ID: 682722
Sample Name:
suddenlink.doc.08.11.22.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:41:26
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

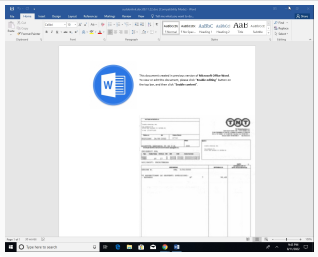
Windows Analysis Report

suddenlink.doc.08.11.22.doc

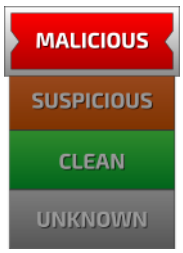
Overview

General Information

Sample Name:	suddenlink.doc.08.11.22.doc
Analysis ID:	682722
MD5:	13f0a9bd5a2a4fd.
SHA1:	bb6d3ab2c01d30..
SHA256:	04042893124fdb..
Tags:	doc IcedID
Infos:	



Detection

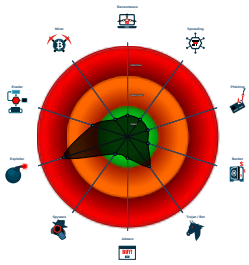


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 3116 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Software Vulnerabilities

Document exploit detected (UrlDownloadToFile)

System Summary

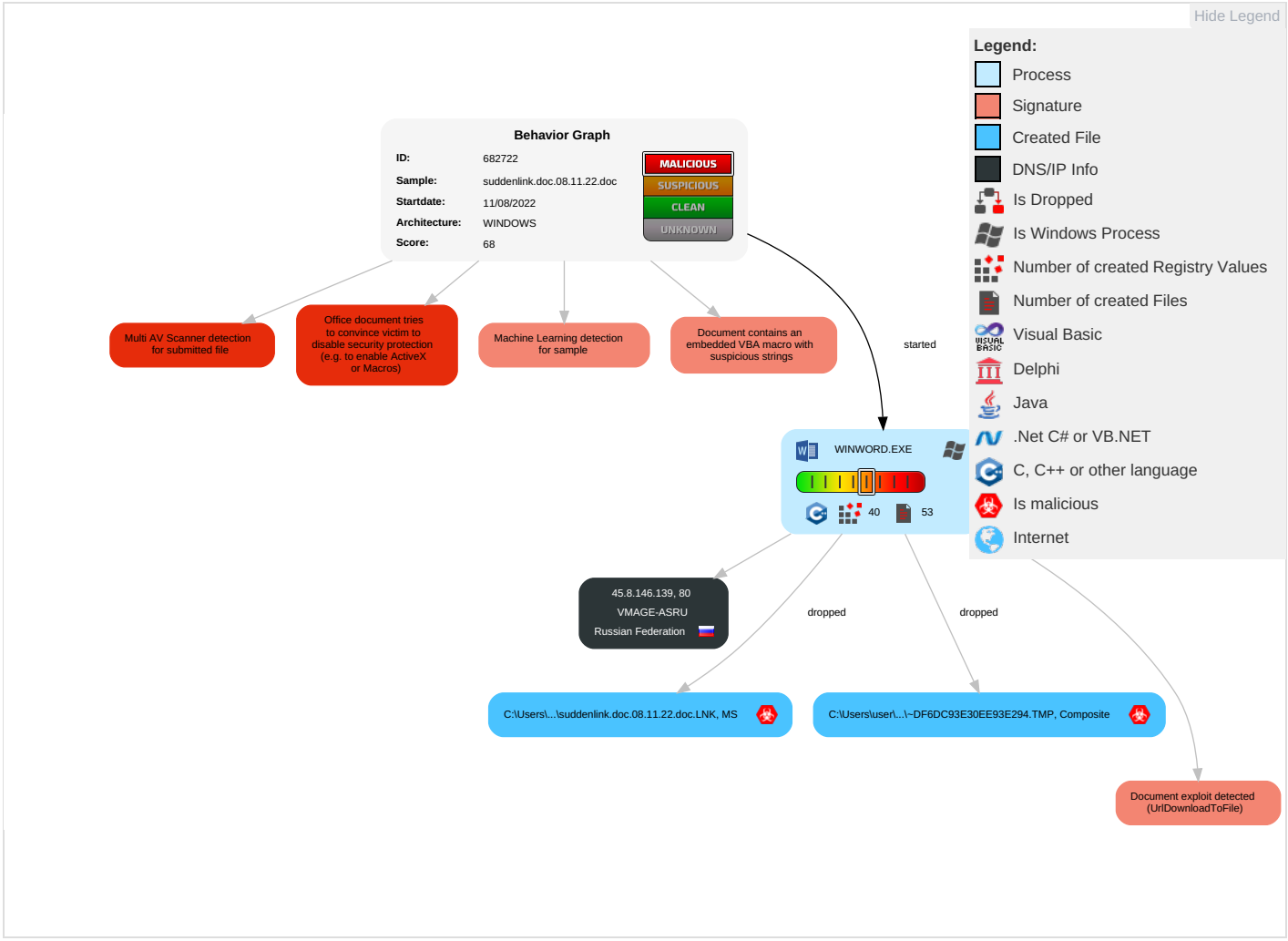
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains an embedded VBA macro with suspicious strings

Mitre Att&ck Matrix

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

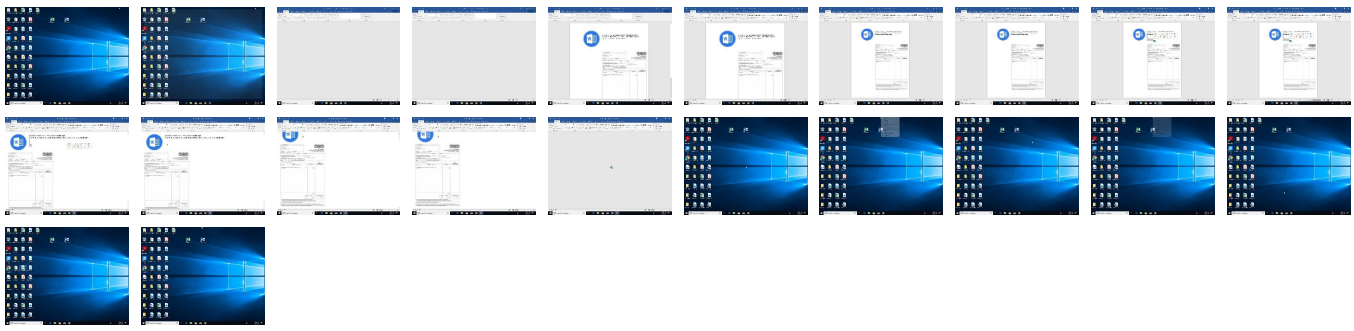
Behavior Graph

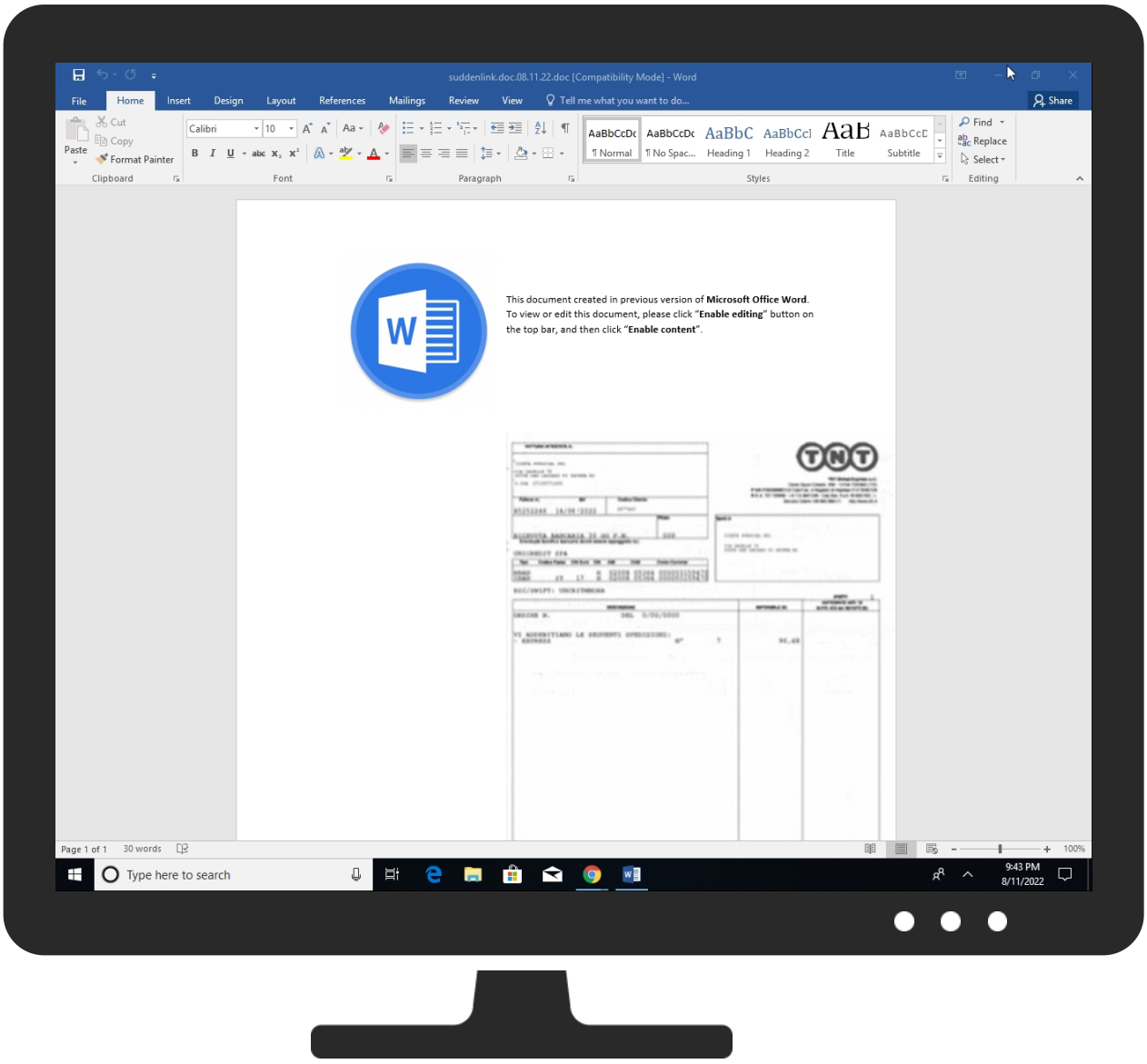


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
suddenlink.doc.08.11.22.doc	25%	Virustotal		Browse
suddenlink.doc.08.11.22.doc	18%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
suddenlink.doc.08.11.22.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF6DC93E30EE93E294.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

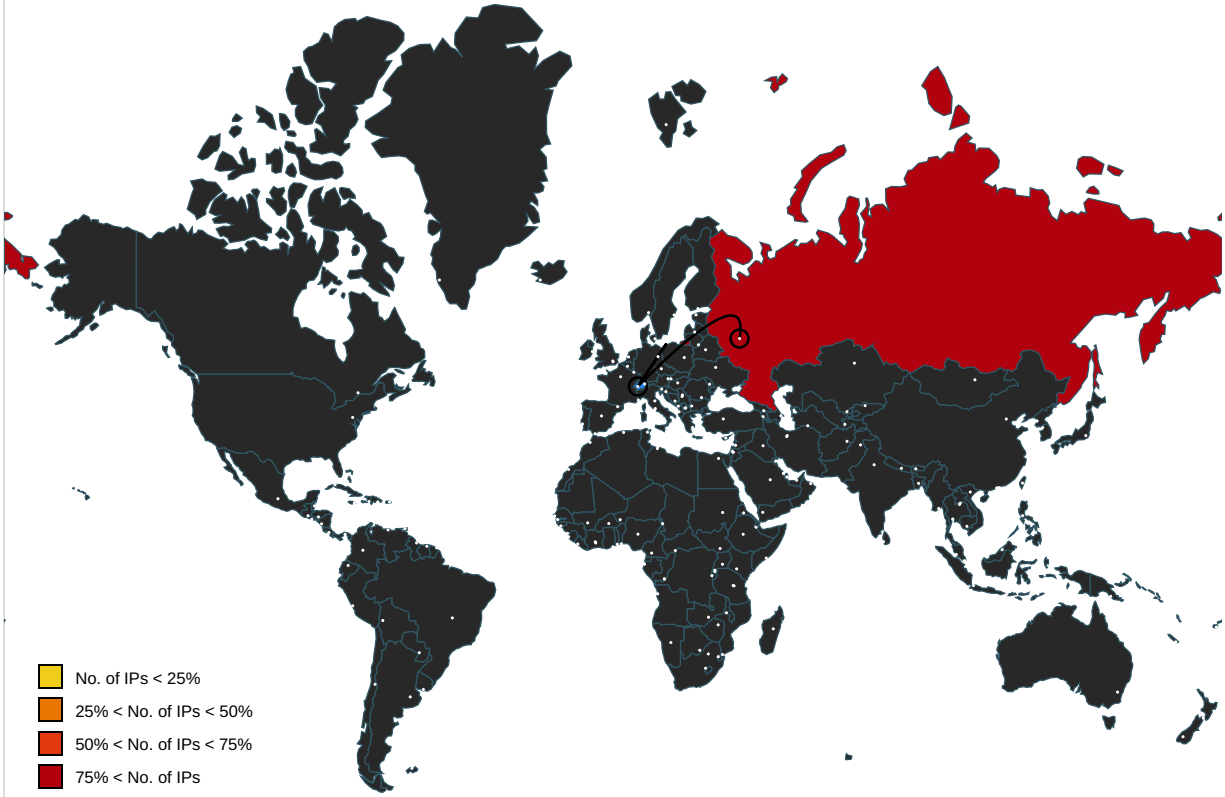
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://login.microsoftonline.com/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://shell.suite.office.com:1443	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://autodiscover-s.outlook.com/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://roaming.edog.	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://cdn.entity.	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://powerlift.acompli.net	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://cortana.ai	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://api.aadrm.com/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://api.microsoftstream.com/api/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://cr.office.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://graph.ppe.windows.net	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://my.microsoftpersonalcontent.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://messaging.engagement.office.com/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://web.microsoftstream.com/video/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://dataservice.o365filtering.com/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://ncus.contentsync.	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://weather.service.msn.com/data.aspx	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://apis.live.net/v5.0/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://messaging.lifecycle.office.com/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://management.azure.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://outlook.office365.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://wus2.contentsync.	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://api.office.net	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://entitlement.diagnostics.office.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://outlook.office.com/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://outlook.office365.com/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://webshell.suite.office.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://management.azure.com/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://devnull.onenote.com	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messaging.action.office.com/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://ncus.pagecontentsync.	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://messaging.office.com/	9DABE267-8D28-4A46-920F-03320802FC01.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	9DABE267-8D28-4A46-920F-03320802FC01.0.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:	682722
Start date and time:	2022-08-11 21:41:26 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	suddenlink.doc.08.11.22.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.expl.winDOC@1/11@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.88.191, 52.109.88.40, 52.109.76.35
- 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\9DABE267-8D28-4A46-920F-0332 0802FC01

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):	5.358148161465603
Encrypted:	false
SSDEEP:	1536:NcQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:81Q9DQe+zuXYr
MD5:	85D5A0CC2B97ECA2389BE32944E85E6B
SHA1:	8BF3217B16BED651794407CE1BDD382FE756388D
SHA-256:	E24B12639A012F5976B4E68DD3C6E96FB2652D891C2FA55E90462C6FF5984344
SHA-512:	8FC47628C000D53E5456D8770D92BEBB31923753200BD6084E899D8D96E19145AB4428118DB71CB372D88A2498D38FF0828DBF27C2821BB3D8076C877B1D817D
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="2022-08-11T19:42:27">.. 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\67134B8C.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):	256025
Entropy (8bit):	7.98021203163416
Encrypted:	false
SSDEEP:	6144:x+Js5bWmwngQ8+C5K7jGQvBxyLuv/YQ2M2xkUfpaj:xcstWmIrC54qGxyKozMW/pq
MD5:	A510821080102B59B41A4B4F7517A2E9
SHA1:	0DE77D02B1EC5854FB491938966A1F21A45B6342
SHA-256:	C00890A5BD755B16A7EDD3639B0499D2DF25D47C1B7869D66DCFDCF4C1128655
SHA-512:	5A993B2FAF68F531EA18473952ECE1E208668789D4652647A8D8B1DD98CB219F6A367AF746FAB3AB73E16DB5AC85EAD3FAB2F24B3408B103445DC47C3886F76A
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!...!.....IDATx^....fWU.3#*m.C.....G..$.H$(.B..Q@R.3.@T..!!..2.....J.@...$Dh.j....L.....1u...}..U;.<....>.k. ..k.....k..K\C..=1F..>C....2...aL>.&..!...P.}!.4...k.V.H...LM'.\.,.....<..dH.....kG..C..2..J#$2.r.c.I....z.h...d[^...0k.3n....5...Yc...y..AO.H.../.....z+."uW.....i..Z~"...[...zj.j.Z(.u.Z.*W Q.*?..W...k.....E..k....#..Z^b..T~..6M.....O....t.^C../.5ni..+w.h.I...5....4....h.GB.|^..'].5T....IE...L{..^....d..d..[.^..g.5_i=T..L.1.....|.@MW@o.A+..4....f.-=Q.K...a.....r....E[~ V.m.d..Ue2nQef...+..1...7A..k.h.=~.J.eA.+..'.\..Vn...=]....m.X..C+.\.Y<Pym...1.P...2I'T.SCE.-...A....^....|;....JT.5.Z^.U..yP....t.z....{r....LW~"iU...4h. iI...f.. dG..)W.g..r-..=.^iI..k.+.. .6..g..k.H..\.Z..y..[..L....C.k...o.5..h.....Np...P..d.....iO.|..v.A.....X....t..zr5..K.U.\.^..{@...#.?&..m..o.u|.c.5_.....|...W..A.+..V.....m...z<@:....Z..,.q.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F770E9F7.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 380 x 526, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	79862
Entropy (8bit):	7.9850226558494
Encrypted:	false
SSDEEP:	1536:3oqyPqib6IbiXmcfDBFdEU8yslk2ZGBlGUCk4+:3yqtImXmcbBFopLwlGDkH
MD5:	F673388F14A0B0E6160D7E31FB8B27A7
SHA1:	792480CA5B43D57E2A0A65466D77A294DA9D55C3
SHA-256:	0D79507FBC5D3C1843F0584E92FFD8B8F2862B4AE569BEB934963B30185E6489
SHA-512:	957C95FE8ED7DC213F027C59952F3F2AB5DFE6ED91944880D230AFC7B2B9EFFD812000FBF26CD6948DD3C478CB9B049C97405F6EBD4A86E3D10241DA3A0B692A
Malicious:	false
Reputation:	moderate, very likely benign file

Preview:	.PNG.....IHDR...|.....4.!... .IDATx...{#...9g...p...l.+....^x..[..'.....9...g.K.t7.0#...Ca....S..[o.:.N:.v.'.....r...W...q.....!.....q.CF.g..._.c.y.....,.;9....6.._z...,./.....nt.../..g.t..._....._./.-.....F.....+mt.X.../...+...0:....../.^.{...b.}.`0.X,....V..|.8N0.$..\...@0....l.ZqB.+?_...fR}....%.\.....Y,.\|A..r..Z..B~8..t.P.~.Cc[p.D.W.INn...f....5....c.If.V....Oh$Y...|....GI.....q... .....u..../..b.`.0.L.@ 0.L..@(.....Ac..Rd...o.....6~x..v..t._...Ph6.E"..... .T.._,..p..e.1.o.....qf.uk/.km/w.Z..<...9.'.|>..B.PH.....K.J.8...$.;.\|>g...A..3\..'._e....pX6x..(..m....Kc6...a.By;.P..R..M.u..p2.\|....7..0V.kO..n...v#..\|>.....pm.....B..$..-..h4:.N#..r..D"|n<...ak..`0.k.g....d@q..Cf<wk..oW.....5.....V.U.+$.*...?.2..r..6...}:=.e.j.l.)/....*....Y..t:.L.....vG.H...t.j....:..`0..FL.H$....d.P(..DB...j%.....g.Y..<??o.Z...t.....l.P(.r.X,&k..._.Fm>..Z....^.7...)...8.X.X,...t:..Dd-.{%.....y.8.x<...h6..H$.H.\..`;[..O....(.....B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{6C1B6A7F-BA2D-469A-BB01-09A37C1CDA0A}.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:DMlzfRLZRW4WZ1MFKuQ9cc3xn82lshakwkvXlDlWlHllFlwZZR+/vlk:4LG1ND9Pxn82Shakw+P
MD5:	633AE63C3E41605BA4AB12E88F26F800
SHA1:	C2A590BE1E2A7F2D87785FAAE94583CA97AED41F
SHA-256:	06B76C39AE90D3FB8A4E204E35F60C42649C89A1E2FB7E82E21C3092BACE2B40
SHA-512:	CC80489B0D03B909E024C2348F55BFD505D015158B14755FA9E343CEBF6D9E97787C8ED3B61D35C7C271F7E21928739D87E23550D15B17B06C28302C65BE44F
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{F4F973F8-3D15-4697-9215-2E0CAB2CDA76}.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\~DF6DC93E30EE93E294.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):	4.438932260613683
Encrypted:	false
SSDEEP:	768:vAgAAuBuNN3kuKmmYHKc5Tw/Pwi6mudzB:v9AAuBuN8YHD+Emu
MD5:	5A7204FD3359FD1084362ED1D510C41B
SHA1:	D52F4265513233431B178C33F27DBC4B7B67CE4D
SHA-256:	D4D2ED2A485353762E999814354442FF401F6FFCDE54BF497F182B3A10B2C2B6
SHA-512:	F289EDAAF00D8AB5613386402212C858B03F607FB0539479A56091D9E53503BDE38DA82AD11D48BA64E6CF35E1D6B38993FEF68C43D0F4B9BA0BA29635EBC93C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

Preview:	.....>..... .....G.....&... .....!..."..#...$...%.....'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8.....:...;...<...=...>.....@...A... B...C...D...E...F...9...]...I...J...K...N...M.....O...P...Q...Z...S...T...U...V...W...X...Y...L...[...\...^....._...`...a.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	105
Entropy (8bit):	4.562792901762571
Encrypted:	false
SSDEEP:	3:bDuMJlOUBA9ML0dRjbbBCmX1Xw9ML0dRjbbBCv:bC6oK0dlbbBwK0dlbbBs
MD5:	3F60945FB9D58F8592D55E8795101908
SHA1:	797CC764F4ADCCF21612D68C5853674CD446B48E
SHA-256:	2E16BA707538C59552A63FB808A0A34D37A2153FA9CBF8CBA8DCE63E03EB4ED8
SHA-512:	175FEEB5252AD79990492779DF0E0B4E58C854542DCA62630F2EDD50F3943DA5D44502F8A074585B82C642499138496FFF3CDC42893B2A5E7BB49651BB47DD4E
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..suddenlink.doc.08.11.22.doc.LNK=0..[doc]..suddenlink.doc.08.11.22.doc.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\suddenlink.doc.08.11.22.doc.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:31:43 2022, mtime=Fri Aug 12 03:42:30 2022, atime=Fri Aug 12 03:42:24 2022, length=2221142, window=hide
Category:	dropped
Size (bytes):	1120
Entropy (8bit):	4.693255753363581
Encrypted:	false
SSDEEP:	12:8GtEJqvbUNauElPCH2bQ8sS0Yvey+WrZ/f0nkjEjAF/hv0dlL14nnqD0R5D4t2Y9:8lEJqEJ8sr8ZHBQAFSdlZJDqb7aB6m
MD5:	36331FDA0FA609507BDF56829C1E2B63
SHA1:	3DA224447B871F8462C10F29D9AA3881710E4A2F
SHA-256:	DF8170F5C97DFC2402E1BBE450B72E9F0696DFD3A58074FC51CC1F9787D28170
SHA-512:	4CEEF6DB01B62C2A75DCB3129533DE9ED59DB18725D9520A879002AFE0C49BCFC67B361E2A5E8923D5C62E262FA5857B9FF25A20A23160E123B32D2386577E70
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ..._`...3....#.....~?.....V.!.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...UF%.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....hT....user.<.....Ny..UF%.....S.....S.h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..UF%.....Y.....>.....OE.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.V.!..UM% .SUDDEN~1.DOC..h.....hT...UM%....h.....s.u.d.d.e.n.l.i.n.k...d.o.c...0.8...1.1...2.2...d.o.c.....a.....-.....`.....>.S.....C:\Users\user\Desktop\suddenlink.doc.08.11.22.doc..2.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.s.u.d.d.e.n.l.i.n.k...d.o.c...0.8...1.1...2.2...d.o.c.....:.,.LB.)...As...`.....X.....226546..... ..!a..%.H.VZAj.....-...!a..%.H.VZAj.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2

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):	2.4605609678762783
Encrypted:	false
SSDEEP:	3:Rl/Zd03X/ymMlp/lXlqJRBKUuRe/n:RtZubJHKc/n
MD5:	CD478BC324F81149C8B7168A49D1DC84
SHA1:	609E4F837546929CFE2652F28405DABB3DBECFA1
SHA-256:	DDB7B9E6FE01D33CD8206DCCB7DC31884EDF06E7F400F2EDC43560386319AACB
SHA-512:	952E2C2FFB6B0F5D6F20C72463A4E325E3702CA2FD5F88D0C3213B72CC2C4CDCD9B80BBC65D81BBCFCB73B46825A89E1520963631DD477D21EF32E13340FB792
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....6....1.....:...62.....T.....6C..-.4.>...23.....

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\~$ddenlink.doc.08.11.22.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4482152888639326
Encrypted:	false
SSDEEP:	3:Rl/Zd03X/ymMlp/lXlqJRBKUujjlln:RtZubJHK4l
MD5:	0DB2B56B5E5014EF14915F6A35B2AD88
SHA1:	6137A0B1F948A89E1F463E9DE3B6893BACEC4127
SHA-256:	646202850E6554F3DACB11F0C47804E24882FD9EC2093AD47F53F0F8D1F64EA9
SHA-512:	AE4C99DDC70A85C33417452C993AA8E7DD3A510C5A0FC71E106700FD13D7EB89477ECFAE90DD97CE66E14C3E4043F9A0F40FA925BADB5424902169FB9809412
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....6....1.....:...62.....T.....6C..-.4.>...23.....0...

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993530464050495
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:	suddenlink.doc.08.11.22.doc
File size:	2315700
MD5:	13f0a9bd5a2a4fd90924a953eb9b1642
SHA1:	bb6d3ab2c01d3058964cd6493a691ad9971307ca
SHA256:	04042893124fdbf007cfdb673ef878ac9a47f37f871c1e5322ec46945915abc1
SHA512:	4a5d5d80a802886231ff33a37f2bb5e319aee424fe965e69638e77491680543885514bd314e633e2be51475b5585705b0ed1d111bc4dd612d94e82f7a725fc9b
SSDEEP:	49152:T/6jUrhhEP6jf4bkgrMk3tuXBJzExnppCcssLxoO:TyjTijf8IFxJzqppCEoO
TLSH:	49B533C47306AF5D811748F0201FBF87EA705485A71B935929ABF68DCEF260DB2C794A
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/682722/sample/suddenlink.doc.08.11.22.doc"	
Indicators	
Has Summary Info:	
Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

Streams with VBA	
VBA File Name: ThisDocument.cls, Stream Size: 2764	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2764
Data ASCII:	. . A t t r i b u t . e V B _ N a m . e = " T h i . s D o c u m e n . t " . . . B a s . . 1 N o r m a l . . . V G l o b a l ! . S p a c . l F a . l s e . J C r e a . t a b l . . P r e d e c l a . . I d . . # T r u . " E x p . o s e . . T e m p . l a t e D e r i . v . $ C u s t o m l i z C . P . . . . . D . ? P t r S a . f e F u n c t i o n . . . . . L i b " . u s e r 3 2 " . A l i a s " K . i l l T i m e r . " (B y V a l . . A s L o n g . ' , . . . # . & . . . .) . # P "
Data Raw:	01 bf b4 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 44 6f 63 75 6d 65 6e 10 74 22 0d 0a 0a 8c 42 61 73 01 02 8c 31 4e 6f 72 6d 61 6c 02 2e 19 56 47 6c 6f 62 61 6c 21 01 aa 53 70 61 63 01 6c 46 61 08 6c 73 65 0c 4a 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72 75 0d 22 45 78 70 08 6f 73 65 14 1c 54

VBA Code

Streams	
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 357	
General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	357
Entropy:	5.311948833105888
Base64 Encoded:	True
Data ASCII:	I D = " { A B 2 E 8 1 4 C - A 2 D F - 4 4 3 8 - 9 9 9 3 - 4 F 2 7 6 A 3 4 4 A E 0 } " . . 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 = " 3 8 3 A E 7 1 D E B 1 D E B 1 D E B 1 D E B " . . D P B = " 7 0 7 2 A F 5 0 B 0 5 0 B 0 5 0 " . . G C = " A 8 A A 7 7 8 8 7 8 8 8 7 8 7 7 " . . . . [H o s t E x t e n d e r I n f o] . . & H 0 0 0 0 0 0
Data Raw:	49 44 3d 22 7b 41 42 32 45 38 31 34 43 2d 41 32 44 46 2d 34 34 33 38 2d 39 39 39 33 2d 34 46 32 37 36 41 33 34 34 41 45 30 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

General	
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:	1.9253220393231318
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 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 22 00 1f 00 00 00 00 00 01 00 01 00 00 00 01 00 71 07 00 00 00 00 00 00 00 00 00 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:	2.6961948881008246
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . P . . . . . p . . . . . ` . ! . . . . . , . . p . . . . . a . . . . . ` . a . . . . . X . . p . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 50 00 b1 08 00 00 00 00 00 00 00 00 00 00 00 04 70 08 00 fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 485	
General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	485
Entropy:	6.299718761930016
Base64 Encoded:	True
Data ASCII:	. . . . . 0 . . . . . H . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . * W d - . . . " . < . . . . r s t d o . l e > . . s . t . . d . o . l . e . (. . h . . ' . 9 \\ G . { 0 0 0 2 0 4 3 l 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 V C . . . . (m . ! O . f f i c g O . f Q . i . c g . . g 2 D F 8 D 0 4 . C - 5 B
Data Raw:	01 e1 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 2a 57 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 01 39 5c 47 00 7b 30 30 30 32

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 21:42:33.847374916 CEST	49743	80	192.168.2.3	45.8.146.139
Aug 11, 2022 21:42:36.876610041 CEST	49743	80	192.168.2.3	45.8.146.139
Aug 11, 2022 21:42:42.877187967 CEST	49743	80	192.168.2.3	45.8.146.139

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 3116, Parent PID: 756

General

Target ID:	0
Start time:	21:42:25
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:	0x1280000
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\tstC2AF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstC2DE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstC2DF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstC2E0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	659F977C	unknown
C:\Users\user\AppData\Local\Temp\yD2B0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	146746AB	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	14676626	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	14676626	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	14676626	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14676626	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	14676626	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	14676626	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	14676626	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	14676626	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	14676626	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	14676626	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	14676626	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	14676626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F770E9F7.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	65925805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\67134B8C.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	65925805	unknown
C:\Users\user\AppData\Local\Temp\~DF6DC93E30EE93E294.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	65925805	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstC2AF.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstC2DE.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstC2DF.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstC2E0.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\yD2B0.tmp	success or wait	1	14674702	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DF6DC93E30EE93E294.TMP	success or wait	1	65925805	unknown
C:\Users\user\Desktop\~$ddenlink.doc.08.11.22.doc	success or wait	1	65925805	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F770E9F7.png	0	65536	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 7c 00 00 02 0e 08 02 00 00 00 34 fd 21 fd 00 00 20 00 49 44 41 54 78 fd fd fd 7b 23 d1 fd 1b 39 67 10 04 fd 70 fd fd fd 6c fd 2b fb fd fd fd 5e 78 fd fd 5b fd fd 27 07 0e 13 08 10 39 fd fd fd 67 fd 4b fd 74 37 fd 30 23 da fd fd 43 61 fd 0e fd e9 53 fd fd 5b 6f 05 3a fd 4e 3a fd 76 1c 27 10 08 04 02 fd fd 72 19 0c 06 57 fd fd fd 71 04 02 fd fd fd 21 fd 04 02 01 fd fd 71 fd 43 46 fd 67 fd fd 1c 5f 0e 63 fd 79 fd fd fd 11 fd fd 0f fd 2c fd 3b 39 fd 0c fd fd 36 13 fd 5f 7a fd 04 fd 2c fd 2f d7 fd fd fd fd 6e 74 fd fd fd 2f d7 fd 67 fd 74 fd fd fd 5f 14 fd 08 fd fd fd 1c 5f fd 2f fd 2d fd fd fd fd fd fd 46 fd fd fd fd fd 2b 6d 74 fd 58 fd fd 79 2f fd fd fd 2b fd	PNGIHDR|4! IDATx{#9gpl+^x['9gK t70#CaS[o:N:v'rWq!qCFg _cy,;96_z,/nt/gt__/- F+mtX/+	success or wait	2	65925805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\67134B8C.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 57 55 fd 33 23 2a 6d fd 43 fd fd fd fd fd 47 fd fd 24 fd 48 24 28 fd 42 26 05 51 40 52 13 33 fd 40 54 14 fd 21 21 09 fd 32 fd fd fd 10 fd 1a fd 4a 90 40 fd 14 fd 24 44 68 fd 6a 11 fd 48 fd 4c fd 04 fd fd fd fd 9c fd 31 75 fd fd fd 7d 7f 1b 55 3b fd 3c fd fd fd fd 3e fd 6b fd fd fd 6b 0f fd fd fd fd fd fd fd 6b fd fd 4b 5c 43 fd 18 3d 31 46 fd fd 3e 43 fd fd fd fd 32 fd fd fd 61 4c 3e fd 26 fd fd 21 fd fd fd 50 f5 7d 21 fd 34 00 fd	PNGIHDR7sRGBgAMAapHYs!!IDATx^f WU3#*mCGH(BQ@R3 @T!!2J@$DhjL1u}U; <>kkkK\C=1F>C2aL>&!P }!4	success or wait	4	65925805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\suddenlink.doc.08.11.22.doc	unknown	14	success or wait	2	65B82FF3	unknown
C:\Users\user\Desktop\suddenlink.doc.08.11.22.doc	unknown	4	success or wait	16	65B8253D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	658F765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	658F765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	end of file	1	658F765D	unknown
C:\Users\user\Desktop\suddenlink.doc.08.11.22.doc	1871619	184	success or wait	2	65925805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	65938A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	65938A84	RegCreateKeyExA

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	65938A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2A7A1	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	65925805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2A7A1	2A7A1	binary	04 00 00 00 2C 0C 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 CC C1 D9 0F 06 AE D8 01 A1 A7 02 00 A1 A7 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	success or wait	1	65925805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	File Path	unicode	C:\Users\user\AppData\Local\Temp\imgs.htm	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2022-08-11T21:43	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	65925805	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358364678	1426784263	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358364683	1426784268	success or wait	1	658F765D	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C00000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1358364678	1426784263	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100C040000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784263	1426784264	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100C040000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784264	1426784265	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100904000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784268	1426784269	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100904000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784269	1426784270	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C00000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784263	1426784264	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C00000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784264	1426784265	success or wait	1	658F765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2A7A1	2A7A1	binary	04 00 00 00 2C 0C 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 CC C1 D9 0F 06 AE D8 01 A1 A7 02 00 A1 A7 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 2C 0C 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A1 A7 02 00 A1 A7 02 00 00 00 00	success or wait	1	65925805	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00	00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

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

Disassembly

No disassembly