ID: 682622
Sample Name: actionplan doc 08.11.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:29:09
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

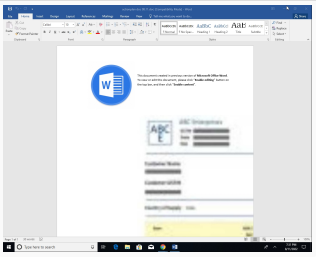
Windows Analysis Report

actionplan doc 08.11.doc

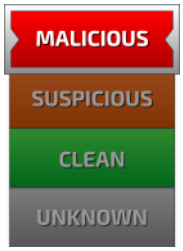
Overview

General Information

Sample Name:	actionplan doc 08.11.doc
Analysis ID:	682622
MD5:	933338ca2c25cf…
SHA1:	e518d12b7bb4ad.
SHA256:	abc8d1097f0249..
Tags:	doc IcedID
Infos:	



Detection

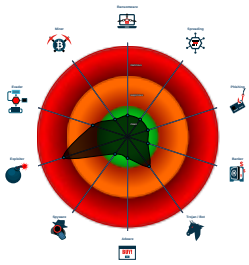


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 6108 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

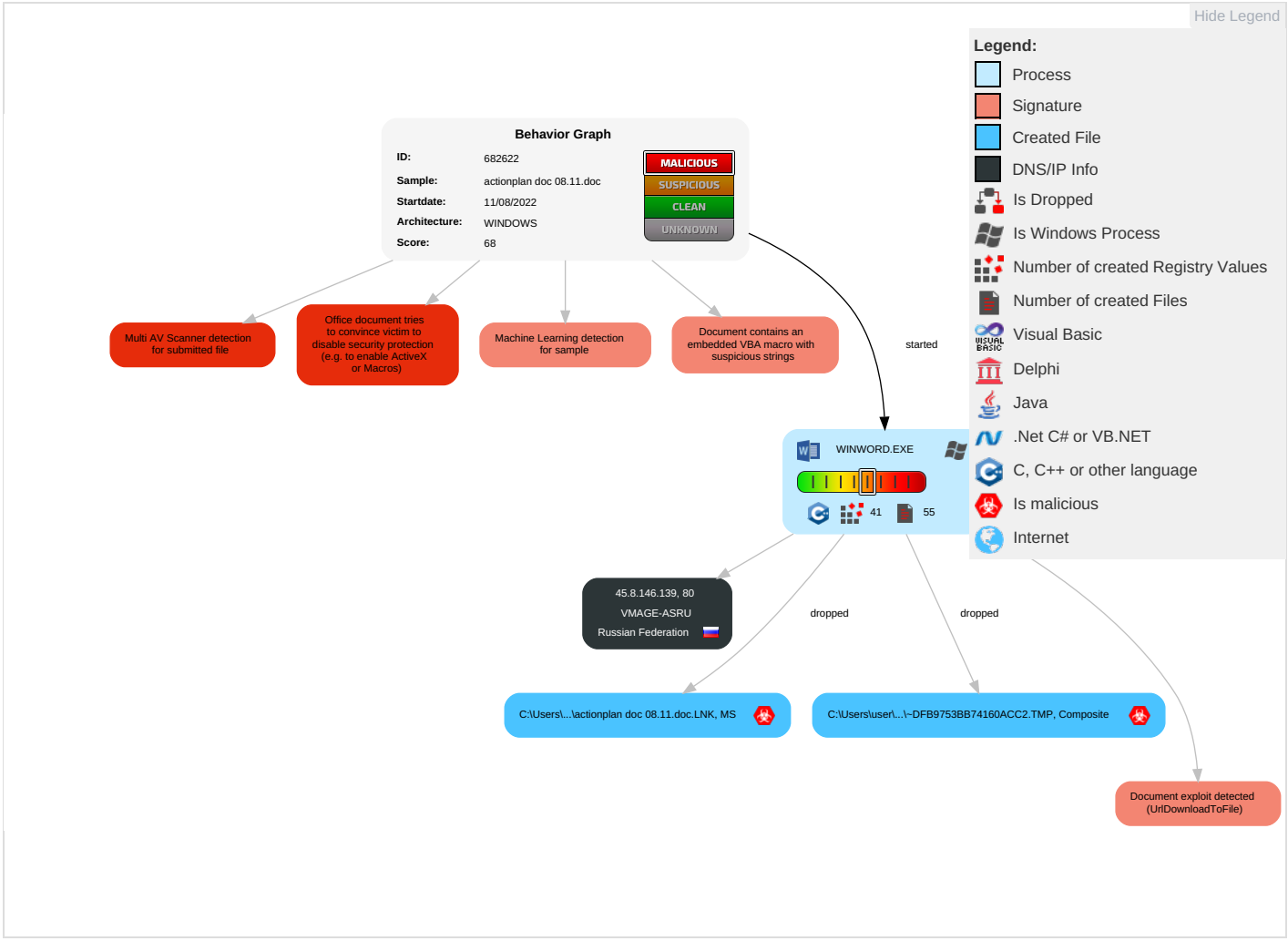
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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

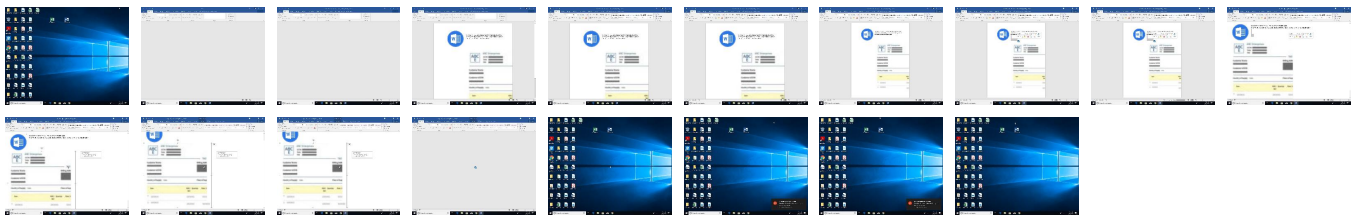
Behavior Graph

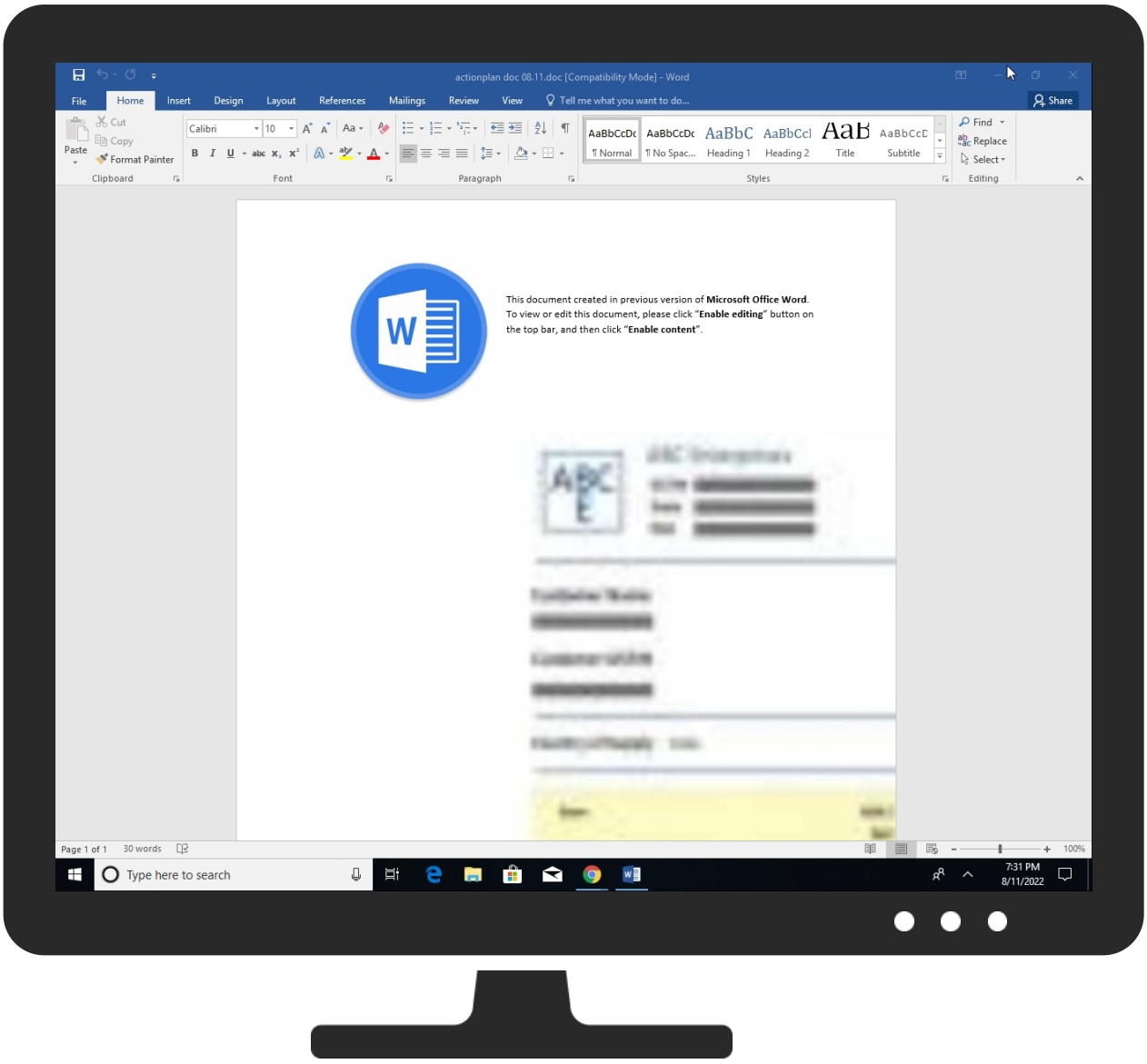


Screenshots

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
actionplan doc 08.11.doc	25%	Virustotal		Browse
actionplan doc 08.11.doc	18%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
actionplan doc 08.11.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DFB9753BB74160ACC2.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

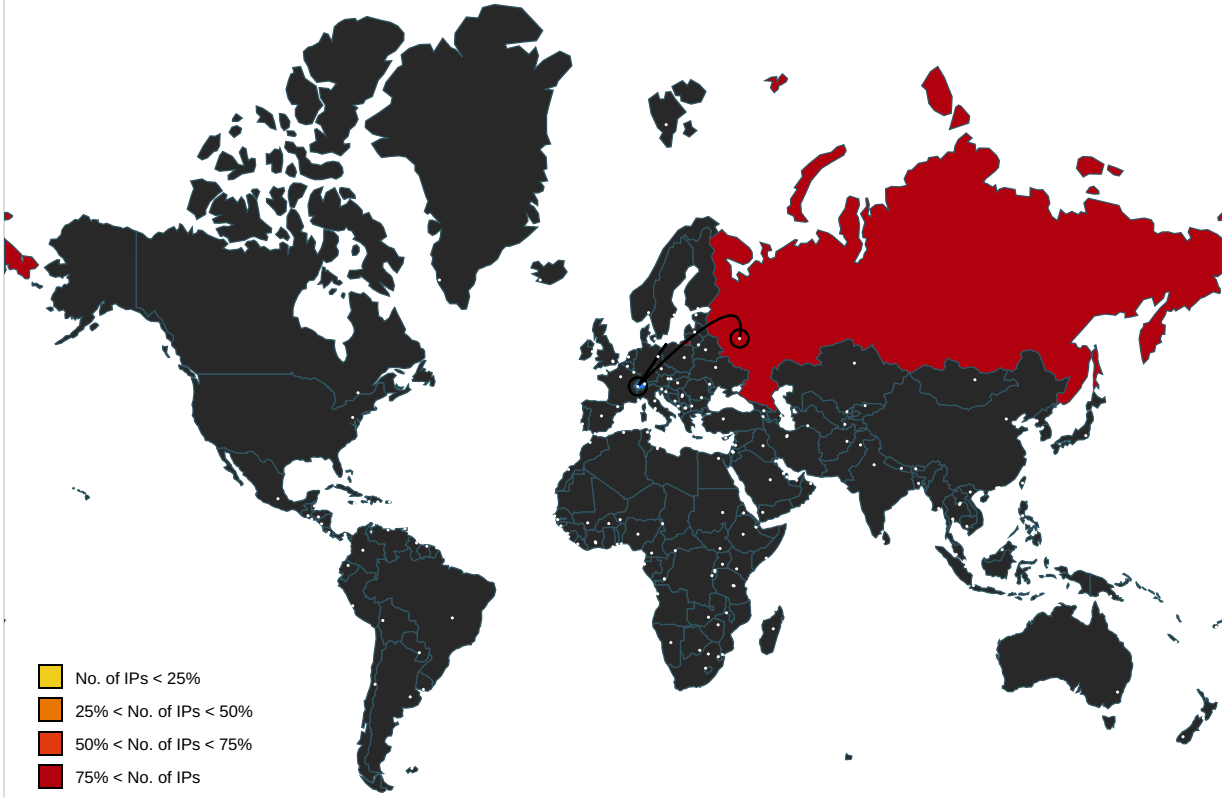
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://login.microsoftonline.com/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://shell.suite.office.com:1443	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://autodiscover-s.outlook.com/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://roaming.edog.	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://cdn.entity.	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://powerlift.acompli.net	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://cortana.ai	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://api.aadrm.com/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://api.microsoftstream.com/api/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://cr.office.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://graph.ppe.windows.net	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://my.microsoftpersonalcontent.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://messaging.engagement.office.com/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://web.microsoftstream.com/video/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://dataservice.o365filtering.com/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://ncus.contentsync.	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://weather.service.msn.com/data.aspx	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://apis.live.net/v5.0/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://messaging.lifecycle.office.com/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://management.azure.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://outlook.office365.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://wus2.contentsync.	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://api.office.net	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://entitlement.diagnostics.office.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://outlook.office.com/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://outlook.office365.com/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://webshell.suite.office.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://management.azure.com/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://devnull.onenote.com	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messaging.action.office.com/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://ncus.pagecontentsync.	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://messaging.office.com/	D87A3441-42E7-470D-8213-35F5C80D216F.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	D87A3441-42E7-470D-8213-35F5C80D216F.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:	682622
Start date and time:	2022-08-11 19:29:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	actionplan doc 08.11.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, 52.109.12.24, 52.109.76.36
- 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\D87A3441-42E7-470D-8213-35F5C80D216F

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):	5.358147427520502
Encrypted:	false
SSDEEP:	1536:9cQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:s1Q9DQe+zuXYr
MD5:	4582F5FAFB337D9880EE6CC198D3BDE6
SHA1:	AD377A39C53710BAAAD5469225E0405416DF6964
SHA-256:	DC19BED1A1ED161E8CEFF63CCED101D42D5EC3DBC5F82296F969BEBD35738D69
SHA-512:	E6A5B5F27FBF3F4A2D8FD5FAA17C3D061FFFF608D87BBD4808245329D80CAF951B4D69FD6FC382C9B7726A85C2250A8AF42F69F4ACC48E0DE189048A3ABAF093
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="2022-08-11T17:30:28">.. 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\541FF1C0.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):	256042
Entropy (8bit):	7.978343657002507
Encrypted:	false
SSDEEP:	6144:SD1K9VMjF68qkupr4FNRfRglzGWMOM+lQzPyWae2q:SDEVJBXkR63MWQOHq
MD5:	303B22B7FFAF96496093E5DB3938B563
SHA1:	672080C107AACED7AB0D77E5AA3055ECBFA494DC
SHA-256:	AEF779CE0BA64FA155A6867374198754FCADABCBEB5C378A67A6B6846B18F0BB
SHA-512:	49FD4F26EA3DCE9742D0E5C134C30EB535C58F0B42458AABF546FDD5C053845FC62C65B87AA99478A754A00146BAAA0A0088E926CABB7EE2E8FBDD2F6DEBA368
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!...!.....IDATx^....fGU.s..8.3...?.3.hh..JTD%....$}#\U ..($!..&.HB.ol'!.`"i...\lE..d...r....9}O.5..<...[{.^]..... K..j.U.j.Z...~....+<`..=$...X.....|.....q..$2./....1..u...V^OF.N.W....z&_"...d....+*.t....Z.D.[.*#A.G.C...3..^.C..5.q.....`V.h.c`<.Z...23_..U^.?.Z....Un.f!.S..1.Y^i .Yo.o.....zH..'u.C.... I.Y.+. ...2..... ...V.U....OZ-...f... n.5...m,.zec..'j>.=...t"i...+*..+O-O.....Z..Z.D-...-.h.....6N..zy.}...W..g..v.j...1:.^un...r0..D.+..k....VdY.@....j.+k..j>..8.=.....^.m.VV/.<.....rH...[..m.... Q.U.t[.....:.....^..8.3]....-..I.h.....r..gl.j..@.W.D..m.$-.3..AK.|.....Y6.N.>.z.....+...*=...m.^...cu@..t....t...*.....~....1..+..'z.D-.t..D.ky{a.~...+#.].6.....z...O$...[^.%j].KW....-..r.,!.H.@M W....W...*.....j..h..A[...t..7..e-....k{..my.y.kH.h.h..5.D...6].h.U..3.C[..6.B-.}..X.!Q.c.v.Z.....=.D..tm7..L.M..|.l../.....V....8..c.....N..[Z.{m%.t.K.....|.m..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C0CEAFFB.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 636 x 613, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	113730
Entropy (8bit):	**7.990292786537194**
Encrypted:	**true**
SSDEEP:	3072:ShIiMUFV26oUc72Dl+oj/Yc6oGqdxVJw0c8N2mirB0VZp:ShMggmEceUi8N2miK/
MD5:	E0B30095BE35E9494E5073277D4FC1A1
SHA1:	19D39B036989A331F5389E377FBE565436599894
SHA-256:	EA952A68D25232D981CDBE0CD6DA947A9386D4BFFD5D1BE2EF80C4A1246AC3E2
SHA-512:	A524907D5D60AA77DB0BA3A3BF114EA7F8AEA9190ADAA84A0C78F96EC8E333AB124D68C84863E83E735D602117B0F3422746C9C4A0D6823CC8B51B652C41977E
Malicious:	false
Reputation:	moderate, very likely benign file

Preview:	.PNG.....IHDR...|...e.....V.R.. .IDATx.....4.....~.:..t."...$.....d..+...%Y.,V.(...7...03""".O.....?>..y.}.v.&u.....?0.....g.NH.....F...$..H.....km.%"D .=.f;.....A....O..w ..,"n...U....N~?".....'...7w)A..l.+.....7....q|..q.7?.....v.f...6....x._<.On.WLm..>s<.-.....".....".._..~a....f=..7.....P.~...,gD..:.P..,.*.....c...;.B...q..1.>|.....R.7m...7.....,".p7%. M.":...9..P.8.!..?.... .)".....A..Z..rA.).g.7..'QD.....@$.....*..oC. .6w...lP...lN..1X...H.....q....X{.s..A.....w..l....l`..t.C87.p.k...H>r...),..n...Dd.R.c..xHs.nWv.....>.j.WCi.. .....a...}.t\_....A.q..t..^A..Q..g,...P.h.n.nm....7....YYT.....jl.....yR>s...w.....|.z..L.....\.FP.....QG...0.....2...@T.*....C.....M...;...i....Y8...R.Y*....~.;.CA.....q....6`.....~.....2.g."... ../..{x.(...o..p...YW&+//[.....]....h....s....&...m_.)tG...s....<...].R..w..!.....A;.....I.,\.I@...&.....0[.\a?..`.#2upVW.4.{..c.JMZ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{34D97BE2-6C3D-4A31-9A42-1C2930589F97}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{5481821B-5863-4C7A-B07B-A94021ED3E0F}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.131668560158345
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82lakwkvHl7ltlHllGlwZZ9/vlk:4LG1ND9Pxn82Ykr2
MD5:	025EBE58F9C92597094D86E039A32D58
SHA1:	D73979ED793C0A2A5BBB4AE7CBCE87D0D0973F88
SHA-256:	8EB62112275DABF61C8A732F94C221C2936FB70C59400691BC7D5033F630CCFA
SHA-512:	E9620FC1E4749F6DBE815962994FE81BD2A740E22F7D95B7B2DF96F79E1E3A9FF2F2A0DD74B02FABC56B169A426F8C8C13490212D335740C117D7A5DE9AA7FF 6
Malicious:	false
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\Temp\~DFB9753BB74160ACC2.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):	4.443054133900035
Encrypted:	false
SSDEEP:	768:V877j9RRcJwpgUU1WhQLpCY3PFzk0FyNt:avDRcqpdOWhQIY/
MD5:	BFCAF8C73B6D8C5066D7F24701F0EE46
SHA1:	9AAE0FF40B0D8C153821B78850CEC520B9384252
SHA-256:	E7B12BDA7ADA8E9A4986AC19889F0097BA45A55868C3A4412568C11A2DF94D46
SHA-512:	82B5742BEA5C63622BEBBF31EECAC53803764EBC5C353809D84703BFBD87226AF262ECA1D33DDB60C95201D3E0B447BA629E028880777C416C89E2AD7EB41A 64
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\actionplan doc 08.11.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 15:31:51 2022, mtime=Fri Aug 12 01:30:30 2022, atime=Fri Aug 12 01:30:23 2022, length=2255878, window=hide
Category:	dropped
Size (bytes):	1105
Entropy (8bit):	4.728372674090069
Encrypted:	false
SSDEEP:	12:82C5U6gcuElPCH28+HhEYeRF+WGdppK6w4JjAM/+Px2la96w4JDBVz5VN4t2Y+x4:8bgh+BxdqCAMGPx2U+DTzLf7aB6m
MD5:	C30CC9DF59856DA55386307A74B29BFA
SHA1:	C351F45B549A94AF7CE61D1A290EBC60798D6E61
SHA-256:	0C639BE5480FAF3DFB60483792E03D6F773BD1491BC15A2365ABB1FA76607603
SHA-512:	2A28CB424830873B97863DEDCABA7A58308120E5340D0FB2673FFC07431E3CC16B3730D099C087D692934D08EE27486E6C9ACE9A132DFC4DE6E4C37758CB3AD
Malicious:	**true**
Preview:	L.....F.... .....'..3...{.}.....Ly....l".....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.....d#..h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..U.....Y.....>.....z..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9...~.2..l"..U.. .ACTION~1.DOC..b.....hT...U.....h.....i...a.c.t.i.o.n.p.l.a.n. .d.o.c. .0.8...1.1...d.o.c.....^.....-.....]....>.S.....C:\Users\user\Desktop\actionplan doc 08.11.doc../.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.a.c.t.i.o.n.p.l.a.n. .d.o.c. .0.8...1.1...d.o.c.....:..,.LB.)...As...`.....X.....936905.....!a..%.H.VZAj...F.....-..!a.%.H.VZAj...F.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	99
Entropy (8bit):	4.603745323857137
Encrypted:	false
SSDEEP:	3:bDuMJlcGHQpxU4dzCmX1JdQpxU4dzCv:bCfxFdzwxFdzs
MD5:	6F46005AE28DCF91A0D2E8B1C5CC2836
SHA1:	576E750FA407E8C607E0EA7D7BCBCECDF870CC8E
SHA-256:	D5D7E37F9B82ADDA77309B477841C70E1149867892550D83932EBFAF62838C1D
SHA-512:	1C84AEAF7A9F4C94E9E15EF077D51944E624CC18B8F897B8F7446C72C892F6369018B13C314AAD088E9E7741A1F32F7B5A3A9BEF5D490A0CC8AC438E552A1658
Malicious:	false
Preview:	[folders]..Templates.LNK=0..actionplan doc 08.11.doc.LNK=0..[doc]..actionplan doc 08.11.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):	2.218887756988307
Encrypted:	false
SSDEEP:	3:Rl/ZdLYHlqK9LtljlqK5Iddtr:RtZRYImbUiIddB
MD5:	271404C277BE351846F1D2E391194A8A
SHA1:	1659AFB75C2891123C311854DD3B0ED67B128C63
SHA-256:	AB3149234C6FC6B172CE41CA125F4D5340F36ECD8DED607F784D7856B5885165
SHA-512:	EC9A2DA1C61266005CBF4D1BF7ABEF1D70FC60F79C27F9D9689E038867C29792551B41EE43587B7A6909257DB6DA9CD09CB157A7B6342930737C702B1DE7CAE
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....dG.e.....$.....6C.....G.e.....H.....6C.....G.e.....

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\~$tionplan doc 08.11.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.218887756988307
Encrypted:	false
SSDEEP:	3:Rl/ZdLYHlqK9LtljlqK5Iddtr:RtZRYImbUiIddB
MD5:	271404C277BE351846F1D2E391194A8A
SHA1:	1659AFB75C2891123C311854DD3B0ED67B128C63
SHA-256:	AB3149234C6FC6B172CE41CA125F4D5340F36ECD8DED607F784D7856B5885165
SHA-512:	EC9A2DA1C61266005CBF4D1BF7ABEF1D70FC60F79C27F9D9689E038867C29792551B41EE43587B7A6909257DB6DA9CD09CB157A7B6342930737C702B1DE7CAE
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....dG.e.....$.....6C.....G.e.....H.....6C.....G.e.....

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.99386898063047
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:	actionplan doc 08.11.doc
File size:	2349822
MD5:	933338ca2c25cfda5c124455216d6709
SHA1:	e518d12b7bb4addf1dc041a05575031890c1b4d7
SHA256:	abc8d1097f0249c749f2c7d7058be1b39c88e21d26d45d76985c989289565214
SHA512:	57d89f7b2319e6725bc72e06b3e00b13b4e23445a723bb84fc3d0d199b8546b7e30de68c4b90a3244aaad7b974c3e6bbe8695ab0cacac8aef18ccceae3c741c5
SSDEEP:	49152:4ek4NG5JJHbICOlcYIHMwvTXaZ4D18AnhBmqB8Rplib7IFysec7htI:rkV5JJ7ILlcYIHTvTX/15v9bZFyseghi
TLSH:	ACB5337CC120B149C3363F5C594A05B98C9F5E67F7C498395E2F680AE56EA2A4ED0ACC
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/682622/sample/actionplan doc 08.11.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: 2879	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2879
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 / , . . . - . . . .) .
Data Raw:	01 1f 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:	5.2699223718129895
Base64 Encoded:	True
Data ASCII:	I D = " { 8 C 3 6 5 0 1 C - 8 4 9 B - 4 4 8 9 - 8 3 5 7 - D 4 0 B 9 9 7 E 0 0 E 4 } " . . 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 = " C 0 C 2 7 1 7 7 7 5 7 7 7 5 7 7 7 5 7 5 7 7 5 " . . D P B = " 8 0 8 2 3 1 3 2 3 2 3 2 3 2 3 2 " . . G C = " 4 0 4 2 F 1 F 2 F 2 F 2 F 2 0 D " . . . . [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 38 43 33 36 35 30 31 43 2d 38 34 39 42 2d 34 34 38 39 2d 38 33 35 37 2d 44 34 30 42 39 39 37 45 30 30 45 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:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

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

General	
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:	1.9285410655228268
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . P . . . . . " . . . . . q . . . . . A . . . . . ` . . . . . ` i . . . . .
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 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:	2.6979594211082003
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . P . . . . . p . . . . . 1 . . . . . ` . 1 . . . . . , . . p . . . . . q . . . . . Q . . . . . ` . . . . . 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 ff 00 00 00 00 78 00 00 00 08 00 50 00 c1 08 00 00 00 00 00 00 00 00 00 00 00 00 04 70 08 00 fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 486	
General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	486
Entropy:	6.304584198764293
Base64 Encoded:	True
Data ASCII:	. . . . . 0 . . . . . H . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . 0 S d - . . . " . < . . . . r s t d o . l e > . . s . t . . d . o . l . e . (. . h . . ^ . * \ \ . G { 0 0 0 2 0 4 3 0 - . . . . C . . . . . 4 6 } # 2 . 0 # . 0 # C : \ \ W i n . d o w s \ \ s y s @ t e m 3 2 \ \ . e 2 . . t l b # O L E . A u t o m a t . i o n . E N o r (m a l E N C r . m . a F . . c E C . . . . . m . ! O f f i c g O . f . i . c g . . g 2 D F 8 D 0 . 4 C - 5 B F A
Data Raw:	01 e2 b1 80 01 00 04 00 00 00 03 00 30 aa 02 02 90 09 00 20 14 06 48 03 00 a8 80 00 00 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 00 08 06 12 09 02 12 80 30 53 f4 64 2d 00 0c 02 22 0a 3c 02 0a 16 02 72 73 74 64 6f 08 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 00 28 0d 00 68 00 11 5e 00 03 2a 5c 00 47 7b 30 30 30

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 19:30:35.760811090 CEST	49740	80	192.168.2.3	45.8.146.139
Aug 11, 2022 19:30:38.776093006 CEST	49740	80	192.168.2.3	45.8.146.139
Aug 11, 2022 19:30:44.776688099 CEST	49740	80	192.168.2.3	45.8.146.139

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: **6108**, Parent PID: **756**

General

Target ID:	0
Start time:	19:30:24
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:	0x320000
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\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\yDF4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14A246AB	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	14A26626	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	14A26626	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	14A26626	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	14A26626	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	14A26626	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	14A26626	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	14A26626	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	14A26626	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	14A26626	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	14A26626	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	14A26626	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	14A26626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C0CEAFFB.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\541FF1C0.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\~DFB9753BB74160ACC2.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\yDF4.tmp	success or wait	1	14A24702	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DFB9753BB74160ACC2.TMP	success or wait	1	65975805	unknown
C:\Users\user\Desktop\~$tionplan doc 08.11.doc	success or wait	1	65975805	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C0CEAFFB.png	0	65536	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 7c 00 00 02 65 08 02 00 00 00 fd 56 fd 52 00 00 20 00 49 44 41 54 78 fd fd fd fd fd 34 0a fd fd fd fd fd fd 7e fd fd 3a fd fd 74 fd 22 fd fd 03 24 04 fd fd fd fd fd 64 fd fd 2b fd fd fd 25 59 1f 2c 56 01 28 fd fd fd 37 0d 54 fd 30 33 22 22 22 00 fd 4f fd fd fd fd fd fd 3f 3e fd fd 79 fd 7d fd 76 fd 26 75 fd 0f 1e fd ff fd 3f 30 fd fd fd 0d fd 67 fd 4e 48 fd fd fd fd fd db fd 0a fd fd 2e 1e 1c 46 fd fd fd 24 00 00 48 1e 7f 18 fd fd 06 fd fd fd 6b 6d fd 25 22 44 20 fd 3d fd 66 3b fd fd 16 11 fd fd 06 fd ec fd 41 fd 1d fd fd 4f fd fd 77 fd fd 2c 22 6e a7 fd fd 55 fd fd 19 fd 4e 7e 3f 22 fd fd 0b fd fd 27 fd fd fd 37 77 29 41 fd fd 6c fd 2b fd fd fd 01 fd 37	PNGIHDR|eVR IDATx4~:t"$d+%Y,V(703"""'O?>y}v&u? 0gNH.F$Hkm%"D = f;AOw,"nUN~?"'7w)Al+7	success or wait	2	65975805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\541FF1C0.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 0b fd 66 47 55 fd 73 fd fd 38 fd 33 fd fd fd 3f fd 33 fd 68 68 fd 03 4a 54 44 25 fd 08 fd 08 24 7d 23 5c 55 20 fd fd 28 24 21 09 fd 26 10 48 42 2d 6f 49 27 21 fd 60 22 69 fd fd fd 5c 6c 45 01 fd 64 fd 09 08 72 45 fd fd fd 39 7d 4f fd 35 fd fd 3c fd fd fd 5b 7b fd 5e 5d fd fd fd fd fd 4b fd fd 6a 6a 55 fd 6a fd 5a fd fd fd 7e fd fd c0 fd 2b 3c 60 fd 09 3d 24 fd fd fd 58 1a fd 19 fd fd 7c fd fd fd fd fd fd 71 fd fd 24 32 0d 2f fd 6f aa fd 31 fd fd	PNGIHDR7sRGBgAMAa pHYs!!IDATx^fGUs83? 3hhJTD%$}#\U ($!&HBol'!` "i\lEdr9}O5<[{^]KjUjZ~+ <`=$X|q$2/1	success or wait	4	65975805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	6594765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	6594765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	end of file	1	6594765D	unknown
C:\Users\user\Desktop\actionplan doc 08.11.doc	1872006	184	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\2EAB5	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\2EAB5	2EAB5	binary	04 00 00 00 DC 17 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 2D AE E1 A0 F3 AD D8 01 B5 EA 02 00 B5 EA 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	2022-08-11T19:31	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_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358364678	1426784263	success or wait	1	6594765D	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	6594765D	unknown
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	6594765D	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\00006109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784263	1426784264	success or wait	1	6594765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784264	1426784265	success or wait	1	6594765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784268	1426784269	success or wait	1	6594765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784269	1426784270	success or wait	1	6594765D	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	6594765D	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	6594765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2EAB5	2EAB5	binary	04 00 00 00 DC 17 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 2D AE E1 A0 F3 AD D8 01 B5 EA 02 00 B5 EA 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	04 00 00 00 DC 17 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 B5 EA 02 00 B5 EA 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 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	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				

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

Disassembly

No disassembly