ID: 417616
Sample Name: Claim Covid Tvx - Bandoir PBR.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:16:41
Date: 19/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

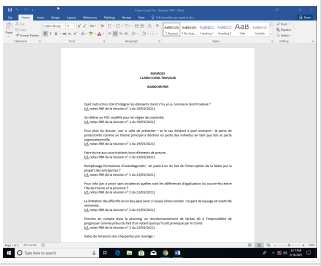
Analysis Report Claim Covid Tvx - Bandoir PBR.docx

Overview

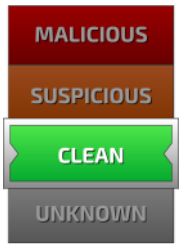
General Information

Sample Name:	Claim Covid Tvx - Bandoir PBR.docx
Analysis ID:	417616
MD5:	405825f6d97456d.
SHA1:	74a879ae98debb..
SHA256:	3d6b6526bbc916..
Infos:	

Most interesting Screenshot:



Detection

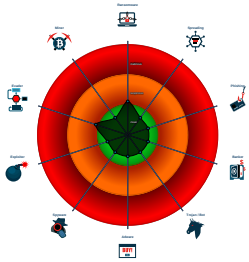


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 6248 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

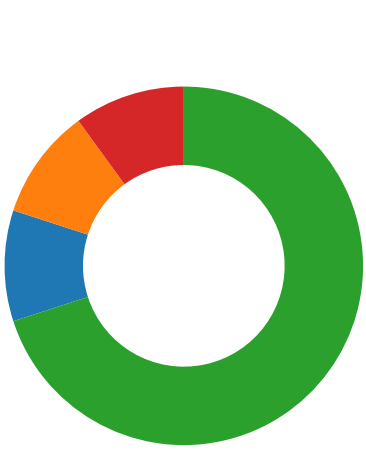
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



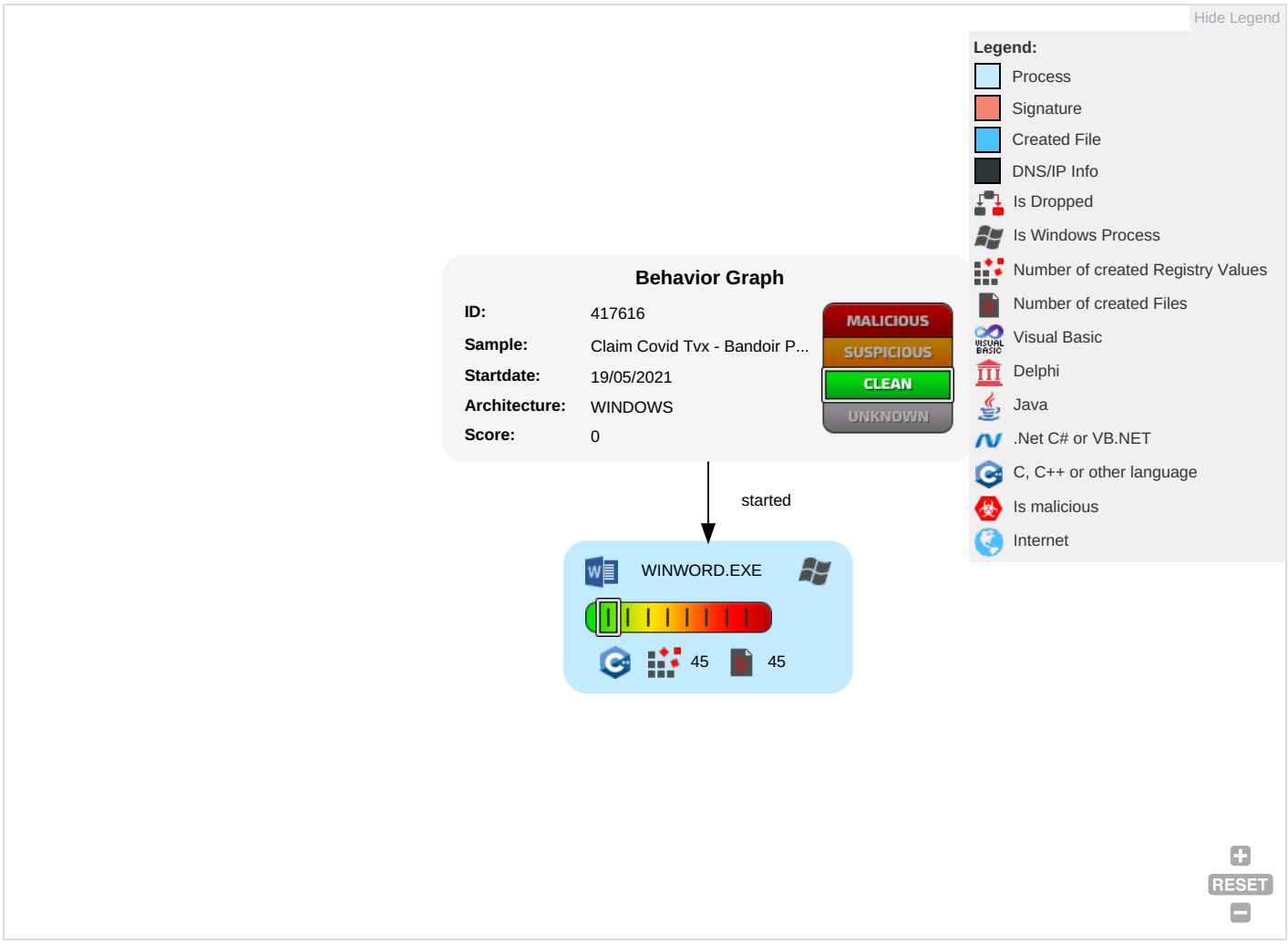
Click to jump to signature section

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

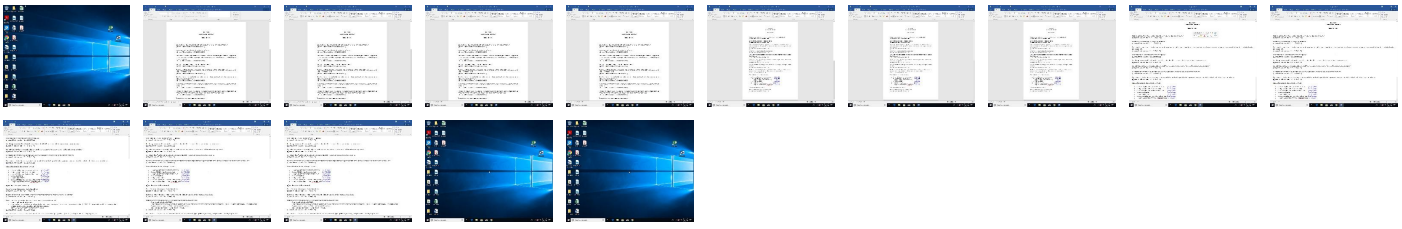
Behavior Graph

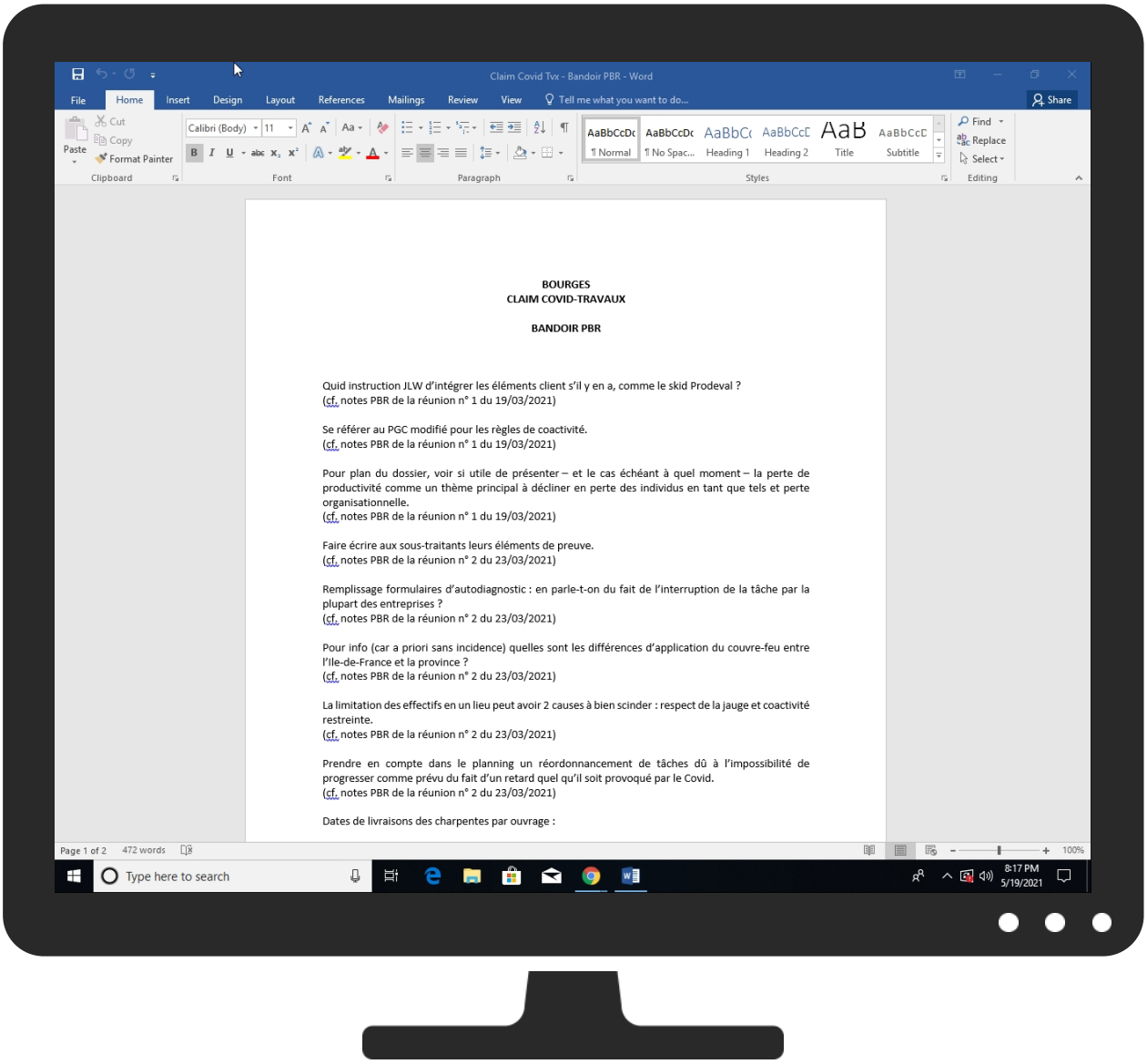


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

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	
http://https://powerlift.acompli.net	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://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	
http://https://wus2.contentsync.	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://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	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://login.microsoftonline.com/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://shell.suite.office.com:1443	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://autodiscover-s.outlook.com/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://cdn.entity.	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://cortana.ai	017E6514-9C86-422D-A14F-55B0CD085360.0.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	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://api.aadrm.com/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://api.microsoftstream.com/api/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://cr.office.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://graph.ppe.windows.net	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://store.office.cn/addinstemplate	017E6514-9C86-422D-A14F-55B0CD085360.0.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=	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	017E6514-9C86-422D-A14F-55B0CD085360.0.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	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://web.microsoftstream.com/video/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://graph.windows.net	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://dataservice.o365filtering.com/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://ncus.contentsync.	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://weather.service.msn.com/data.aspx	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://apis.live.net/v5.0/	017E6514-9C86-422D-A14F-55B0CD085360.0.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	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://management.azure.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://wus2.contentsync.	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://api.office.net	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://incidents.diagnosticssdf.office.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://entitlement.diagnostics.office.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://outlook.office.com/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://templatelogging.office.com/client/log	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://outlook.office365.com/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://webshell.suite.office.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://management.azure.com/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://devnull.onenote.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://ncus.pagecontentsync.	017E6514-9C86-422D-A14F-55B0CD085360.0.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	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://messaging.office.com/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://augloop.office.com/v2	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://skyapi.live.net/Activity/	017E6514-9C86-422D-A14F-55B0CD085360.0.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	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://dataservice.o365filtering.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://directory.services.	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false		high
http://https://staging.cortana.ai	017E6514-9C86-422D-A14F-55B0CD085360.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	417616
Start date:	19.05.2021
Start time:	20:16:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Claim Covid Tvx - Bandoir PBR.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:	22
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@1/10@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): 204.79.197.200, 13.107.21.200, 104.42.151.234, 93.184.220.29, 20.82.210.154, 92.122.145.220, 168.61.161.212, 52.109.88.177, 52.109.12.21, 52.109.8.22, 52.109.76.36, 184.30.24.56, 84.53.167.113, 13.107.5.88, 13.107.42.23, 51.103.5.159, 93.184.221.240, 20.82.209.183, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, ocsp.digicert.com, wildcard.weather.microsoft.com.edgekey.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, afdo-tas-offload.trafficmanager.net, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net, prod-w.nexus.live.com.akadns.net, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, e15275.g.akamaiedge.net, l-0014.config.skype.com, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, cs11.wpc.v0cdn.net, arc.trafficmanager.net, nexus.officeapps.live.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, config.edge.skype.com, client.wns.windows.com, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, prod.configsvc1.live.com.akadns.net, wu.ec.azureedge.net, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, config.officeapps.live.com, l-0014.l-msedge.net, skypedataprdcolwus16.cloudapp.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\017E6514-9C86-422D-A14F-55B0CD085360	
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):	134818
Entropy (8bit):	5.369478569328462
Encrypted:	false
SSDEEP:	1536:ecQIKNEgBXA3gBwlpQ9DQW+zjh34ZldpKWXboOilX5ErLWME9:YEQ9DQW+zNXO8
MD5:	898376A3D63649A3057898D3AE7F677C
SHA1:	545966E6F427D2ADCC2DB9B5707C3A3D807041D0
SHA-256:	32B3021822B2703E138DAFBBB40B3688E0A18FB3F6F2687E8681CE6D8F90C5ED
SHA-512:	768C495C11504955BDBC2C7232B95CF066257C689BA8D497E478213304A1F04BBA597816880D25FEE8EB4556E9D644ED90C57013D0F109D312D290B306869C2C
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="2021-05-19T18:17:32">.. Build: 16.0.14116.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{6D4EB022-1520-42A7-BC21-5CFC71D64976}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{EDB964CD-34DB-46C8-9731-E5F81802CF02}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	8118

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{EDB964CD-34DB-46C8-9731-E5F81802CF02}.tmp	
Entropy (8bit):	3.5683146808303308
Encrypted:	false
SSDEEP:	192:n0M0kmZMaLqMEDOAuO4ROHZOHV0Oe40no/6Qy6QEAKx6b:0UmZH+TyzRYo2/bngtyFEAc0
MD5:	7BEE0FE6548FC35A5B904CA17B71E4B7
SHA1:	0BF626F096104D23E97110FB101E5ADEAF567657
SHA-256:	A6F64C487CE1D78F1BDF7E7A088530CFF6A734E3E4A885E2794650C028285D2A
SHA-512:	2A2A1ADD516BB88F4390DB371729F3533482EBFDE1FE6555E1D59754BEA410A57C284FF1A4B6C6422FD78C2738A7BBD2ECC41AC5472FC4D49782610C9C6573
Malicious:	false
Reputation:	low
Preview:	..B.O.U.R.G.E.S...C.L.A.I.M. .C.O.V.I.D...T.R.A.V.A.U.X.....B.A.N.D.O.I.R. .P.B.R.........Q.u.i.d. .i.n.s.t.r.u.c.t.i.o.n. .J.L.W. .d.. i.n.t...g.r.e.r. .l.e.s. ...l...m.e.n.t.s. .c.l.i.e.n.t. .s.. i.l. .y. .e.n. .a.,. .c.o.m.m.e. .l.e. .s.k.i.d. .P.r.o.d.e.v.a.l...?...(.c.f.....n.o.t.e.s. .P.B.R. .d.e. .l.a. .r...u.n.i.o.n. .n.....1. .d.u. .1.9./.0.3./.2.0.2.1.).....S.e. .r...f...r.e.r. .a.u. .P.G.C. .m.o.d.i.f.i... .p.o.u.r. .l.e.s. .r...g.l.e.s. .d.e. .c.o.a.c.t.i.v.i.t.....(.c.f.....n.o.t.e.s. .P.B.R.....:...<...T...V...X...Z.....p...r.....F...H.....V...X.....0...0..... ....gd.....gdX1.....gdic.....

C:\Users\user\AppData\Local\Temp\msoA226.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:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA878 41
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\Claim Covid Tvx - Bandoir PBR.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 13:47:07 2020, mtime=Thu May 20 02:17:33 2021, atime=Thu May 20 02:17:30 2021, length=16919, window=hide
Category:	dropped
Size (bytes):	2320
Entropy (8bit):	4.73531712281555
Encrypted:	false
SSDEEP:	24:8/OcVYbwM8+MVANKVN48+MkDyl7aB6my/OcVYbwM8+MVANKVN48+MkDyl7aB6m:8mcVYbw/aNKDoB6pmcVYbw/aNKDoB6
MD5:	79E44D525E809EB1531C8DA524DB16BB
SHA1:	92A9AAD6E4FD271A2B5133583120DC0DB07A4F67
SHA-256:	3772B7F826E7099380E3A96E1927B8F3A65E89D29DA9743DA7D3BF3C3C64F98D
SHA-512:	75157B7A43637BC4DD0A2B72F15FD96AB4297E799DB31BA696234A07CE7872DCB88A8AFA819A5EB20C8A14D202B2396729D835E453B6C15601B1986FAC82929
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....8...r...&M.....&M...B.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...R*.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....T.1.....>Q.u..user..>.....NM..R*.....S.....'..a.l.f.o.n.s.....~.1.....>Q.u..Desktop.h.....NM..R*.....Y.....>.....s@-.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....2..B...R0. .CLAIMC~1.DOC..v.....>Q.u.R0.....f.....Kt..C.l.a.i.m. .C.o.v.i.d. .T.v.x. .-. .B.a.n.d.o.i.r. .P.B.R...d.o.c.x.....i.....-.....h.....> .S.....C:\Users\user\Desktop\Claim Covid Tvx - Bandoir PBR.docx..9.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.l.a.i.m. .C.o.v.i.d. .T.v.x. .-. .B.a.n.d.o.i.r. .P.B.R...d.o.c.x..... :..,.LB.)...Aw...`.....X.....287400.....!a..%.H.VZAj....Xt.+.....W...!a..%.H.VZAj....Xt.+.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1

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):	127
Entropy (8bit):	4.633463401585562
Encrypted:	false
SSDEEP:	3:Hto0IcBHfZul+o0IcBHfZulmxWto0IcBHfZulv:HtoxcB/QhxcB/QzoxcB/Q1
MD5:	26BE34E6054191E5EAA93606038A3C16
SHA1:	671BC0CDD872A1C10DB1A4D4EF884C59040CECEE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA-256:	2101CA14A43981BACFB60766DFB9ED0426DA3203C508F6CD4ADD2FC6E5058103
SHA-512:	8EE47E6679401C330A36EC7F295B606EFD060A88B9BB8719236D7279F1CCEAC1390D9774FD60039A75EA80B7BC32EE5256181CEB7780F2BF4DFFC5C7CB877C3 4
Malicious:	false
Reputation:	low
Preview:	[misc]..Claim Covid Tvx - Bandoir PBR.LNK=0..Claim Covid Tvx - Bandoir PBR.LNK=0..[misc]..Claim Covid Tvx - Bandoir PBR.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1806496452223483
Encrypted:	false
SSDEEP:	3:Rl/ZdsolABlqKZvl5lqKla4mpt5:RtZKoaOCvU+adD5
MD5:	988CD76BF07F70F9F185812CEC373448
SHA1:	66BA56234E07D532820E5CC2D1A51CF99B4E1448
SHA-256:	341D9C384B212D23F82944B5DA3A2649D72A2CA9EC806DA8C1A494104E69CE03
SHA-512:	1A74DC196E2267C148F79AE89AB0E8E41729E53053B45DA3B87C1F321F18B938C19B2C20135AB7502F310286D37544F8FC7BE675721AA8F32DE18C8580D268A4
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....8).M.%.....T.....6C.....<).M.&.....H.....6C.....).M.'.....$...

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3 342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryFR040c.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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$aim Covid Tvx - Bandoir PBR.docx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1806496452223483
Encrypted:	false

C:\Users\user\Desktop\~$aim Covid Tvx - Bandoir PBR.docx

SSDEEP:	3:Rl/ZdsolABlqKZvl5lqKla4mpt5:RtZKoaOCvU+adD5
MD5:	988CD76BF07F70F9F185812CEC373448
SHA1:	66BA56234E07D532820E5CC2D1A51CF99B4E1448
SHA-256:	341D9C384B212D23F82944B5DA3A2649D72A2CA9EC806DA8C1A494104E69CE03
SHA-512:	1A74DC196E2267C148F79AE89AB0E8E41729E53053B45DA3B87C1F321F18B938C19B2C20135AB7502F310286D37544F8FC7BE675721AA8F32DE18C8580D268A4
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....8).M.%.....T.....6C.....<).M.&.....H.....6C.....).M.'.....$...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.441952861067262
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:	Claim Covid Tvx - Bandoir PBR.docx
File size:	16919
MD5:	405825f6d97456d98d1620db5d1f8314
SHA1:	74a879ae98debb1449692440266e37738d2a7d72
SHA256:	3d6b6526bbc91680db4b6aac33f809bd1758c37be92c6a5193620011c74bcf5e
SHA512:	84d105938a5b92e54cc410f5d25f89d11c0e582492b50cd85d6edb8853bb07f305147b791b755c8e104256eb5d619bb090b922e32b90f647aa76ea3e2a61a9f5
SSDEEP:	192:jh04RPS8YGxTtIsERnKzYpkyAqiCyOA8MS48TuX63DWs9YeYmCAsxGnpX5fx/La/:dhVxT2ZNzAqi+AlVmCOndbDCzke
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
May 19, 2021 20:17:23.193439960 CEST	54302	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:23.233391047 CEST	53784	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:23.242609978 CEST	53	54302	8.8.8.8	192.168.2.5
May 19, 2021 20:17:23.266032934 CEST	53	53784	8.8.8.8	192.168.2.5
May 19, 2021 20:17:23.419303894 CEST	65307	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:23.454391003 CEST	53	65307	8.8.8.8	192.168.2.5
May 19, 2021 20:17:23.668441057 CEST	64344	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:23.701472998 CEST	62060	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:23.716197014 CEST	53	64344	8.8.8.8	192.168.2.5
May 19, 2021 20:17:23.748080969 CEST	53	62060	8.8.8.8	192.168.2.5
May 19, 2021 20:17:24.260726929 CEST	61805	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:24.287029982 CEST	53	61805	8.8.8.8	192.168.2.5
May 19, 2021 20:17:25.219938040 CEST	54795	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2021 20:17:25.254148960 CEST	53	54795	8.8.8.8	192.168.2.5
May 19, 2021 20:17:26.171206951 CEST	49557	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:26.197520018 CEST	53	49557	8.8.8.8	192.168.2.5
May 19, 2021 20:17:27.057033062 CEST	61733	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:27.096728086 CEST	53	61733	8.8.8.8	192.168.2.5
May 19, 2021 20:17:27.151319981 CEST	65447	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:27.174463034 CEST	53	65447	8.8.8.8	192.168.2.5
May 19, 2021 20:17:28.509195089 CEST	52441	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:28.532723904 CEST	53	52441	8.8.8.8	192.168.2.5
May 19, 2021 20:17:29.564441919 CEST	62176	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:29.590425014 CEST	53	62176	8.8.8.8	192.168.2.5
May 19, 2021 20:17:31.046998024 CEST	59596	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:31.070113897 CEST	53	59596	8.8.8.8	192.168.2.5
May 19, 2021 20:17:32.188293934 CEST	65296	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:32.215003014 CEST	53	65296	8.8.8.8	192.168.2.5
May 19, 2021 20:17:32.641459942 CEST	63183	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:32.688021898 CEST	53	63183	8.8.8.8	192.168.2.5
May 19, 2021 20:17:33.252104998 CEST	60151	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:33.296492100 CEST	53	60151	8.8.8.8	192.168.2.5
May 19, 2021 20:17:34.283885002 CEST	60151	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:34.315618992 CEST	53	60151	8.8.8.8	192.168.2.5
May 19, 2021 20:17:35.291547060 CEST	60151	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:35.317531109 CEST	53	60151	8.8.8.8	192.168.2.5
May 19, 2021 20:17:35.458484888 CEST	56969	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:35.482055902 CEST	53	56969	8.8.8.8	192.168.2.5
May 19, 2021 20:17:37.052423000 CEST	55161	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:37.075999022 CEST	53	55161	8.8.8.8	192.168.2.5
May 19, 2021 20:17:37.308626890 CEST	60151	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:37.345324993 CEST	53	60151	8.8.8.8	192.168.2.5
May 19, 2021 20:17:41.324037075 CEST	60151	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:41.355669022 CEST	53	60151	8.8.8.8	192.168.2.5
May 19, 2021 20:17:50.312611103 CEST	54757	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:50.352821112 CEST	53	54757	8.8.8.8	192.168.2.5
May 19, 2021 20:17:56.167798996 CEST	49992	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:56.201343060 CEST	53	49992	8.8.8.8	192.168.2.5
May 19, 2021 20:17:56.851614952 CEST	59736	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:56.875581980 CEST	53	59736	8.8.8.8	192.168.2.5
May 19, 2021 20:17:56.930810928 CEST	51058	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:56.930860996 CEST	52636	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:56.954364061 CEST	53	51058	8.8.8.8	192.168.2.5
May 19, 2021 20:17:56.954399109 CEST	53	52636	8.8.8.8	192.168.2.5
May 19, 2021 20:17:59.320317030 CEST	60075	53	192.168.2.5	8.8.8.8
May 19, 2021 20:17:59.346663952 CEST	53	60075	8.8.8.8	192.168.2.5
May 19, 2021 20:18:00.643158913 CEST	55016	53	192.168.2.5	8.8.8.8
May 19, 2021 20:18:00.690125942 CEST	53	55016	8.8.8.8	192.168.2.5
May 19, 2021 20:18:02.097224951 CEST	64345	53	192.168.2.5	8.8.8.8
May 19, 2021 20:18:02.130069971 CEST	53	64345	8.8.8.8	192.168.2.5
May 19, 2021 20:18:18.495903015 CEST	57128	53	192.168.2.5	8.8.8.8
May 19, 2021 20:18:18.539336920 CEST	53	57128	8.8.8.8	192.168.2.5
May 19, 2021 20:18:38.770735025 CEST	54791	53	192.168.2.5	8.8.8.8
May 19, 2021 20:18:38.815757990 CEST	53	54791	8.8.8.8	192.168.2.5
May 19, 2021 20:18:45.691498041 CEST	50463	53	192.168.2.5	8.8.8.8
May 19, 2021 20:18:45.728144884 CEST	53	50463	8.8.8.8	192.168.2.5
May 19, 2021 20:19:00.922507048 CEST	50394	53	192.168.2.5	8.8.8.8
May 19, 2021 20:19:00.959621906 CEST	53	50394	8.8.8.8	192.168.2.5
May 19, 2021 20:19:07.767666101 CEST	58530	53	192.168.2.5	8.8.8.8
May 19, 2021 20:19:08.767359018 CEST	58530	53	192.168.2.5	8.8.8.8
May 19, 2021 20:19:08.811439037 CEST	53	58530	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 6248 Parent PID: 792

General

Start time:	20:17:30
Start date:	19/05/2021
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:	0xb00000
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	6675977C	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$aim Covid Tvx - Bandoir PBR.docx	success or wait	1	66685805	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\Claim Covid Tvx - Bandoir PBR.docx	5989	261	success or wait	1	66685805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	66698A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	66698A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	66698A84	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	66685805	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\218A0	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	66685805	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	66685805	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	66685805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	66685805	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	66685805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\218A0	218A0	binary	04 00 00 00 68 18 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 BF 71 CC BE 26 4D D7 01 A0 18 02 00 A0 18 02 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	66685805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2021-05-19T20:18	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	1808811949 0	success or wait	1	66685805	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	1387462664	1387462665	success or wait	1	66685805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1387462665	1387462666	success or wait	1	66685805	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	66685805	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	66685805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	66685805	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	66685805	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
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	66685805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	doc	wpd doc	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\218A0	218A0	binary	04 00 00 00 68 18 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 BF 71 CC BE 26 4D D7 01 A0 18 02 00 A0 18 02 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 68 18 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A0 18 02 00 A0 18 02 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	66685805	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 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 FF FF FF FF 00 00 00 00 00 00 00 00				

Disassembly