ID: 682633
Sample Name:
berniesbooksdocument08.11.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:40:09
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

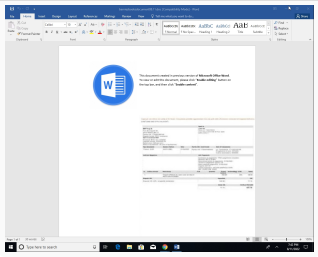
Windows Analysis Report

berniesbooksdocument08.11.doc

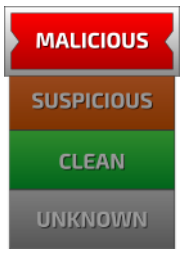
Overview

General Information

Sample Name:	berniesbooksdocument08.11.doc
Analysis ID:	682633
MD5:	2b10f2617b3285..
SHA1:	448e513536aa0c..
SHA256:	3b86f8aff12d2b3..
Tags:	doc IcedID
Infos:	



Detection

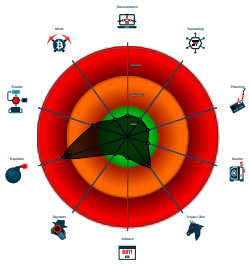


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 5752 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

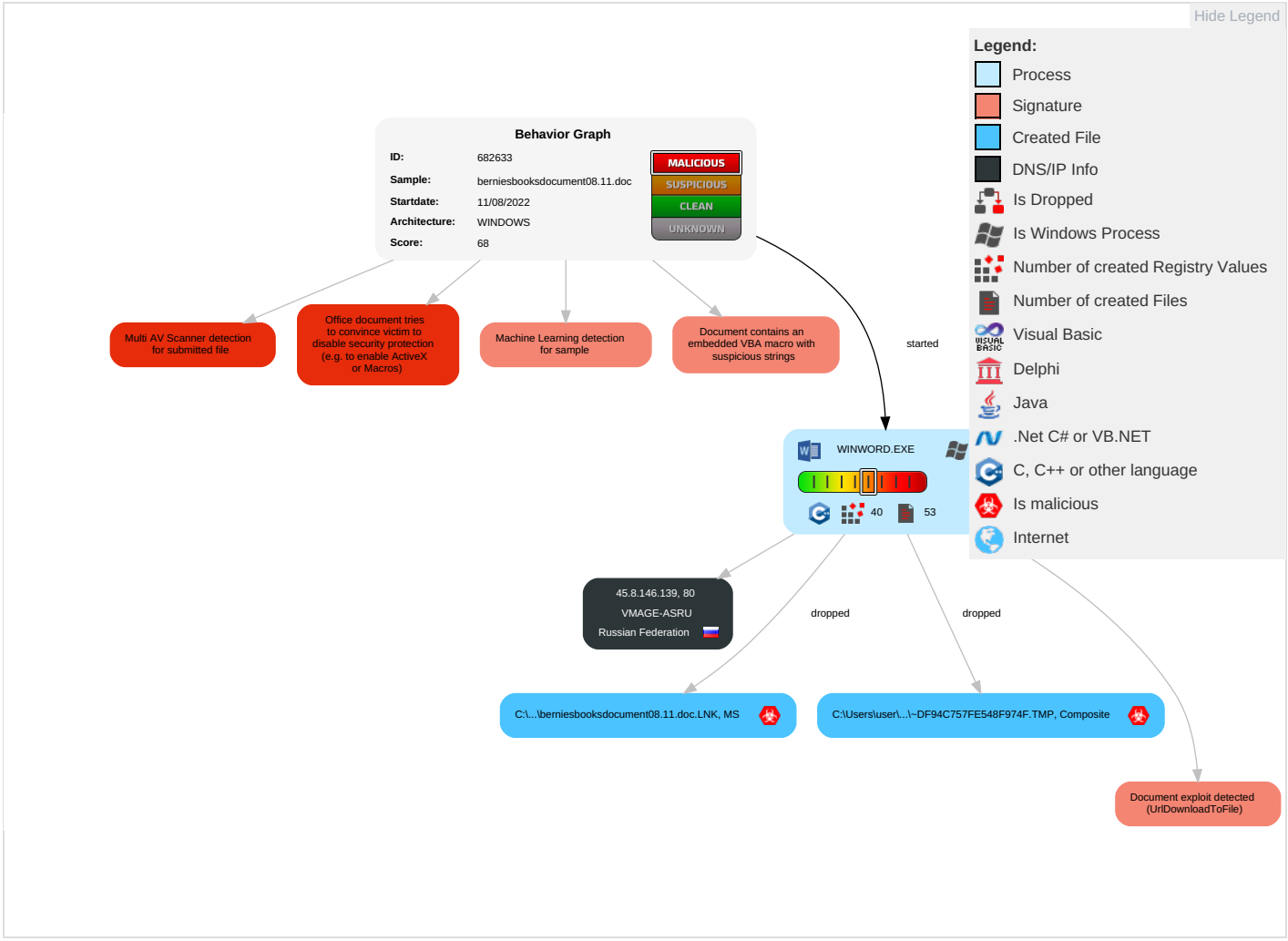
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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

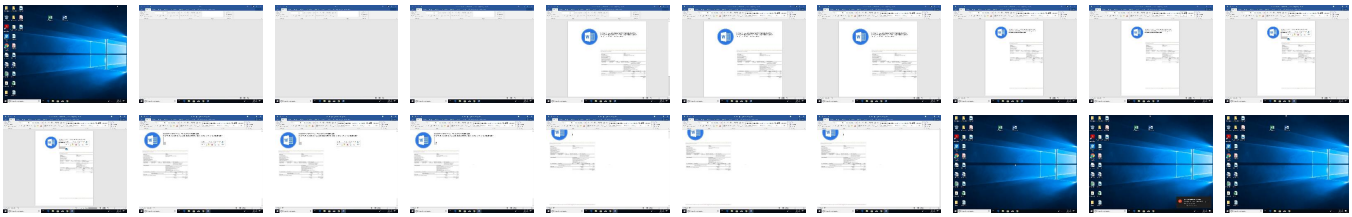
Behavior Graph

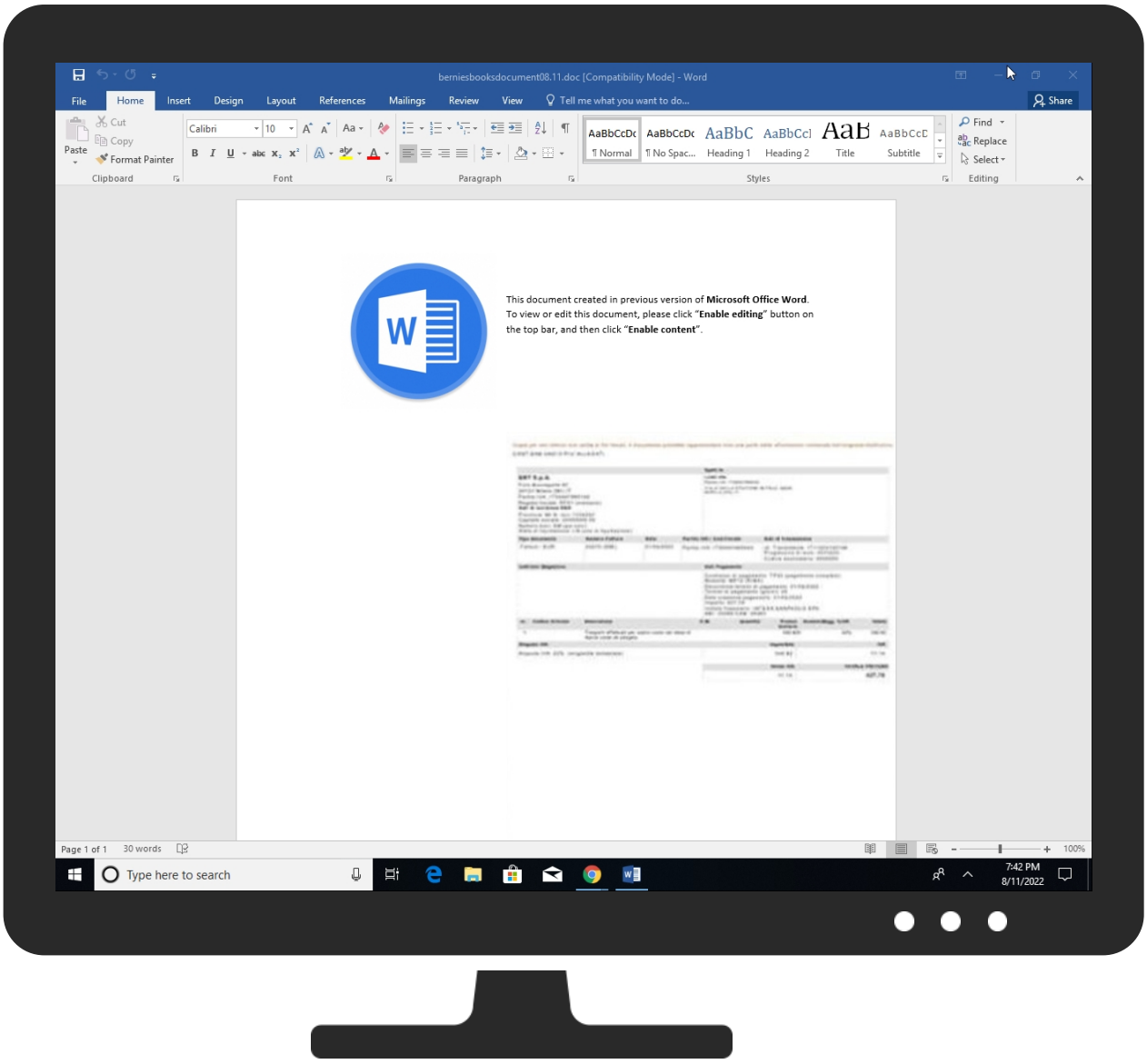


Screenshots

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
berniesbooksdocument08.11.doc	25%	Virustotal		Browse
berniesbooksdocument08.11.doc	15%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
berniesbooksdocument08.11.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF94C757FE548F974F.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

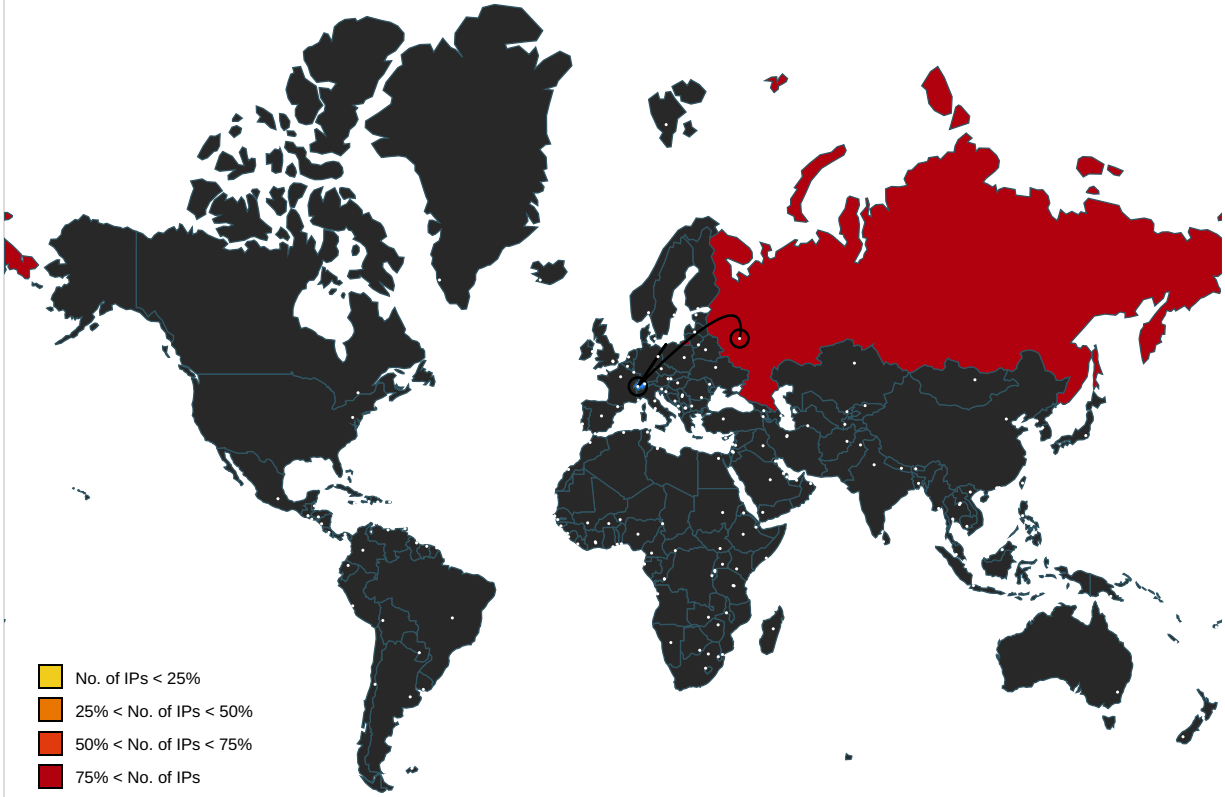
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://login.microsoftonline.com/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://shell.suite.office.com:1443	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://autodiscover-s.outlook.com/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://roaming.edog.	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://cdn.entity.	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://powerlift.acompli.net	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://cortana.ai	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://api.aadrm.com/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://api.microsoftstream.com/api/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://cr.office.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://graph.ppe.windows.net	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://my.microsoftpersonalcontent.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://messaging.engagement.office.com/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://web.microsoftstream.com/video/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://dataservice.o365filtering.com/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://ncus.contentsync.	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://weather.service.msn.com/data.aspx	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://apis.live.net/v5.0/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://messaging.lifecycle.office.com/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://management.azure.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://outlook.office365.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://wus2.contentsync.	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://api.office.net	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://entitlement.diagnostics.office.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://outlook.office.com/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://outlook.office365.com/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://webshell.suite.office.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://management.azure.com/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://devnull.onenote.com	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messaging.action.office.com/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://ncus.pagecontentsync.	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://messaging.office.com/	9776AE02-6E66-4695-8702-04ED8D3C50EB.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	9776AE02-6E66-4695-8702-04ED8D3C50EB.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:	682633
Start date and time:	2022-08-11 19:40:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	berniesbooksdocument08.11.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

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, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.32.24, 52.109.12.23, 52.109.88.39
- 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
- Report size getting too big, too many NtQueryAttributesFile calls found.

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\9776AE02-6E66-4695-8702-04ED8D3C50EB

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):	5.3581472434791655
Encrypted:	false
SSDEEP:	1536:zcQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:K1Q9DQe+zuXYr
MD5:	ACC825E2E9E38DC8B695DC06C6E81DCF
SHA1:	721511992C31C9A85B297EB8DE71CC4CD1AAE4C0
SHA-256:	32D1183E3B7FFF51F028F2D92B501171AA84E81654449D0BF1A2B9C2BE6FD1F1
SHA-512:	B0847AA1439F55B4B377D49B5227ABF251CB3A365BD78B9A967DF3F850CA8ABE68F01286B315AE3885167AAA1F40DE7EE3ACD499A615AD5F1388A959A531BD3D
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="2022-08-11T17:41:17">.. 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\52BE902B.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):	256671
Entropy (8bit):	7.979736340067979
Encrypted:	false
SSDEEP:	6144:Vfyh4MxT1EpRNkndfG4Ir9+2H1RKOqub+rERqbbp3IbFy:NetTcREfPIHH1Rrqq+rEMbbp308
MD5:	5D6FF676E3D91EA33D11782C19FFAF1E
SHA1:	EB5C878B461B6697A0AED6CDF46271D082D26EDA
SHA-256:	6AD88EF0BBE4928886AFCBE59B5C6AF268BC8962DEA7636C7BFB4A593A6FD77C
SHA-512:	5533683E86C4E76D4183C5733FA9EAEDEB81157C5215C7C1E95531E70C1326B72AD8ADE41F284368A42D0DC51AC948730D81D3630246519270D39281297269E5
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!...!.....IDATx^.....GU.39..x...:....<.....E..... (..$!.....3.0.....h+2.FQ..a.$...=$aN....{=kgu...7.u..V.Z5 <UkU.S..6....._.-H....-.d.6.....m.[z.M.Yu.....*=.g[A/_.%f.....U.dTZ.[.ci.N...m<Q.t0+o>..L..V...t`.....x.....@;>I.{...|.;.?..<..^...=....Z...z.-o..{|-.....S.I...".Z9.. \.... ..ie..m....g...p.. %za.Zf.YA2..]...>+o..x..... .....W..0H.'....*z.DM..k..5...*O....R.H....x...c..X..p.GK...p.....L..*.N..S..x+....Z.g...{.....c...2..+.....-...e..{<..8I.6=.`VZE..kz....xE...+.....d.$..D.>..m.(B...B....j....~K..^..3...=Z..Wyg.K.. .u....hi.W]U|8..g..pE....C....*.....i.@.N.....o.[:.....A..D/.~..ZZ.KzMoAZ}....*.....=:h..^}@.>.c...n1+OM.p[N..g..5^.zHY....8.=.6..v@%2..k:h.-..O.:.....$...>..'..KPN[.....t..mZ..W..z|.....?.c<UV..h-.g?...Z$....y...V.l[.j..0...W....Yi .cy{.y...../].....*2...Md<yk<1..~...'.xE/-e.1.1..c|.....e.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FEF36052.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 410 x 568, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	61935
Entropy (8bit):	7.988218918927523
Encrypted:	false
SSDEEP:	1536:vFo53cC4vJ7Y8qgUmqhIIPI2MM+ikJU78DPaFx:vy53qv6nmII0I2ngJAEan
MD5:	4800E90C87A78932178C7D338BA32F43
SHA1:	8006244EDAFF9A31546A17FCF99CB61DA4F69417
SHA-256:	8CD11EB654C64C7315F7B2904D123532F7993FAF2F210B250C4C4D670200FF73
SHA-512:	58994BDC81FF937B05B307C161F852383DAA8504EA17522CD96CDE6EBF99E4992BA64DBEA532424AC16FBD8273999295DBBB74E48A77AAB2122C5701633DC7A3
Malicious:	false
Reputation:	moderate, very likely benign file

Preview:	.PNG.....IHDR.....8.....X.L.. .IDATx..}i..F.-..\r.E.l..u..3....L....^TR-.....DF...*I.e;i.:U.L&...pq.p.1.HD.Z.@.6.._cc.....>.n....2v..c.%...)..G.?|...>k...bf.....c0.sy..$...a....<.....> ".=X1.....1.^|.....|!.....I`E..c.#.T.....'.'.....$6&L1.0.H...X&".cp.l...p.>..?.@?.1.Tp.....Y...=D.]....).w=...~..yp...{x/.....d}1.G.h..b."1..-}.0x...O.....<. &n...0.1...el...."".. ....C<t..A.H.. 4O.L.G....v...6Bd....W{..>..;W.....E.#<..s.^...Q...B.o.=l.lB{...1.ab.$D..:WB$O..V..>..k...y~.w".....A...-.D..;.I.4b.D..E".3...1...f....J.~xv.35G&&....?.acR...P.N....)...U.J....F.I...c$... .. ...a..z&...1..I...D...b.A4.....U.._.D.Z...E.6.G9t..=..qj...^L.$.;...>..S&dD.X... 1...0.{~.w..P.....1.U(....j.PM.....9J..[.O2...).12swy%.3..M?NGt_.....Z.....?F..+.....[4@.=.....; ."..6..i.c..qH4...Ll...8.kl....=""..!..h.g7.\'.....Bb.A...f..o).+..`..++..?u..<.i.M..Gvs..@w.$.2X..'.[.h.8h.3..G.g.E...3..d.)..V*../$)...."%...F....~...s.1@|.....dE.8D|..d.....N.z..(...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{4A67762D-93FC-414F-B3FB-2E9A2A2CA3C8}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.123533094102747
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82lakwkvzlPvllvlHll4vlwZZJ/vlk:4LG1ND9Pxn824krDziT
MD5:	42351AB6AF2118C6741D423B8C584B9B
SHA1:	B218C3ECC3620AB6EDE75FFAC962CA99D4927DE7
SHA-256:	B43CF154493DCC883CFDA39EF5A16F2BC749554FA7804159BD8491FF7A86A8F9
SHA-512:	382BBD1ACA119E158C3C4486516451FEC66F5E616C5A3437FB94B54F5B2E651E76FDB81BD6310A0B69C661C600A1F0AA04D1C27D25430AE8D51D01D753A9FC6
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{DAD70EA0-457E-4A69-832F-387C53F7CCB5}.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\~DF94C757FE548F974F.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	4.452242565616529
Encrypted:	false
SSDEEP:	768:Bi10Cw76gITZvoUUOtLuvrKIeRorvl3BCj:Bi6Cq6gQvVVtKpOor
MD5:	FCE4A2005F82DC3921C8173CEB620F76
SHA1:	23C7D88603074F06F6439EA4CAD9551554D6AEC9
SHA-256:	454E963A3441186E1366D1495F7CA2F56005FA0572FD596F25758557F5A4D66F
SHA-512:	C6937D4E02BECE3E9E7638194E35CDB3D42DB7A0053271018B2FFA7854FFB2112BC5B846A43739688826EACD0BED983C93CEDC05F221763F8224F2E9DAFB92D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\berniesbooksdocument08.11.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 15:31:46 2022, mtime=Fri Aug 12 01:41:20 2022, atime=Fri Aug 12 01:41:12 2022, length=2204163, window=hide
Category:	dropped
Size (bytes):	1130
Entropy (8bit):	4.724353926945833
Encrypted:	false
SSDEEP:	12:8hbZWs1RU9uElPCH2KcbYtLQ+WwN1Hl9BiqOjAT/3cmwBi+DwlgP5gR4t2Y+xIBx:8hb4IcM1H5iATPcb1DwCPO77aB6m
MD5:	02C426E74D3EBEABDF5304DD44FBB9E8
SHA1:	6090705DCB0C4D8ED7CEC5D320E952BBED59241E
SHA-256:	DE9D8D8E3DCC51422116E4058EE7963AE0CD3188A834EB81C7A6FB0AEB8D905D
SHA-512:	8DED508909945E316178AEC28E7198CDA4E707C3CB415DCAF443B76CBEF4F0E503DF8636FA3152F68C3CFF96D8BE7B87E9C3139359546685F4F18DAA9228B71 A
Malicious:	**true**
Preview:	L.....F.... .....3...J....._.M.....!.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...U.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1 .8.1.3.....P.1.....hT....user.<.....Ny..U.....S.....,&|.h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..U.....Y.....>.....od9.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-. 2.1.7.6.9.....2...!..U'. .BERNIE~1.DOC..l.....hT...U'.....h.....b.e.r.n.i.e.s.b.o.o.k.s.d.o.c.u.m.e.n.t.0.8...1.1...d.o.c.....c.....-.....b.....>.S.....C:\U sers\user\Desktop\berniesbooksdocument08.11.doc..4.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.b.e.r.n.i.e.s.b.o.o.k.s.d.o.c.u.m.e.n.t.0.8...1.1...d.o.c.....:.,.LB.)...As..`.....X. .....760639.....!a..%.H.VZAj...w.....-..!a..%.H.VZAj...w.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3

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):	109
Entropy (8bit):	4.656786023512679
Encrypted:	false
SSDEEP:	3:bDuMJlfyNS58JRQUjdzCmX14BS58JRQUjdzCv:bCUyZJG4dz6dJG4dzs
MD5:	88A6F1F506240DB87837382649E2F57A
SHA1:	33553CF8F2A0D6E3CFB55B8A0C3AE4A032F743FB
SHA-256:	E644F2C0DCE8F75BBFB91D2308FDAF411DDFA8EF0E31D70CBA46A544B927CC97
SHA-512:	30F696EC999D2B58C16B7B91E96377B4C05A2B6292D325A4189A3971B1523D6997CEC542999692D6F8F0B67CC8FD000799FA169B32421A0AC9B6E23EF5FB95D2
Malicious:	false
Preview:	[folders]..Templates.LNK=0..berniesbooksdocument08.11.doc.LNK=0..[doc]..berniesbooksdocument08.11.doc.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.353959910568412
Encrypted:	false
SSDEEP:	3:Rl/Zd+vkT/hSR+MgQ/luMClqKnmZlqfZ:RtZ/ixuA8mmfZ
MD5:	2992D726CEBB2BBB07315BCF73B645A6
SHA1:	60198AF79AA2A8BC1A8641BF70B1431C0BE991FE
SHA-256:	44B46EB18FE8D422F7C1744B58E2CA22415212E5054B6E573AE55E8C82ED1F2F
SHA-512:	AE3815CB0302481405EED6A3E7710FDC86C9D6C99A4DB4877EB53179370F4ED206BD601C04BFEA16907B2AA87330F743A389EDE716603A3896AB88BEED0666E 6
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....C.).$...^.i@..iT..i`..iDB.iZR.i.C.).%.....T.....6C.....C.).&.....

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\~$rniesbooksdocument08.11.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.353959910568412
Encrypted:	false
SSDEEP:	3:Rl/Zd+vkT/hSR+MgQ/luMClqKnmZlqfZ:RtZ/ixuA8mmfZ
MD5:	2992D726CEBB2BBB07315BCF73B645A6
SHA1:	60198AF79AA2A8BC1A8641BF70B1431C0BE991FE
SHA-256:	44B46EB18FE8D422F7C1744B58E2CA22415212E5054B6E573AE55E8C82ED1F2F
SHA-512:	AE3815CB0302481405EED6A3E7710FDC86C9D6C99A4DB4877EB53179370F4ED206BD601C04BFEA16907B2AA87330F743A389EDE716603A3896AB88BEED06666
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....C.).$...^.i@..iT..i`..iDB.iZR.i.C.).%.....T.....6C.....C.).&.....

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993790073605077
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:	berniesbooksdocument08.11.doc
File size:	2298836
MD5:	2b10f2617b32857999df1cf5f19f0d8d
SHA1:	448e513536aa0c576b123d5b243e1bdc6d261d6f
SHA256:	3b86f8aff12d2b32461a0b20f01f3d13ee062c80cb647ce09ff33f296b1f9e47
SHA512:	f99a1ffdb12b9fe4bc512f33ef98fa989312951fdbfc6aa8cc09d0725cbb90e2c11727dced788991e00087859054b273f09917d2fa3b52cd5be54ecd257dd85c
SSDEEP:	49152:tIjQhPf8F7u26T076/JsKhCa8CCGEEt1yEU:WjufCre/1UMEEzyh
TLSH:	73B533F8C2706D07F858D195355BEAF27960C6A2863B5EE9F275131BE139B1F4070B28
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/682633/sample/berniesbooksdocument08.11.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: 2850	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2850
Data ASCII:	.J.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. "kernel.32" Alia.s "Virtu.alProtec.t" (ByVa.l . As Long.5,
Data Raw:	01 4a b4 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 44 6f 63 75 6d 65 6e 10 74 22 0d 0a 0a 8c 42 61 73 01 02 8c 31 4e 6f 72 6d 61 6c 02 2e 19 56 47 6c 6f 62 61 6c 21 01 aa 53 70 61 63 01 6c 46 61 08 6c 73 65 0c 4a 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72 75 0d 22 45 78 70 08 6f 73 65 14 1c 54

VBA Code

Streams	
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365	
General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	365
Entropy:	5.222695960979116
Base64 Encoded:	True
Data ASCII:	ID="{8FB13CC5-98A3-44C0-B65D-DC235779DEF4}"..Document=ThisDocument/&H00000000..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="8381840B030F030F030F030F"..DPB="060401880788B898B898B"..GC="898B8E938F938F6C"....[Host Extender Info]..
Data Raw:	49 44 3d 22 7b 38 46 42 31 33 43 43 35 2d 39 38 41 33 2d 34 34 43 30 2d 42 36 35 44 2d 44 43 32 33 35 37 37 39 44 45 46 34 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: PROJECTwm, File Type: data, Stream Size: 41	
General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.0773844850752607
Base64 Encoded:	False
Data ASCII:	ThisDocument.T.h.i.s.D.o.c.u.m.e.n.t.....
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7	
General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	ISO-8859 text, with no line terminators
Stream Size:	7
Entropy:	1.8423709931771088

General	
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:	1.9282501947973256
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . P . . . . . " . . . . . q . . . . . A . . . . . ` . . . . . ` i < . . . . .
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 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:	2.6851031014715843
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . ` . . . . . p . . . . . Q . . . . . Q . P . . . . . 0 . . p . . . . . ` . . . . . \\ . . p . . . . . q . . . . .
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 00 00 00 00 78 00 00 00 08 00 60 00 e1 08 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 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:	6.2963537460893955
Base64 Encoded:	True
Data ASCII:	. . . . . 0 . . . . . H . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . [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 2e 5b 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 19:41:26.923190117 CEST	49742	80	192.168.2.3	45.8.146.139
Aug 11, 2022 19:41:29.992841005 CEST	49742	80	192.168.2.3	45.8.146.139
Aug 11, 2022 19:41:35.988784075 CEST	49742	80	192.168.2.3	45.8.146.139

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: **5752**, Parent PID: **756**

General

Target ID:	0
Start time:	19:41:13
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:	0xf00000
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\tstE0C6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B8BC02	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\tstE0F6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B8BC02	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\tstE0F7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B8BC02	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\tstE0F8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B8BC02	GetTempFileNameA
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	65A4977C	unknown
C:\Users\user\AppData\Local\Temp\yF963.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	144546AB	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	14456626	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	14456626	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	14456626	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	14456626	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	14456626	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	14456626	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	14456626	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	14456626	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	14456626	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	14456626	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	14456626	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	14456626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FEF36052.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	65975805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\52BE902B.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	65975805	unknown
C:\Users\user\AppData\Local\Temp\~DF94C757FE548F974F.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	65975805	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstE0C6.tmp	success or wait	1	65B8BC23	DeleteFileA
C:\Users\user\AppData\Local\Temp\tstE0F6.tmp	success or wait	1	65B8BC23	DeleteFileA
C:\Users\user\AppData\Local\Temp\tstE0F7.tmp	success or wait	1	65B8BC23	DeleteFileA
C:\Users\user\AppData\Local\Temp\tstE0F8.tmp	success or wait	1	65B8BC23	DeleteFileA
C:\Users\user\AppData\Local\Temp\yF963.tmp	success or wait	1	14454702	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DF94C757FE548F974F.TMP	success or wait	1	65975805	unknown
C:\Users\user\Desktop\~$rniesbooksdocument08.11.doc	success or wait	1	65975805	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FEF36052.png	0	61935	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 fd 00 00 02 38 08 02 00 00 00 fd 58 fd 4c 00 00 20 00 49 44 41 54 78 fd fd 7d 69 fd fd 46 fd 2d 10 11 5c 72 fd 45 fd 6c fd fd 75 fd fd 33 fd fd 07 fd 4c fd fd fd fd 5e 54 52 2d fd fd fd 08 fd 0f fd 44 46 fd fd fd 2a 49 fd 65 3b 69 fd 3a 55 fd 4c 26 17 fd 06 70 71 01 70 fd 31 fd 48 44 fd 5a fd 40 fd 36 11 fd 5f 63 63 fd fd 00 fd fd fd fd fd e0 3e 3e fd 6e 07 0e 1b fd 32 76 7f fd 63 fd 25 07 fd fd 29 fd fd 47 fd 3f 7c fd fd 5c 3e 6b 11 fd fd 62 66 fd fd fd fd fd fd 63 30 1f 73 79 ef fd 24 fd fd fd 61 fd fd fd fd 3c fd 0b fd fd 1f fd 0e 3e 22 fd 3d 58 31 10 11 0b fd fd 31 fd 5e 49 7c 2e fd fd fd fd 15 7c 21 0b 09 fd fd 19 49 60 45 fd fd 63 fd 23 fd 54 0f fd 7f fd 15 fd 27 fd 27 13 fd 18 fd	PNGIHDR8XL IDATx}iF-\rElu3L^TR-DF*Ie;i:UL&pqp1HDZ@6_cc>n2vc%)G?|>kbfc0sy$a<>"=X11^|.|!|`Ec#T"	success or wait	1	65975805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\52BE902B.png	0	65536	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 fd 00 00 01 fd 08 06 00 00 00 37 fd fd 00 00 00 01 73 52 47 42 00 fd fd 1c fd 00 00 00 04 67 41 4d 41 00 00 fd fd 0b fd 61 05 00 00 00 09 70 48 59 73 00 00 21 fd 00 00 21 fd 01 04 fd fd fd 00 00 fd fd 49 44 41 54 78 5e fd fd 09 fd fd 47 55 fd 33 39 0f fd 78 23 fd fd 3a fd fd fd fd 3c 02 1d fd 10 06 45 14 fd fd 9c fd fd 14 1c 20 28 fd 08 24 21 03 fd 02 01 98 fd fd fd 33 fd 30 fd 11 04 fd 11 0e 68 2b 32 fd 46 51 fd 0c 61 08 24 7d fd fd 3d 24 61 4e fd fd fd ff 7b 3d 6b 67 75 fd fd fd 37 fd 75 3a fd 56 fd 5a 35 3c 55 6b 55 fd 53 fd fd 36 fd df fd fd fd 12 fd fd 5f fd 2d 48 fd fd fd 1e 2d fd 64 fd 36 fd fd fd fd fd 6d fd 5b 7a fd 4d 34 59 75 02 fd fd 0e fd fd 1e	PNGIHDR7sRGBgAMAapHYs!!IDATx^GU39x:<E($!30h+2FQa$=$aN{=kgu7uVZ5<UkUS6_-H-d6m[zMYu	success or wait	4	65975805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\berniesbooksdocument08.11.doc	unknown	14	success or wait	2	65B8BA5F	ReadFile
C:\Users\user\Desktop\berniesbooksdocument08.11.doc	unknown	4	success or wait	16	65B8BA5F	ReadFile
C:\Users\desktop.ini	unknown	176	success or wait	1	65975805	unknown
C:\Users\user\Desktop\berniesbooksdocument08.11.doc	1871734	333	success or wait	2	65975805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	65988A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	65988A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	65988A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	65975805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2DB05	success or wait	1	65975805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	65975805	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	65975805	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	65975805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2DB05	2DB05	binary	04 00 00 00 78 16 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 A7 26 EB 24 F5 AD D8 01 05 DB 02 00 05 DB 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 00 00 00	success or wait	1	65975805	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 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	65975805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2022-08-11T19:42	success or wait	1	65975805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	65975805	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2DB05	2DB05	binary	04 00 00 00 78 16 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 A7 26 EB 24 F5 AD D8 01 05 DB 02 00 05 DB 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	04 00 00 00 78 16 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 05 DB 02 00 05 DB 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	success or wait	1	65975805	unknown

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

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

Disassembly

⊘ **No disassembly**