ID: 383148
Sample Name: Coronavirus pandemic.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:43:47
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

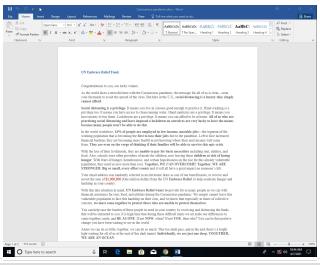
Analysis Report Coronavirus pandemic.docx

Overview

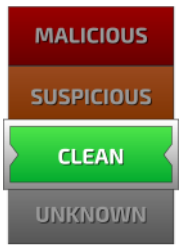
General Information

Sample Name:	Coronavirus pandemic.docx
Analysis ID:	383148
MD5:	8f525ec48db9a3c..
SHA1:	8b1792b84b7005..
SHA256:	42566c5d227dff8..
Tags:	docx
Infos:	

Most interesting Screenshot:



Detection

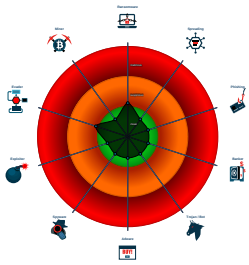


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 1008 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

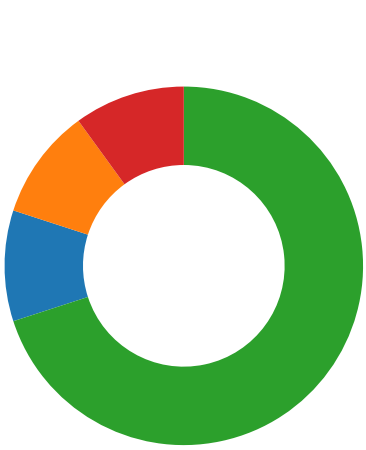
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



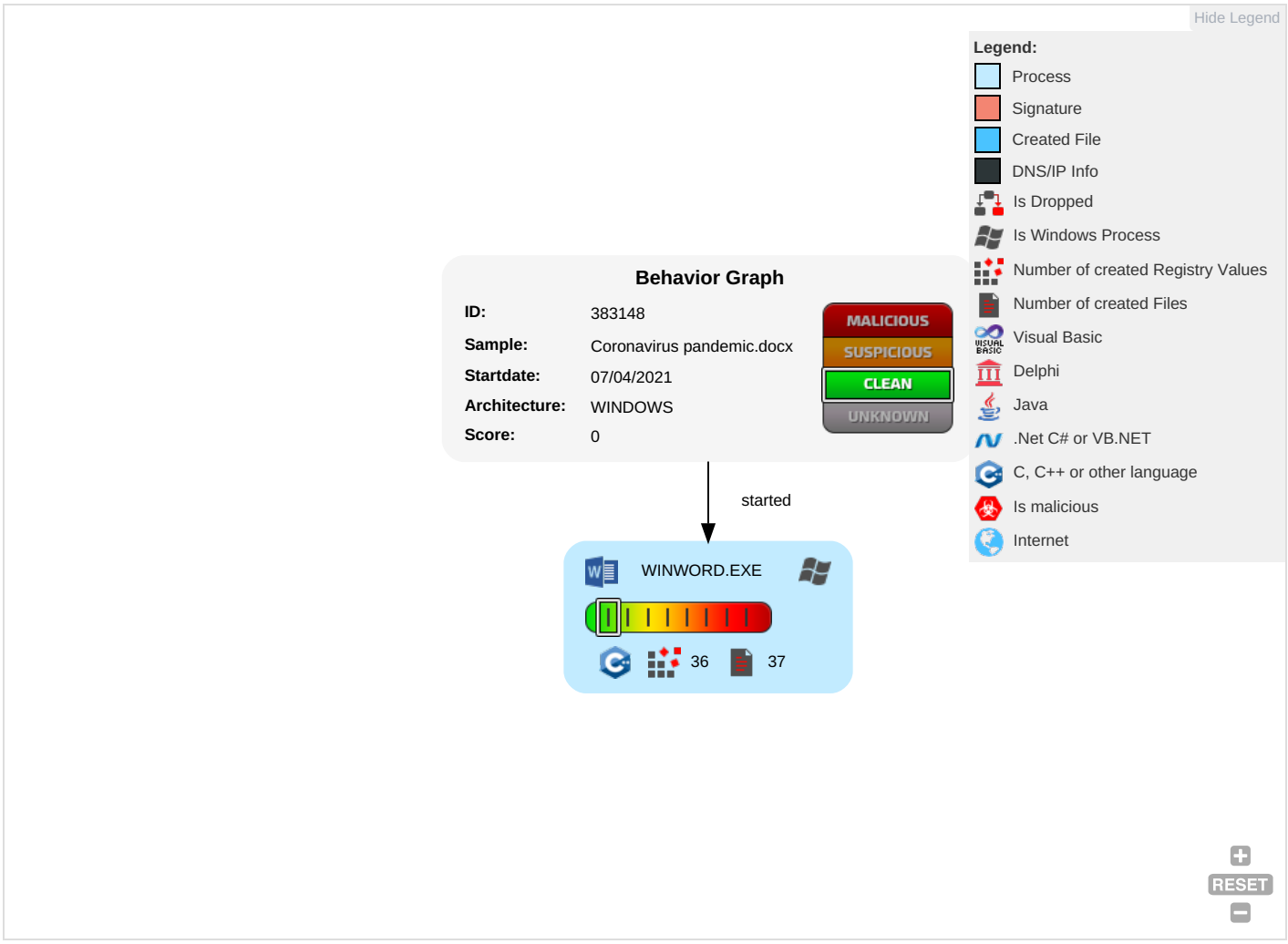
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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	Windows Management Instrumentation	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	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	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 1	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

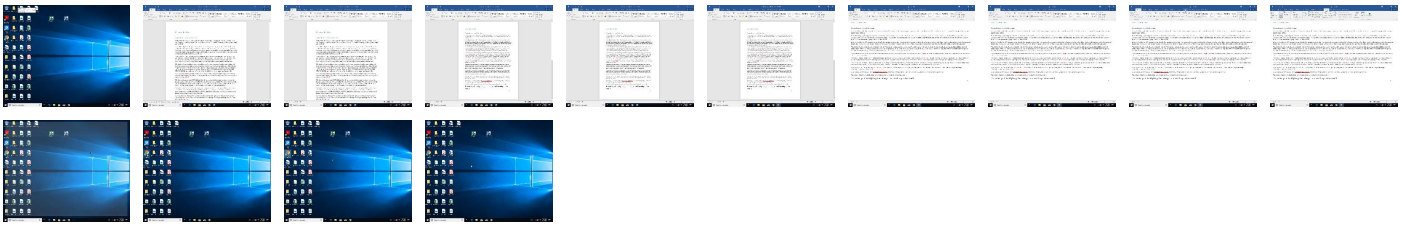
Behavior Graph

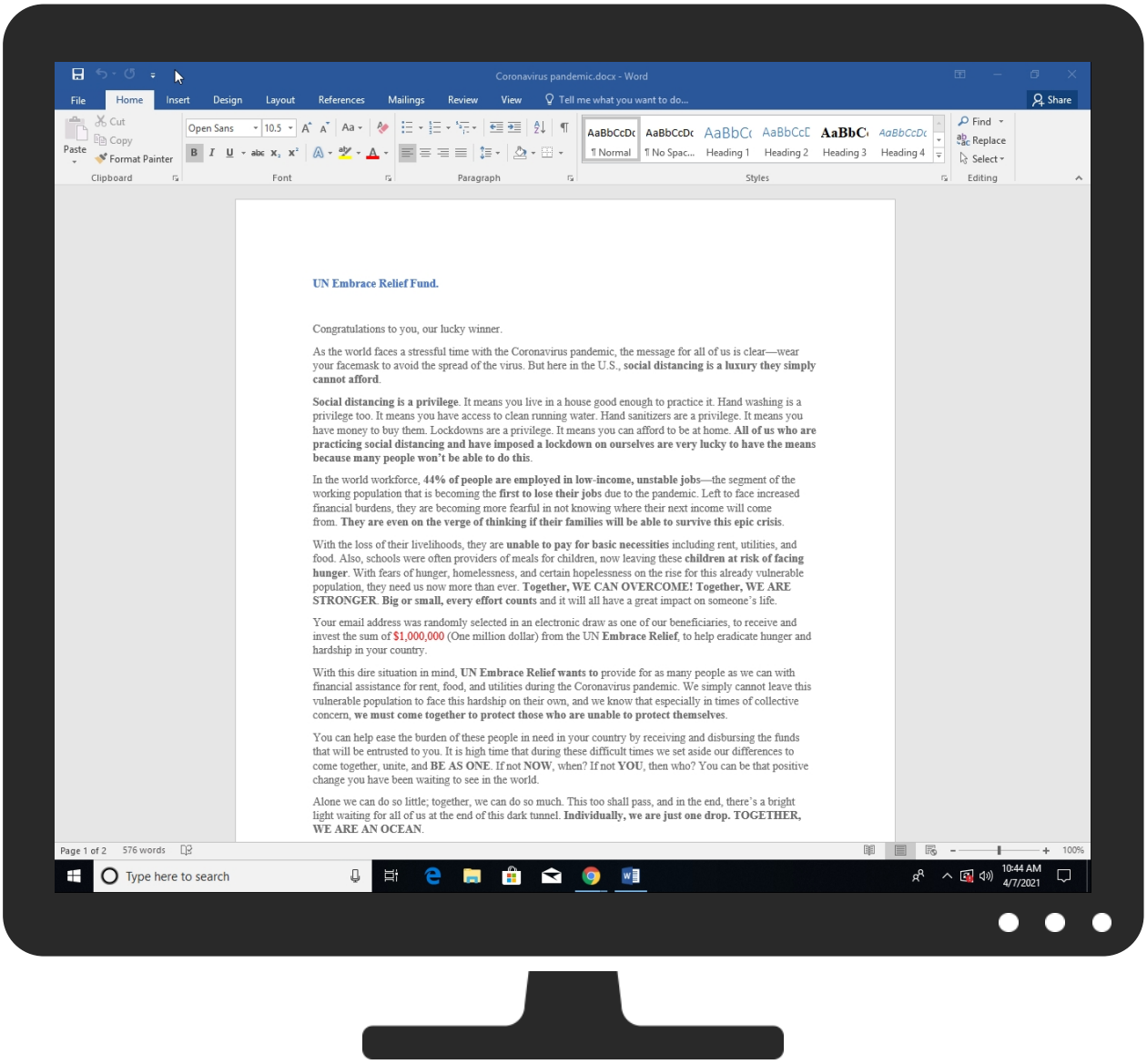


Screenshots

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
Coronavirus pandemic.docx	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	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://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	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://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.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://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	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://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	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://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	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	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	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	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://login.microsoftonline.com/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://shell.suite.office.com:1443	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://autodiscover-s.outlook.com/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://cdn.entity.	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://cortana.ai	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://api.aadrm.com/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://api.microsoftstream.com/api/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://cr.office.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://graph.ppe.windows.net	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://store.office.cn/addinstemplate	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev0-api.acompli.net/autodetect	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://web.microsoftstream.com/video/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://graph.windows.net	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://dataservice.o365filtering.com/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://ncus.contentsync.	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://weather.service.msn.com/data.aspx	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://apis.live.net/v5.0/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://management.azure.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://wus2.contentsync.	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://api.office.net	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://incidents.diagnosticssdf.office.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://entitlement.diagnostics.office.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://outlook.office.com/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://templatelogging.office.com/client/log	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://outlook.office365.com/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://webshell.suite.office.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://management.azure.com/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://devnull.onenote.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://ncus.pagecontentsync.	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://messaging.office.com/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://augloop.office.com/v2	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://skyapi.live.net/Activity/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://dataservice.o365filtering.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://directory.services.	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.windows-ppe.net/common/oauth2/authorize	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false		high
http://https://staging.cortana.ai	A354DBD0-A08D-422F-90A3-E85F18D7B7BE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383148
Start date:	07.04.2021
Start time:	10:43:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Coronavirus pandemic.docx
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:	18
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winDOCX@1/8@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 23.54.113.53, 204.79.197.200, 13.107.21.200, 40.88.32.150, 104.42.151.234, 52.109.88.177, 52.109.12.23, 52.109.8.25, 13.88.21.125, 104.43.193.48, 20.82.210.154, 95.100.54.203, 93.184.221.240, 51.103.5.159, 52.255.188.83, 104.43.139.144, 23.10.249.26, 23.10.249.43, 20.54.26.129, 20.50.102.62 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, nexus.officeapps.live.com, arc.trafficmanager.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, prod.configsvc1.live.com.akadns.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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\A354DBD0-A08D-422F-90A3-E85F18D7B7BE	
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):	133170
Entropy (8bit):	5.3710169286179985
Encrypted:	false
SSDEEP:	1536:TcQIeNquBXA3gBwqpQ9DQW+zAM34ZldpKWXboOilXNErLdME9:vVQ9DQW+zTXiJ
MD5:	514F7BF0F0A3FF8E9593EC5C557CB5FC
SHA1:	B49C00B20EFA49DE351C827036EDE3EC3AB8533F
SHA-256:	18F1C4509CAC7A843DED8EBBEBA87AD889EFB61C84285CB9EF5935C74FEC8E38
SHA-512:	60FD0595D09D5C3A19AB38D5B11327C43CA3909F62276C56760A0DB9D3EDD3E24310A94A5186B69E54DEC0AF092CD80CDCD2DB634CFDCA45E5A360CADE999C4
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="2021-04-07T08:44:32">.. Build: 16.0.13925.30526-->.. <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.Word\~WRS{099D4456-906F-4297-A267-395210B4A021}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	8704
Entropy (8bit):	3.643235732815873
Encrypted:	false
SSDEEP:	96:B/8txwIHlREaH5vWPW7wwn9VU0xrhSOn7q7xZjE/yCb3MiI15Gobr/eEBGP/YGc:5lIHlREaZe+7wwHRrUDHjE/yYA16c
MD5:	CD99CDBE1544840CCF72278CC477D9F0
SHA1:	E3BBB1829872159368BF3995BD6D208920084EDA
SHA-256:	641F11A0953210C7AAB002FD67255D7919FEA327A972DF417471DD78B4BC80B1
SHA-512:	2255DCF66CDEABB9FD17EC40837F500AFD97FFD8A7747B85E72B1396569317B5298C97051C20979AB38FF4BCB4E15D8A17240F2EBFE1D7908B8CBAF1184207CF
Malicious:	false
Reputation:	low
Preview:	..U.N. .E.m.b.r.a.c.e. .R.e.l.i.e.f. .F.u.n.d.....C.o.n.g.r.a.t.u.l.a.t.i.o.n.s. .t.o. .y.o.u.,. .o.u.r. .l.u.c.k.y. .w.i.n.n.e.r.....A.s. .t.h.e. .w.o.r.l.d. .f.a.c.e.s. .a. .s.t.r.e.s.s.f.u.l. .t.i.m.e. .w.i.t.h. .t.h.e. .C.o.r.o.n.a.v.i.r.u.s. .p.a.n.d.e.m.i.c.,. .t.h.e. .m.e.s.s.a.g.e. .f.o.r. .a.l.l. .o.f. .u.s. .i.s. .c.l.e.a.r.. w.e.a.r. .y.o.u.r. .f.a.c.e.m.a.s.k. .t.o. .a.v.o.i.d. .t.h.e. .s.p.r.e.a.d. .o.f. .t.h.e. .v.i.r.u.s... .B.u.t. .h.e.r.e. .i.n. .t.h.e. .U...S...,...s.o.c.i.a.l. .....2...6.....f... ...X...f...H...~...h...<...~...D.....gd{}b.....$..d.....9D..a$.gd{}b.....dh.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{B6869D89-96E9-49F0-B15B-63F168951986}.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{B6869D89-96E9-49F0-B15B-63F168951986}.tmp	
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\mso6491.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlrojAxh4bxdtT/CS3wkxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWKbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A
SHA-512:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA87841
Malicious:	false
Reputation:	high, very likely benign file
Preview:	GIF89a....w..!..MSOFFICE9.0.....sRGB.....!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3.!..MSOFFICE9.0.....cmPPJCmp0712.....!.....,.....'.:,..b...RQ.xx.....,+.....yy..;..b.....qp.bb.....uv.ZZ.LL.....xw.jj.NN.A@....zz.mm.^_.....yw.....yx.xw.RR.,*.++.....8....>.....4567...=.../0123.....<9:.()*+,-.B.@...."#$%&'..... !.....C.?....A;<...HT(..;

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Coronavirus pandemic.docx.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=Wed Sep 30 14:03:41 2020, mtime=Wed Apr 7 16:44:32 2021, atime=Wed Apr 7 16:44:30 2021, length=15421, window=hide
Category:	dropped
Size (bytes):	2220
Entropy (8bit):	4.728089787574786
Encrypted:	false
SSDEEP:	48:8NvfRNPjwRHnLaB6pNvfRNPjwRHnLaB6:8pvwFnLaKpvwFnLa
MD5:	04C80E81AA3FCE7AAFBF73DCE4A5C149
SHA1:	0A7FE0B08BD09B13246FA82EDBBF904463073CC3
SHA-256:	289FC694520CE57851F80F0537ACCDA417A86C20E32F4C40CF19FC4944A1FDA4
SHA-512:	8D1D4A17CFE327AB659A743D32AB05A48C8F152ABCC276D699C27EFD578987B9C46DCF6B4D26633B867A41F6ACE75ADC6C1E8B5F428572878BF81307BF36B92
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....j.:....p...+...p]..+..=<.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....q\..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny..R.....S.....Y.N.h.a.r.d.z.....~.1.....>Qwx..Desktop.h.....Ny..R.....Y.....>.....6.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.=<...R.. .CORONA~1.DOC..d.....>Qux.R.....h.....=.-.C.o.r.o.n.a.v.i.r.u.s. .p.a.n.d.e.m.i.c...d.o.c.x....._.....-.....^.....>.S.....C:\Users\user\Desktop\Coronavirus pandemic.docx..0....\....\....\....\....\.D.e.s.k.t.o.p.\.C.o.r.o.n.a.v.i.r.u.s. .p.a.n.d.e.m.i.c...d.o.c.x.....:..,.LB.)...As...`.....X.....035347.....!a..%.H.VZAj...}..-.....-..!a..%.H.VZAj...}..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2

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):	115
Entropy (8bit):	4.570921251306772
Encrypted:	false
SSDEEP:	3:HtDiBVS+LviBVSmxWtDiBVSv:Ht2V7qVg2Vc
MD5:	3ED8DDC4884897984D431AAACAB9E082
SHA1:	B3D049D3771F3F8E5CF3D4F62DE40BCB30A04FC1
SHA-256:	D41A55313423DA59273B0A0E25E3C8EF34F6470EAC164BB3C6B95484C5A995D8
SHA-512:	CCA1CF36A8DE4488AAA86EB298AE7D5857C7274D44FD7BE2C4CE1577C762F34CDC1C99AB6398D4506FFFF078027BAF8081445FEB7BFD00CCC1C81643D994D7B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Preview:	[misc]..Coronavirus pandemic.docx.LNK=0..Coronavirus pandemic.docx.LNK=0..[misc]..Coronavirus pandemic.docx.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):	3.2806617440194796
Encrypted:	false
SSDEEP:	3:Rl/Zd+LE7VlXtlSL19ilxV3AmLU+gn:RtZaEhW6h7gn
MD5:	8F992AA56A789704E97825360E6ACC04
SHA1:	72F49894D4FCA8CB6500A72DEB0D88443B9B1011
SHA-256:	A0DF478FF7FD9C95C8CA6EC4E5C2188F69F799DF1ED39F7C392123A81F9370E4
SHA-512:	130B4CC8BD3EE1764C54DD70F311F0D5CA03C50ADE7C66B7AC0A873B76FF001FCC612423AB94235B255E1DAFBAE9B1D3E7E6023F149CE49ECED330D1CAED35E
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....^.j@..jT..j`..jDB.jZR.j.....8.9.8.9.8.9.

C:\Users\user\Desktop\~$ronavirus pandemic.docx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.2806617440194796
Encrypted:	false
SSDEEP:	3:Rl/Zd+LE7VlXtlSL19ilxV3AmLU+gn:RtZaEhW6h7gn
MD5:	8F992AA56A789704E97825360E6ACC04
SHA1:	72F49894D4FCA8CB6500A72DEB0D88443B9B1011
SHA-256:	A0DF478FF7FD9C95C8CA6EC4E5C2188F69F799DF1ED39F7C392123A81F9370E4
SHA-512:	130B4CC8BD3EE1764C54DD70F311F0D5CA03C50ADE7C66B7AC0A873B76FF001FCC612423AB94235B255E1DAFBAE9B1D3E7E6023F149CE49ECED330D1CAED35E
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....^.j@..jT..j`..jDB.jZR.j.....8.9.8.9.8.9.

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.360605033888312
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:	Coronavirus pandemic.docx
File size:	15421
MD5:	8f525ec48db9a3caea17354f5113beb8
SHA1:	8b1792b84b70053532ab34b8d62659d1d531affc
SHA256:	42566c5d227dff870976653176f6497eef50bbc0397b8c0507c2801e38ac210a
SHA512:	446a73cd4e72488f1e22831350b6e5ffa43865d36d26e37727a112356b156e9255d6f95cacf3b96b120cff9d227a6ae2a85435063ed822e06fd65535a6d69c74
SSDEEP:	384:dzqi+t8BXgzhCtjn0i13LupzomoI3ntH3Qr+:oigIgQDv13KV/oI1P
File Content Preview:	PK.....!.2.oWf.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:44:23.899863005 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:23.926371098 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:23.978290081 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:23.997157097 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:27.797558069 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:28.806674957 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:28.822088957 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:29.808037043 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:29.822516918 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:30.838164091 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:30.854443073 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:32.094667912 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:32.156312943 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:32.522908926 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:32.556086063 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:33.525691032 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:33.567181110 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:33.833544016 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:33.846781015 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:34.525604010 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:34.541420937 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:35.044347048 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:35.057980061 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:36.541465044 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:36.562011957 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:38.557693005 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:38.571228027 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:39.836117029 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:39.850241899 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:40.557315111 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:40.571409941 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:41.052516937 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:41.067276001 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:51.641535997 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:51.662220001 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:57.752062082 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:57.767802954 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:58.871625900 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:58.883958101 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 7, 2021 10:44:59.629125118 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:44:59.651604891 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 7, 2021 10:45:22.588392973 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:45:22.589734077 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:45:22.608077049 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 7, 2021 10:45:22.611449003 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 7, 2021 10:45:22.656389952 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:45:22.669035912 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 7, 2021 10:45:23.208421946 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:45:23.220789909 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 7, 2021 10:45:34.513078928 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:45:34.525424957 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 7, 2021 10:45:35.224879026 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:45:35.239613056 CEST	53	50540	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:45:36.232712984 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:45:36.245291948 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 7, 2021 10:45:38.936172009 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:45:38.949873924 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 7, 2021 10:45:45.586119890 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:45:45.599395990 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 7, 2021 10:45:46.897816896 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:45:46.910204887 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 7, 2021 10:45:50.237365007 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:45:50.250327110 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 7, 2021 10:45:52.273396015 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:45:52.291496992 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 7, 2021 10:45:58.088119984 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:45:58.114355087 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 7, 2021 10:46:22.954149008 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 7, 2021 10:46:22.968173981 CEST	53	56579	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 1008 Parent PID: 792

General

Start time:	10:44:30
Start date:	07/04/2021
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:	0x90000
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	66B8977C	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$ronavirus pandemic.docx	success or wait	1	66AB5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Coronavirus pandemic.docx	2049	261	success or wait	1	66AB5805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	66AC8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	66AC8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	66AC8A84	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1D618	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	66AB5805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1D618	1D618	binary	04 00 00 00 F0 03 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 00 01 00 00 00 00 00 00 00 00 46 90 21 BC D5 2B D7 01 18 D6 01 00 18 D6 01 00 00 00 00 00 DB 04 00 00 02 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	success or wait	1	66AB5805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2021-04-07T10:45	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	66AB5805	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\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1384579087	1384579088	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1384579088	1384579089	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	WordPerfect 5.x	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	WordPerfect 5.x	WordPerfect 6.x - 7.0	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT632.CNV	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	doc	wpd doc	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1D618	1D618	binary	04 00 00 00 F0 03 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 46 90 21 BC D5 2B D7 01 18 D6 01 00 18 D6 01 00 00 00 00 00 DB 04 00 00 02 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	04 00 00 00 F0 03 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 18 D6 01 00 18 D6 01 00 00 00 00 00 DB 04 00 00 02 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	success or wait	1	66AB5805	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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			Source	
Key Path	Name	Type	Old Data	New Data	Completion	Count	Address	Symbol

Disassembly