4C74A12B94ACBD7A0B18219EBAA8A632F88F757DA84497D6944
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....X.{3.+.....$.....6C.....\..3.,.....P.s3.-.....

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993948464282991
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:	suddenlinkfile08.11.2022.doc
File size:	2366716
MD5:	3b6a5f7e4f048cb005496243fe2a019e
SHA1:	a2f68a276e0b18cb1f11745d9046f4ffa1b1a428
SHA256:	e9258541a5c96fcacb6a2ce349282db7e9403a16fa9f952e8f1f69929dda7abc
SHA512:	f8e777ebbf8ef85d0299552f8580adf97af8eb236fd94f998c47417369bebbfeb54882ca34dcd60c9444cc4624fa0f8d8f32c8037abe29dd50a0b6f478c842f1

SSDEEP:	49152:+YswLHjvPXNnVtQ8364b8uIhZ3fR4Bit3soDB1Nu8aSSaz:+HyDv/hVtQ8K449hZvOit3sU1NWZu
TLSH:	5FB533BF108D46C7E51892FD24DE357412EA8AF18A32FC02A85D851A14A17FF96E7F31
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/682720/sample/suddenlinkfile08.11.2022.doc"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 2811

General

Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2811
Data ASCII:	.B.Attribut.e VB_Nam.e = "Thi.sDocumen.t"...Bas..1Normal...VGlobal!.Spac.lFa.lse.JCrea.tabl. .Pre decla..Id..#Tru."Exp.ose..Temp.lateDeri.v.$CustomlizC.P.... .D.? PtrSa.fe Function .... Lib "us.er32" Al.ias "Set.Timer" (ByVal... ..... As Long.9, ...
Data Raw:	01 42 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:	5.3102107547738004
Base64 Encoded:	True
Data ASCII:	ID="{62DA6FD2-8ADE-45CC-8D66-62369416 71A8}"..Document=ThisDocument/&H00000000..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="C6C42C6834E8FEECFEECFEECFEECFEEC"..DPB="8C8E66BEEA85EB85EB85"..GC="5250B8FC7FFD7FFD80"....[Host Extender Inf
Data Raw:	49 44 3d 22 7b 36 32 44 41 36 46 44 32 2d 38 41 44 45 2d 34 35 43 43 2d 38 44 36 36 2d 36 32 33 36 39 34 31 36 37 31 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:	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: 5100

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	5100
Entropy:	1.9301053137693698
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . 8 . . . . P . . . . " . . . . q . . . . A . . . . ` . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . `) : . . . .
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 22 00 1f 00 00 00 00 00 01 00 01 00 00 00 01 00 71 07 00 00 00 00 00 00 00 00 00 00 a1 07 00 00 00 00 00 00 00 00 00 00 d1 07

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 2724

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	2724
Entropy:	2.6952890745198705
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . . ` . . . . . . . . . . . . . . . p . . . . . . . . . . . . . . . . . A . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . ` . . . . , . . p . . . . a . . . . Q P . . . . \\ . . 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 40 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 60 00 d1 08 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 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:	6.302113664638795
Base64 Encoded:	True
Data ASCII:	. . . . 0 . . . . . . H . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . V 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 fa 56 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 21:35:04.125730038 CEST	49756	80	192.168.2.4	45.8.146.139
Aug 11, 2022 21:35:07.135040045 CEST	49756	80	192.168.2.4	45.8.146.139
Aug 11, 2022 21:35:13.135554075 CEST	49756	80	192.168.2.4	45.8.146.139

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 4928, Parent PID: 804

General

Target ID:	0
Start time:	21:34:54
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:	0xe10000
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\tstA0AF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65AA2F42	unknown
C:\Users\user\AppData\Local\Temp\tstA0B0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65AA2F42	unknown
C:\Users\user\AppData\Local\Temp\tstA0E0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65AA2F42	unknown
C:\Users\user\AppData\Local\Temp\tstA0E1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65AA2F42	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	6591977C	unknown
C:\Users\user\AppData\Local\Temp\yB219.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14AB46AB	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14AB6626	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	14AB6626	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	14AB6626	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	14AB6626	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	14AB6626	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	14AB6626	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	14AB6626	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	14AB6626	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	14AB6626	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	14AB6626	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	14AB6626	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	14AB6626	URLDownloadToFileA
C:\Users\user\AppData\Roaming\Microsoft\Proof	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6581765D	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6581765D	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	6581765D	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A72B1286.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	65845805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\75A754CF.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	65845805	unknown
C:\Users\user\AppData\Local\Temp\~DF8EA7F1853B5DC71D.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	65845805	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstA0AF.tmp	success or wait	1	65AA2F42	unknown
C:\Users\user\AppData\Local\Temp\tstA0B0.tmp	success or wait	1	65AA2F42	unknown
C:\Users\user\AppData\Local\Temp\tstA0E0.tmp	success or wait	1	65AA2F42	unknown
C:\Users\user\AppData\Local\Temp\tstA0E1.tmp	success or wait	1	65AA2F42	unknown
C:\Users\user\AppData\Local\Temp\yB219.tmp	success or wait	1	14AB4702	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DF8EA7F1853B5DC71D.TMP	success or wait	1	65845805	unknown
C:\Users\user\Desktop\~$ddenlinkfile08.11.2022.doc	success or wait	1	65845805	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	6581765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	0	2	fd fd		success or wait	1	6581765D	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	6581765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	16	4	0d 00 0a 00		success or wait	1	6581765D	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A72B1286.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 02 30 08 02 00 00 00 2e fd 0a fd 00 00 20 00 49 44 41 54 78 fd fd fd 73 fd 92 fd 17 48 fd 00 fd 17 51 fd 25 5f fd 4c 32 33 35 55 53 fd 72 fd fd fd fd 78 5e fd fd 5a fd b3 fd 1d 5b 85 12 fd 04 49 00 fd 79 fd 59 5f fd 01 fd fd 7c 4b 2e 54 4a fd 48 10 00 fd fd fd 75 fd fd fd 5e 1a 6f 33 fd 78 fd 31 25 fd fd 0c 3f 67 fd 29 fd 5f 7f fd fd 0f 58 fd fd fd fd fd de fd 15 fd 73 fd fd 7c fd fd fd fd 6c 6b fd fd fd 7b 7b 5e fd 1d 38 4e fd fd 1c fd fd fd 72 34 fd 94 3c fd 7b 77 45 59 fd fd 32 fd 78 fd 31 fd fd 18 63 32 5d fd fd 79 fd fd 0a 5e fd 65 07 6f fd 17 33 fd 64 76 7e fd fd fd fd fd 77 67 58 fd fd 7c fd 5f fd fd fd 1d fd 54 2a fd 56 fd fd fd 5e fd fd fd fd	PNGIHDR0. IDATxsHQ%_L235USrx^[IyY_|KTJHu^o3x1%? g)_Xs|lk{{^8N 4<{wEY2x1c2]y^eo3dv~ wgX|_T*V^	success or wait	2	65845805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\75A754CF.png	0	65536	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 fd 00 00 01 fd 08 06 00 00 00 37 fd fd 00 00 00 01 73 52 47 42 00 fd fd 1c fd 00 00 00 04 67 41 4d 41 00 00 fd fd 0b fd 61 05 00 00 00 09 70 48 59 73 00 00 21 fd 00 00 21 fd 01 04 fd fd fd 00 00 fd fd 49 44 41 54 78 5e fd fd 09 fd 66 47 55 fd 0f 33 2a fd 57 fd fd fd 7a 3f fd fd fd fd 5e 3f 0a 49 00 04 11 05 fd 38 00 02 fd fd 27 fd 41 49 14 51 10 48 42 42 fd fd 40 20 10 42 3a 3d 25 fd fd fd 40 fd 34 1a 21 46 fd 0b 8a 17 30 1a 11 fd fd 4c fd 7d fd fd 31 fd 30 26 7d fd fd fd 7d 7f 6b fd fd 55 fd fd 69 fd fd fd fd fd fd fd 5a fd 6a 3b aa fd fd fd 7d fd 35 fd fd 4d fd 20 3f ab fd 77 fd 48 2e fd 6b 69 fd fd 13 3d 7a 4f 5f fd 1f fd 1c fd 31 1e 7d 21 54 7a 2b 5b fd 31 fd fd	PNGIHDR7sRGBgAMAapHYs!!IDATx^fGU3*Wz?^?I8'AIQHBB@B:=%@4!F0L}10&}}kiZj}5M ?wH.i=zO_1}!Tz+[1	success or wait	4	65845805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\suddenlinkfile08.11.2022.doc	unknown	14	success or wait	2	65AA2FF3	unknown
C:\Users\user\Desktop\suddenlinkfile08.11.2022.doc	unknown	4	success or wait	16	65AA253D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	end of file	1	6581765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	6581765D	unknown
C:\Users\user\Desktop\suddenlinkfile08.11.2022.doc	1871538	334	success or wait	2	65845805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	65858A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	65858A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	65858A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools	success or wait	1	6581765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\1.0	success or wait	1	6581765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom Dictionaries	success or wait	1	6581765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	65845805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	65845805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2843A	success or wait	1	65845805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	65845805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	65845805	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	6581765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C0000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784257	success or wait	1	6581765D	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom Dictionaries	1	unicode	CUSTOM.DIC	success or wait	1	6581765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom Dictionaries	UpdateComplete	dword	1	success or wait	1	6581765D	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	65845805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2843A	2843A	binary	04 00 00 00 40 13 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 6A 00 6F 00 6E 00 65 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 F2 C0 76 93 B9 AD D8 01 3A 84 02 00 3A 84 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	65845805	unknown

Copyright Joe Security LLC 2022

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 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	65845805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2022-08-11T21:35	success or wait	1	65845805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	65845805	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	1358364673	1426784258	success or wait	1	6581765D	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	6581765D	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	6581765D	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\00006109F1009040000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784258	1426784259	success or wait	1	6581765D	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	6581765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784257	1426784258	success or wait	1	6581765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784258	1426784259	success or wait	1	6581765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2843A	2843A	binary	04 00 00 00 40 13 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 6A 00 6F 00 6E 00 65 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 F2 C0 76 93 B9 AD D8 01 3A 84 02 00 3A 84 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	04 00 00 00 40 13 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 6A 00 6F 00 6E 00 65 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 3A 84 02 00 3A 84 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 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	success or wait	1	65845805	unknown

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

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

Disassembly

⊘ **No disassembly**