ID: 406072
Sample Name: Giam Gia Dien dich Covid-19.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:54:04
Date: 06/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report Giam Gia Dien dich Covid-19.docx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 12
Public 13
Private 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 18
General 18
File Icon 18
Network Behavior 19
UDP Packets 19
Code Manipulations 20
Statistics 20
System Behavior 20
Analysis Process: WINWORD.EXE PID: 7020 Parent PID: 800 20
General 20
File Activities 20
File Created 20
File Deleted 21
File Written 21
File Read 23
Registry Activities 24
Key Created 24
Key Value Created 24

Key Value Modified 25
Disassembly 28

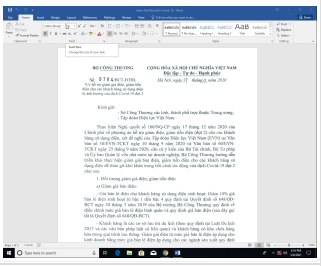
Analysis Report Giam Gia Dien dich Covid-19.docx

Overview

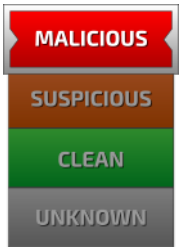
General Information

Sample Name:	Giam Gia Dien dich Covid-19.docx
Analysis ID:	406072
MD5:	3a5ea4602985f1d.
SHA1:	165975dd8d3965..
SHA256:	3d63156060c756..
Infos:	

Most interesting Screenshot:



Detection

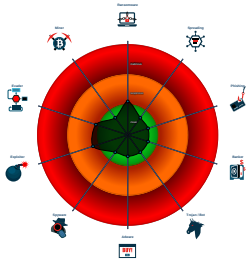


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Allocates a big amount of memory (p…

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 7020 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

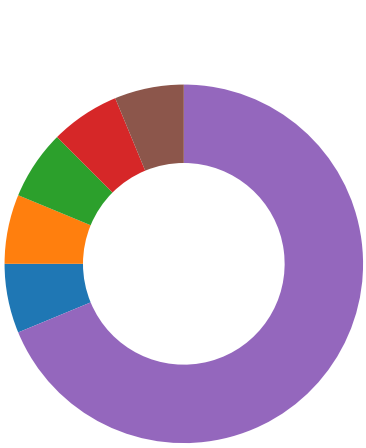
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection



Click to jump to signature section

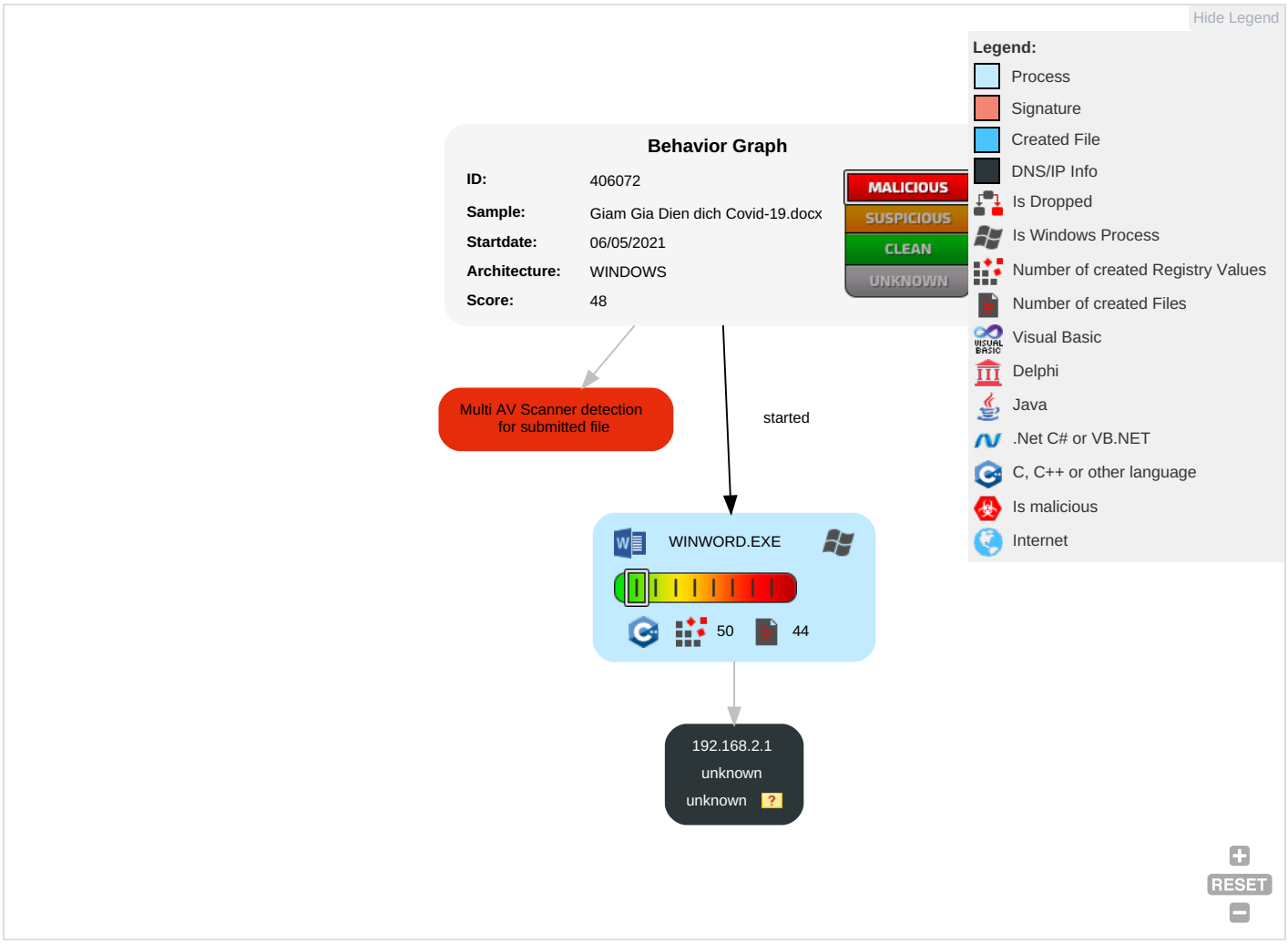
AV Detection:

Multi AV Scanner detection for submitted file

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	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	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

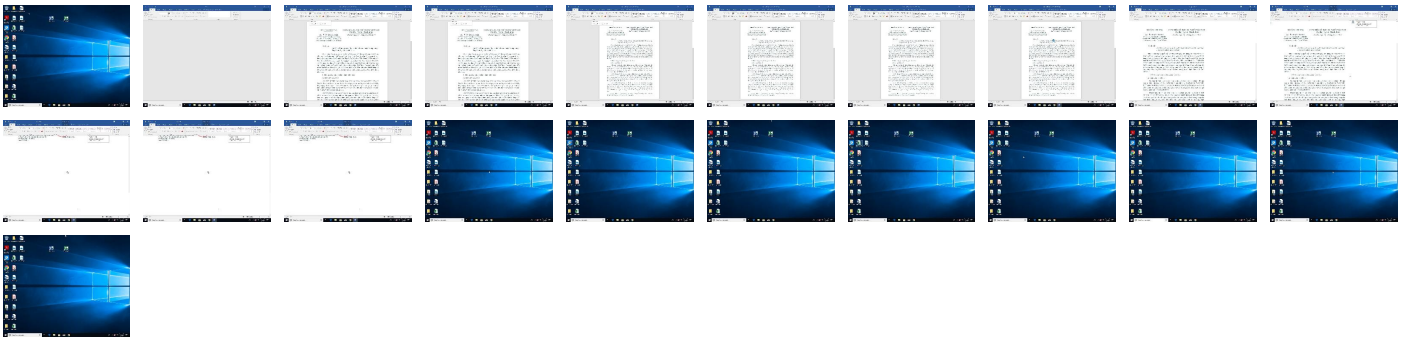
Behavior Graph

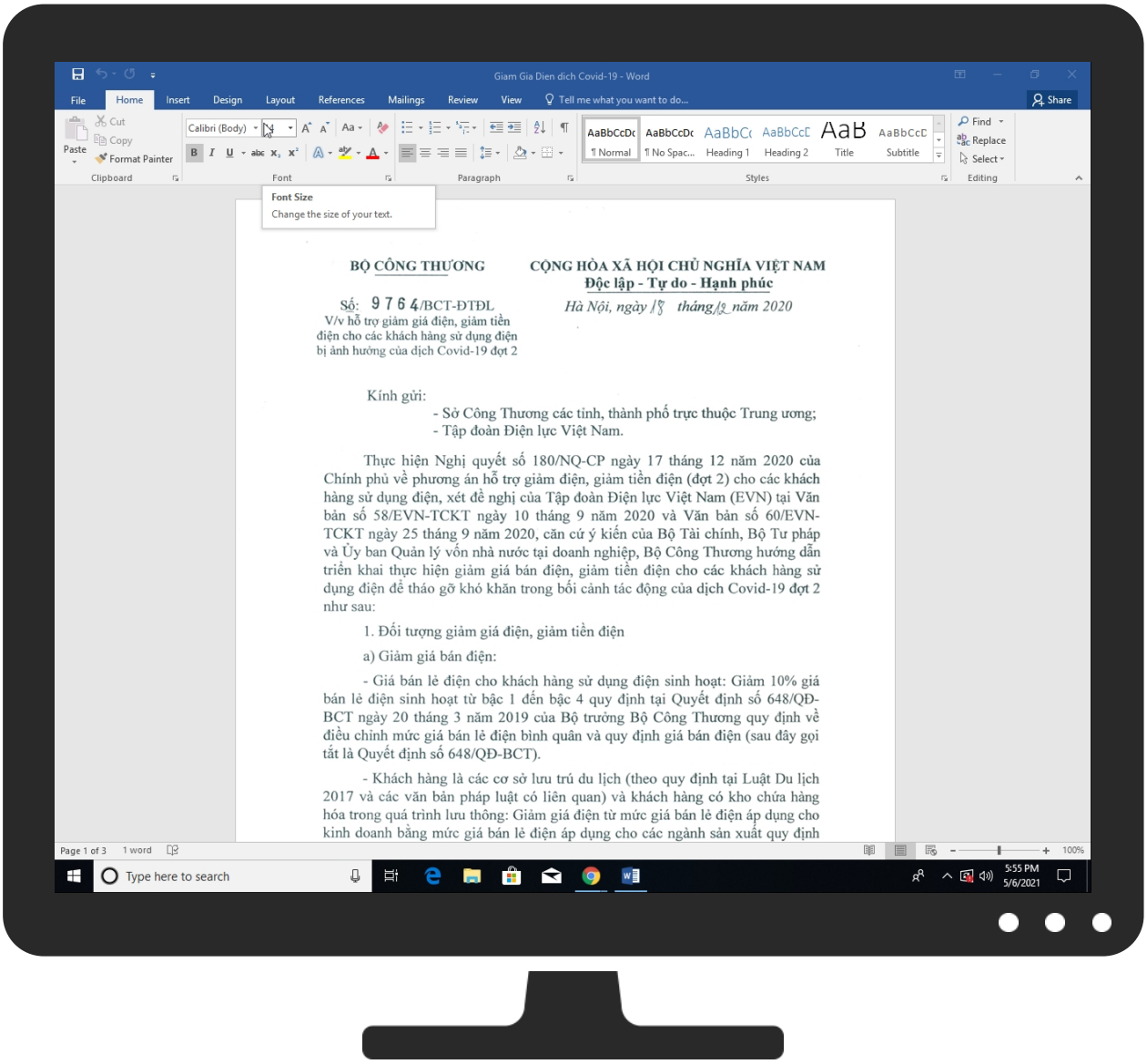


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Giam Gia Dien dich Covid-19.docx	44%	Virustotal		Browse
Giam Gia Dien dich Covid-19.docx	37%	ReversingLabs	Document-Word.Trojan.MacroLess	

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	

Source	Detection	Scanner	Label	Link
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	
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%	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.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://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://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://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://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%	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://ncus.pagecontentsync.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://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://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	
http://https://staging.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

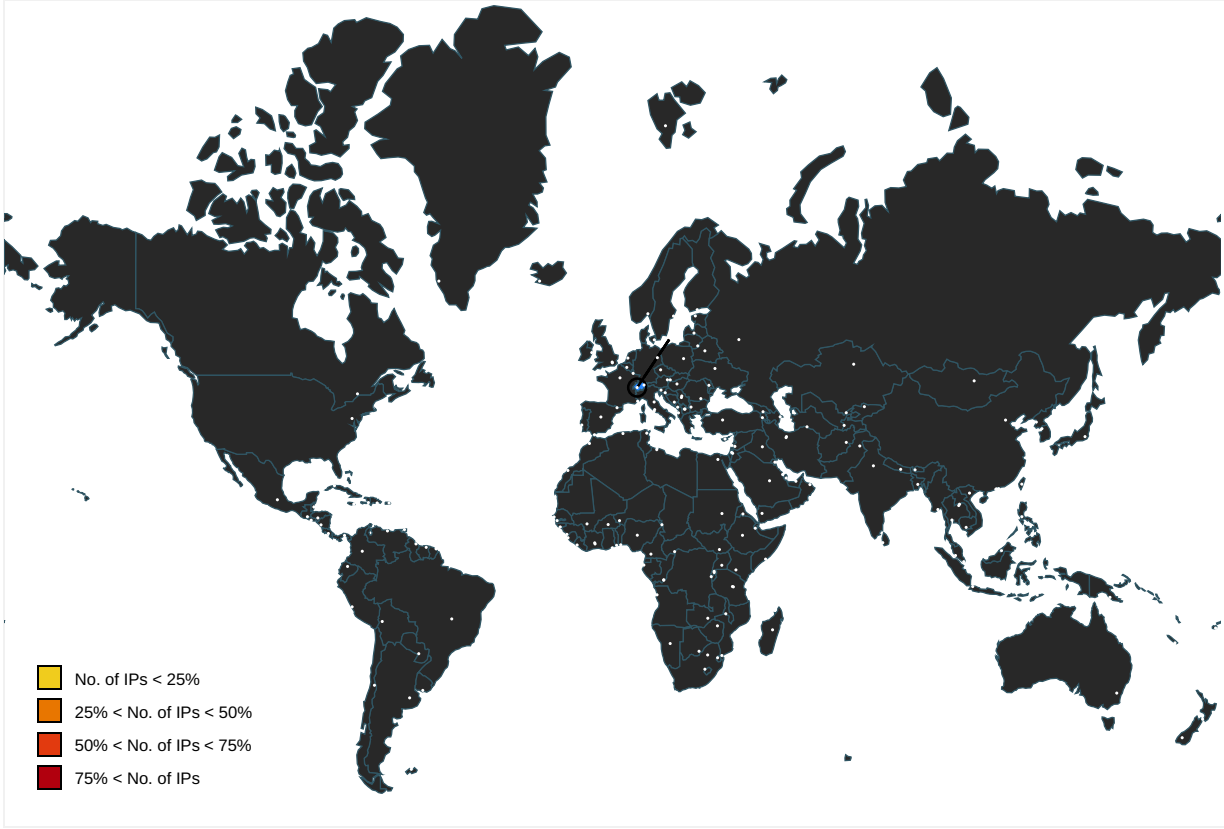
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://login.microsoftonline.com/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://shell.suite.office.com:1443	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://autodiscover-s.outlook.com/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://cdn.entity.	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://powerlift.acompli.net	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://cortana.ai	66796C8F-B35E-4D79-8859-ED4428147AB3.0.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	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cloudfiles.onenote.com/upload.aspx	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://api.aadrm.com/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://api.microsoftstream.com/api/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://cr.office.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://graph.ppe.windows.net	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://store.office.cn/addinstemplate	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://web.microsoftstream.com/video/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://graph.windows.net	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://dataservice.o365filtering.com/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://analysis.windows.net/powerbi/api	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://ncus.contentsync.	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://weather.service.msn.com/data.aspx	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://apis.live.net/v5.0/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://management.azure.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://wus2.contentsync.	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://api.office.net	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://entitlement.diagnostics.office.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://outlook.office.com/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://templatelogging.office.com/client/log	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://outlook.office365.com/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://webshell.suite.office.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://management.azure.com/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.windows.net/common/oauth2/authorize	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://devnull.onenote.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://ncus.pagecontentsync.	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://messaging.office.com/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://augloop.office.com/v2	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://skyapi.live.net/Activity/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://dataservice.o365filtering.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://directory.services.	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false		high
http://https://staging.cortana.ai	66796C8F-B35E-4D79-8859-ED4428147AB3.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	406072
Start date:	06.05.2021
Start time:	17:54:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Giam Gia Dien dich Covid-19.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:	17
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:	MAL
Classification:	mal48.winDOCX@1/13@0/1
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

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\66796C8F-B35E-4D79-8859-ED4428147AB3	
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):	134558
Entropy (8bit):	5.368397724288956
Encrypted:	false
SSDEEP:	1536:gcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:nEQ9DQW+zPXO8
MD5:	7A4C3601BC2DD7954DA1BA3161D3EFC9
SHA1:	A6A4DA1DBD073EE7C3DEE3BBB54523C772FF7618
SHA-256:	7366A55609C83E814D44A31FEEB20CACCF2D567BFECF0BD3848AB75E73AD3F27
SHA-512:	5BB1A67C9B44A42E54BFDDFCCD04A4BB4ADDAC21E8066D18F7378D2DD60DA784394458A5062DD4A8EF47D247D2D605D80CE0D84EF8B9A5D5DA54E580B56D3DC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\66796C8F-B35E-4D79-8859-ED4428147AB3	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-05-06T15:55:00">.. Build: 16.0.14103.30529-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\31990A3A.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1632x2248, frames 3
Category:	dropped
Size (bytes):	179149
Entropy (8bit):	7.498989359361687
Encrypted:	false
SSDEEP:	3072:InZv8DVPECilPPurliFX4zeqyFswxmLNv/Ovlf6r:liDVcCixmkdywg4k
MD5:	CCF44CB88060891D72824C85263B8593
SHA1:	E3F073A33F58ED9A8D30FE5B40C1562B63525549
SHA-256:	A4CF4B260533B8C2E0BB48CC238E3911814C9D2A66D717F027FE7ED84F3E6CD6
SHA-512:	0C1EB2059BBEEA8544A8383222E629C9BB6DF033814EB67E8BCA1049220454C91546A1B20B2808676E34573225204A120C359B2B6888818AEE6F8EEAAA86BEAD
Malicious:	false
Reputation:	low
Preview:	......JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....`.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...(...(...(...(.....P.(...(...(...(..P..1KE..(.....-....M&=(..@.E/Z1@..F3K.K@X@)h...(...Fih...(...(.....ZZB.....L|....(...(..-..M.....wu....SB..;.....4.P...1.-.....P16...-..@1A.....F) q.K@..LsN...c..J(...QE....(.bm..Q@..sK.(.....)h.....).b..m.....Q@..6.....c.4.c..4..R..Z(...2sKE.&)h...Lf...M.=(.-..n=)pii;..FF..b...B)...E.&)1.N..h.x#....Z.1F9..P0...-...R.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\462875DD.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1632x2248, frames 3
Category:	dropped
Size (bytes):	463122
Entropy (8bit):	7.941005620963689
Encrypted:	false
SSDEEP:	12288:guWH4ewApn1KVgYW4MuQPMMvoIcqSKNOOTH/L1PVd:DWOu0VDWV+hqSKNZH/p
MD5:	8DC6D650D41EF0AEE460EA408CFFB095
SHA1:	519D87A644B924FF2843E56E76516000C1C58D03
SHA-256:	3E6B27C4EF54DAEDBEB5364CC83CD0B311145D22F6FFCAB803846116E2E89FC3
SHA-512:	6D23FC0478F6869198180FF70B6AEBDE815FD3133FFBDB3A853D618884E95FB5B01AE11CC4F9490AF88BBA261130A11A2CF677FC087C1354B32726C56239799E
Malicious:	false
Reputation:	low
Preview:	......JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....`.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...(...(...(.....P..(...(...(...)...*A....@.t....]s...i.f.."...].s.h.....K.g...k#H.....`g...PH. ERHP3.b..9.H....n..&...F(U.`.../\..EE.....1...(.aE.P...H..#$.J\s.(.QE..(...(.E.....R.1@.....f) ..8..(4.O(.1C:.7.f....G!R.W...R*...Q.P....<Q..0(....).4r.($t.j].....R..`...E1.F.9P]z.....@.R.4.h.4.f..P..K@4P0..(...-.P.I.Z1@.....F.....!...;..P(..(.0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4E26524C.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1632x2248, frames 3
Category:	dropped
Size (bytes):	397176
Entropy (8bit):	7.917524851464137
Encrypted:	false
SSDEEP:	12288:z3cKJJb9zQkrtlQ3pWcESs5tKvE1kylf6+Aa:tJVHOWcCtThlfaa
MD5:	A932FCE967C7DC635C60325088BE2BC5
SHA1:	7AED834D295BDD62F487DE5834A1CD118434E669
SHA-256:	7EA75C8EC7C814267F116DE05F0C56E7228E6BECF1F245B8FFEC78C6520E3D85
SHA-512:	ADF8F7F5A96699562AEC022883E706543BD676C530455AC0B0852A276E486E09F1EB5D3F7BFAF57966AB531C068D573E0AF5AAF983C71FCC172975703F57DCC
Malicious:	false
Reputation:	low
Preview:	......JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....`.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...(...(...(...(...(...(...(.4..QE..R.Z.(..@...(...(....g....E..QE..QE..QE..QE..Ph...E.....E.....R.@..(.aE.P.A...@1KE..QE..R.R.}N....QE..R.Z(.QE.....(.:Q.R3H}...SI u..@...(.aE.P.E.P..P)qE.....(.....E.P0..(...E...i..-&h..-7.@..(.aE.P.E..&..`P.zR3E...b...M.9.).....Q@.(...(.....);.. ..(.QE..QGz(...(..4...Rt.B.I....Q@.N.-.P .4Sq..:.Nih.g.g.C.t.@.h... .QHh.h...4.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{052071EC-7EE4-48FD-8E75-870D08322BDF}.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{7A43107D-BD67-4CB9-B371-FBE9DF1698C1}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.46639096299572214
Encrypted:	false
SSDEEP:	3:9l99lDKllllzNfWQ7ZlhQteolllzNitkIxZlhQtu:Q//ZWQ7ZUtDl/ktkIxZUtu
MD5:	E52863DC2076CF83086E41F901944AC3
SHA1:	1F598794305C229175327E2CEA1974593F493BD0
SHA-256:	3E6FB8931596CCC486133AFE4CE68FFB4C453F16508D4F3972DBA13A9761C4DD
SHA-512:	7F0DCC452CD8BE9B8BE6C56487A6278387ACB05ED5535815448739E8EAC73935671EA0971A47B690484A4AA4BC3C8601FC0E79AA12F2745577312B60ECE56D3
Malicious:	false
Preview:	....j.....h.h..U..mH..nH..u.....j.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{C15F1D1B-BFCF-4AAA-9EF6-16EE60EE8874}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.363080378556589
Encrypted:	false
SSDEEP:	6:liiiiiiii8l+4V/Nc8++ldL61DX6tD6pV2E67:23dNG+PmBqZ6pV2p7
MD5:	7FB2437513B92CE05C5FE037B1418372
SHA1:	E591EE835CEA59585261EF4F2E57456E6D17D5E1
SHA-256:	10CE8C271F180A67FF2B70401DFFB0C92F662758E40E07AA40FF5C1D243BBDE7
SHA-512:	F68DCC2063857CD7D3BD3C24A0A7B01AF9B3135EE436C20BF1849FB165DF048EBEE61DC37102469BA3FDBD2139D8373960C4613133B7DE1152F0C49615BB261
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...p.r.a.t.e.s.h...p..... ..... ."...&...*.....>...B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{EE3D3D5E-8DA2-48AF-AC16-FD6E2E3754DA}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	3144
Entropy (8bit):	3.3132279149334654
Encrypted:	false
SSDEEP:	24:In4e0D/Ue0D/R4T2fT1hZeI/7haHq7hasGTTOcyfq92fH1H1hu18VTBxPe:I4lUlRNJhZeI9ayanTCcyfxVVh4+TXPe
MD5:	FCC7D2124177FFDA1C61C7C49D516857
SHA1:	D1B794057751DB3E373B138FFC1C88F696450D6B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{EE3D3D5E-8DA2-48AF-AC16-FD6E2E3754DA}.tmp	
SHA-256:	1BA010F67FF6A2733C53D206F7D9AA9F59BBE0B9F5D41F5A10EE801935156ABF
SHA-512:	79C0026C192D35E52B8ADBC045A11A7F44146B16D2D7537316623A83D7B8ADEF5B24E4DA230EAB0572426190FBA69359261E69C3DD7F9CF20D658697A53104F5
Malicious:	false
Preview:	..... .!."#.$.%.&.'.(.).*.+.,.-.../.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>...../...../...../...../..... .{. .D.D.E.A.U.T.O. .c.:.\.\.w.i.n.d.o.w.s.\.\.s.y.s.t.e.m.3.2.\.\.c.m.d...e.x.e. .. /.k. .n.o.t.e.p.a.d...e.x.e.. .}. .....D.D.E.A.U.T.O. .c.:.\.\.w.i.n.d.o.w.s.\.\.s.y.s.t.e.m.3.2.\.\.c.m.d...e.x.e. .. /.k. .c.a.l.c...e.x.e.. ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Giam Gia Dien dich Covid-19.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 06:35:54 2020, mtime=Thu May 6 14:55:00 2021, atime=Thu May 6 14:54:51 2021, length=3831871, window=hide
Category:	dropped
Size (bytes):	2290
Entropy (8bit):	4.763972610932184
Encrypted:	false
SSDEEP:	24:8giqm6PNCIrhllAUb4UDJYo7aB6mygiqm6PNCIrhllAUb4UDJYo7aB6m:85qm2YImU0GY9B6p5qm2YImU0GY9B6
MD5:	137DF7AF050861EB5F7CCE983D76CE29
SHA1:	9E77A8CAFE1C5304CD197EB040566CFA4C627E64
SHA-256:	A4E5495C9C27A01F005AA9B22F963C07708D1164A5CAF2EC06F226D4CD12D852
SHA-512:	E445524AB6691C8980AC4A0069D693A062E72BEC95CBD3BEDDA354814DAACB22FB4C1C9D3BFAB64466FECCD9466877C136DCA61CE6C18B183028FBF5F8087 60
Malicious:	false
Preview:	L.....F.... .....kT....0..+.B....z&.B..?x:.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.~.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,- .2.1.8.1.3.....P.1.....>Q}<..user.<.....N...R.~....#J.....W...j.o.n.e.s.....~.1.....>Q.<..Desktop.h.....N...R.~.....Y.....>.....*...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-. 2.1.7.6.9.....2.?x:..R.~ .GIAMGI~1.DOC..r.....>Q|<.R.~.....V.....G.i.a.m. .G.i.a. .D.i.e.n. .d.i.c.h. .C.o.v.i.d.-.1.9...d.o.c.x.....f.....-.....e.....>.S.... ..C:\Users\user\Desktop\Giam Gia Dien dich Covid-19.docx..7.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.G.i.a.m. .G.i.a. .D.i.e.n. .d.i.c.h. .C.o.v.i.d.-.1.9...d.o.c.x.....:..,.LB.)... As...`.....X.....992547.....!a..%.H.VZAj.....!a..%.H.VZAj.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	121
Entropy (8bit):	4.542396251693991
Encrypted:	false
SSDEEP:	3:HpWsaKtX9icA4o6yhsaKtX9icA4omxWpWsaKtX9icA4ov:HpZaKtX9/faKtX9/aZaKtX9/y
MD5:	A6A003D8A638AAD4B0740F87E1B11870
SHA1:	892CB43317BE13499D66ECA7E4A23FC4582B773E
SHA-256:	D2652ED72E15F5B44F02F36965CCEC9D59ADAB83EB71841B930741268FD7250D
SHA-512:	A51C9327D4D1C48FD77B2F9FF9F4A124C709E06ADA54054C32DC859E1B71E78FF7B736BD714BD8F857A5BC180820E35F3B972629CE06760CDC407D187D5828A
Malicious:	false
Preview:	[misc]..Giam Gia Dien dich Covid-19.LNK=0..Giam Gia Dien dich Covid-19.LNK=0..[misc]..Giam Gia Dien dich Covid-19.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):	2.6127589000032074
Encrypted:	false
SSDEEP:	3:Rl/Zdaw5l/7lqKHEAoY1gl/vliZ3l/tZ:RtZnlUcDoY1gtoZ3lL
MD5:	4AE1B86B132B6537B747C664222FF380
SHA1:	48D795B3331FDBE21610D519F85288B887F1D345
SHA-256:	DFC22C62EC205E778CD6F7163AFE1DB6C1F3006D87F139A06BCEB8DBDBFDCD02
SHA-512:	1B3F2DDA419CDBE2C3432EE3C4316EF98032D14640676157EFA43AD14707ADC8FFE61A28FB3618710C864BCA9947ECB398A84DEB2505A6FD07BFF49370556CD E
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....n.l.....H.....6C.....b.U.....x..s`..sP..s.....f.Q.....

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

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$am Gia Dien dich Covid-19.docx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.6127589000032074
Encrypted:	false
SSDEEP:	3:Rl/Zdaw5l/7lqKHEAoY1gl/vliZ3l/tZ:RtZnlUcDoY1gtoZ3lL
MD5:	4AE1B86B132B6537B747C664222FF380
SHA1:	48D795B3331FDBE21610D519F85288B887F1D345
SHA-256:	DFC22C62EC205E778CD6F7163AFE1DB6C1F3006D87F139A06BCEB8DBDBFDCD02
SHA-512:	1B3F2DDA419CDBE2C3432EE3C4316EF98032D14640676157EFA43AD14707ADC8FFE61A28FB3618710C864BCA9947ECB398A84DEB2505A6FD07BFF49370556CDE
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....n.l.....H.....6C.....b.U....x..s`..sP..s.....f.Q.....

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.986899031192039
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:	Giam Gia Dien dich Covid-19.docx
File size:	3831871
MD5:	3a5ea4602985f1db670f166e111aefd2
SHA1:	165975dd8d3965068f3dc0a2c5b512e5e6a9de1f
SHA256:	3d63156060c7568b2c3065820f698fdadb6e48910ec8259a61c306c13f5692c
SHA512:	cae1180e5a8cc0dae9d4c9c78d4fe2a6c12e229c8ce8db2eb581dee86348aa367176fd48f27e8b34a6308a8f00699b50d6190b32e5b06d64c5432bbbdb54e8ae
SSDEEP:	98304:JoycO1vLPTvgX9l3N6+lsNy93RcY0W7/iJg8:Joqvz8XL3N6gsU9aY0Wcd
File Content Preview:	PK.....!....F.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 17:54:44.545339108 CEST	54531	53	192.168.2.4	8.8.8.8
May 6, 2021 17:54:44.604098082 CEST	53	54531	8.8.8.8	192.168.2.4
May 6, 2021 17:54:45.389695883 CEST	49714	53	192.168.2.4	8.8.8.8
May 6, 2021 17:54:45.438410044 CEST	53	49714	8.8.8.8	192.168.2.4
May 6, 2021 17:54:46.399461031 CEST	58028	53	192.168.2.4	8.8.8.8
May 6, 2021 17:54:46.448299885 CEST	53	58028	8.8.8.8	192.168.2.4
May 6, 2021 17:54:46.631654978 CEST	53097	53	192.168.2.4	8.8.8.8
May 6, 2021 17:54:46.690268040 CEST	53	53097	8.8.8.8	192.168.2.4
May 6, 2021 17:54:47.339766979 CEST	49257	53	192.168.2.4	8.8.8.8
May 6, 2021 17:54:47.391283035 CEST	53	49257	8.8.8.8	192.168.2.4
May 6, 2021 17:54:48.280591011 CEST	62389	53	192.168.2.4	8.8.8.8
May 6, 2021 17:54:48.332278967 CEST	53	62389	8.8.8.8	192.168.2.4
May 6, 2021 17:54:49.347872972 CEST	49910	53	192.168.2.4	8.8.8.8
May 6, 2021 17:54:49.399434090 CEST	53	49910	8.8.8.8	192.168.2.4
May 6, 2021 17:54:50.667917013 CEST	55854	53	192.168.2.4	8.8.8.8
May 6, 2021 17:54:50.719647884 CEST	53	55854	8.8.8.8	192.168.2.4
May 6, 2021 17:54:51.835547924 CEST	64549	53	192.168.2.4	8.8.8.8
May 6, 2021 17:54:51.887182951 CEST	53	64549	8.8.8.8	192.168.2.4
May 6, 2021 17:54:58.455281973 CEST	63153	53	192.168.2.4	8.8.8.8
May 6, 2021 17:54:58.504048109 CEST	53	63153	8.8.8.8	192.168.2.4
May 6, 2021 17:54:59.669050932 CEST	52991	53	192.168.2.4	8.8.8.8
May 6, 2021 17:54:59.717849970 CEST	53	52991	8.8.8.8	192.168.2.4
May 6, 2021 17:55:00.057293892 CEST	53700	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:00.114347935 CEST	53	53700	8.8.8.8	192.168.2.4
May 6, 2021 17:55:00.704899073 CEST	51726	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:00.761957884 CEST	53	51726	8.8.8.8	192.168.2.4
May 6, 2021 17:55:01.715537071 CEST	51726	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:01.773108006 CEST	53	51726	8.8.8.8	192.168.2.4
May 6, 2021 17:55:02.180593967 CEST	56794	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:02.229268074 CEST	53	56794	8.8.8.8	192.168.2.4
May 6, 2021 17:55:02.727840900 CEST	51726	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:02.784909010 CEST	53	51726	8.8.8.8	192.168.2.4
May 6, 2021 17:55:03.818212986 CEST	56534	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:03.869791985 CEST	53	56534	8.8.8.8	192.168.2.4
May 6, 2021 17:55:04.749928951 CEST	51726	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:04.812267065 CEST	53	51726	8.8.8.8	192.168.2.4
May 6, 2021 17:55:07.627441883 CEST	56627	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:07.677165031 CEST	53	56627	8.8.8.8	192.168.2.4
May 6, 2021 17:55:08.757956982 CEST	51726	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:08.815583944 CEST	53	51726	8.8.8.8	192.168.2.4
May 6, 2021 17:55:11.445663929 CEST	56621	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:11.494364977 CEST	53	56621	8.8.8.8	192.168.2.4
May 6, 2021 17:55:12.212789059 CEST	63116	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:12.264298916 CEST	53	63116	8.8.8.8	192.168.2.4
May 6, 2021 17:55:13.191086054 CEST	64078	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:13.239871979 CEST	53	64078	8.8.8.8	192.168.2.4
May 6, 2021 17:55:14.843369007 CEST	64801	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:14.892297029 CEST	53	64801	8.8.8.8	192.168.2.4
May 6, 2021 17:55:15.654515028 CEST	61721	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:15.703294039 CEST	53	61721	8.8.8.8	192.168.2.4
May 6, 2021 17:55:16.798230886 CEST	51255	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:16.847172976 CEST	53	51255	8.8.8.8	192.168.2.4
May 6, 2021 17:55:17.882764101 CEST	61522	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:17.934501886 CEST	53	61522	8.8.8.8	192.168.2.4
May 6, 2021 17:55:19.302222967 CEST	52337	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:19.362895966 CEST	53	52337	8.8.8.8	192.168.2.4
May 6, 2021 17:55:22.929009914 CEST	55046	53	192.168.2.4	8.8.8.8
May 6, 2021 17:55:22.991796017 CEST	53	55046	8.8.8.8	192.168.2.4
May 6, 2021 17:55:39.964828968 CEST	49612	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 17:55:40.024502993 CEST	53	49612	8.8.8.8	192.168.2.4
May 6, 2021 17:56:18.305829048 CEST	49285	53	192.168.2.4	8.8.8.8
May 6, 2021 17:56:18.371023893 CEST	53	49285	8.8.8.8	192.168.2.4
May 6, 2021 17:56:47.628483057 CEST	50601	53	192.168.2.4	8.8.8.8
May 6, 2021 17:56:47.688167095 CEST	53	50601	8.8.8.8	192.168.2.4
May 6, 2021 17:56:55.567514896 CEST	60875	53	192.168.2.4	8.8.8.8
May 6, 2021 17:56:55.746428013 CEST	53	60875	8.8.8.8	192.168.2.4
May 6, 2021 17:56:56.213213921 CEST	56448	53	192.168.2.4	8.8.8.8
May 6, 2021 17:56:56.317822933 CEST	53	56448	8.8.8.8	192.168.2.4
May 6, 2021 17:56:56.772640944 CEST	59172	53	192.168.2.4	8.8.8.8
May 6, 2021 17:56:56.830096960 CEST	53	59172	8.8.8.8	192.168.2.4
May 6, 2021 17:56:56.864912987 CEST	62420	53	192.168.2.4	8.8.8.8
May 6, 2021 17:56:56.922034979 CEST	53	62420	8.8.8.8	192.168.2.4
May 6, 2021 17:56:57.369997978 CEST	60579	53	192.168.2.4	8.8.8.8
May 6, 2021 17:56:57.432935953 CEST	53	60579	8.8.8.8	192.168.2.4
May 6, 2021 17:56:57.966337919 CEST	50183	53	192.168.2.4	8.8.8.8
May 6, 2021 17:56:58.028384924 CEST	53	50183	8.8.8.8	192.168.2.4
May 6, 2021 17:56:58.590169907 CEST	61531	53	192.168.2.4	8.8.8.8
May 6, 2021 17:56:58.647545099 CEST	53	61531	8.8.8.8	192.168.2.4
May 6, 2021 17:56:59.368092060 CEST	49228	53	192.168.2.4	8.8.8.8
May 6, 2021 17:56:59.430543900 CEST	53	49228	8.8.8.8	192.168.2.4
May 6, 2021 17:56:59.914699078 CEST	59794	53	192.168.2.4	8.8.8.8
May 6, 2021 17:56:59.973834991 CEST	53	59794	8.8.8.8	192.168.2.4
May 6, 2021 17:57:00.459115982 CEST	55916	53	192.168.2.4	8.8.8.8
May 6, 2021 17:57:00.516216993 CEST	53	55916	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 7020 Parent PID: 800

General

Start time:	17:54:57
Start date:	06/05/2021
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:	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	65DE977C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4E26524C.jpeg	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	65D15805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\462875DD.jpeg	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	65D15805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\31990A3A.jpeg	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	65D15805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{C15F1D1B-BFCF-4AAA-9EF6-16EE60EE8874}.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65D15805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{7A43107D-BD67-4CB9-B371-FBE9DF1698C1}.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65D15805	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$am Gia Dien dich Covid-19.docx	success or wait	1	65D15805	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4E26524C.jpeg	0	65536	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 08 06 06 07 06 05 08 07 07 07 09 09 08 0a 0c 14 0d 0c 0b 0b 0c 19 12 13 0f 14 1d 1a 1f 1e 1d 1a 1c 1c 20 24 2e 27 20 22 2c 23 1c 1c 28 37 29 2c 30 31 34 34 34 1f 27 39 3d 38 32 3c 2e 33 34 32 ff db 00 43 01 09 09 09 0c 0b 0c 18 0d 0d 18 32 21 1c 21 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 ff c0 00 11 08 08 c8 06 60 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08	......JFIF.............C...... .... $.' ",#.. (7),01444.'9=82<.342. ..C...........2!.!22222222222 2 2222222222222222222222 22222222 22222222........`.."......... ....}........! 1A..Qa."q.2....	success or wait	7	65D15805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\462875DD.jpeg	0	65536	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 08 06 06 07 06 05 08 07 07 07 09 09 08 0a 0c 14 0d 0c 0b 0b 0c 19 12 13 0f 14 1d 1a 1f 1e 1d 1a 1c 1c 20 24 2e 27 20 22 2c 23 1c 1c 28 37 29 2c 30 31 34 34 34 1f 27 39 3d 38 32 3c 2e 33 34 32 ff db 00 43 01 09 09 09 0c 0b 0c 18 0d 0d 18 32 21 1c 21 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 ff c0 00 11 08 08 c8 06 60 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08	......JFIF.............C...... .... $.' ",#.. (7),01444.'9=82<.342. ..C...........2!.!22222222222 2 2222222222222222222222 22222222 22222222........`.."......... ....}........! 1A..Qa."q.2....	success or wait	8	65D15805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\31990A3A.jpeg	0	65536	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 08 06 06 07 06 05 08 07 07 07 09 09 08 0a 0c 14 0d 0c 0b 0b 0c 19 12 13 0f 14 1d 1a 1f 1e 1d 1a 1c 1c 20 24 2e 27 20 22 2c 23 1c 1c 28 37 29 2c 30 31 34 34 34 1f 27 39 3d 38 32 3c 2e 33 34 32 ff db 00 43 01 09 09 09 0c 0b 0c 18 0d 0d 18 32 21 1c 21 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 ff c0 00 11 08 08 c8 06 60 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08	......JFIF.............C...... .... $.' ",#.. (7),01444.'9=82<.342. ..C...........2!.!22222222222 2 2222222222222222222222 22222222 22222222........`.."......... ....}........! 1A..Qa."q.2....	success or wait	3	65D15805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{C15F1D1B-BFCF-4AAA-9EF6-16EE60EE8874}.tmp	unknown	1536	0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 0d 00 70 00 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..(...(...(...(...(...(...(...(... (...(...p.r.a.t.e.s.h. ..p............................	success or wait	1	65D15805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{7A43107D-BD67-4CB9-B371-FBE9DF1698C1}.tmp	unknown	1024	08 00 08 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	65D15805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Giam Gia Dien dich Covid-19.docx	2782749	65536	success or wait	18	65D15805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{EE3D3D5E-8DA2-48AF-AC16-FD6E2E3754DA}.tmp	unknown	512	success or wait	2	65D15805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{EE3D3D5E-8DA2-48AF-AC16-FD6E2E3754DA}.tmp	unknown	512	success or wait	1	65D15805	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{7A43107D-BD67-4CB9-B371-FBE9DF1698C1}.tmp	unknown	512	success or wait	1	65D15805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{7A43107D-BD67-4CB9-B371-FBE9DF1698C1}.tmp	unknown	512	success or wait	1	65D15805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{EE3D3D5E-8DA2-48AF-AC16-FD6E2E3754DA}.tmp	unknown	72	success or wait	1	65D15805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	65D28A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	65D28A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	65D28A84	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	65D15805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	65D15805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	65D15805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\55C9F	success or wait	1	65D15805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	65D15805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	65D15805	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	65D15805	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	65D15805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	65D15805	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	65D15805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Segoe UI	binary	02 0B 05 02 04 02 04 02 02 03	success or wait	1	65D15805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Microsoft JhengHei	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	65D15805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\55C9F	55C9F	binary	04 00 00 00 6C 1B 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 6A 00 6F 00 6E 00 65 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 C4 B9 D5 43 90 42 D7 01 9F 5C 05 00 9F 5C 05 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	success or wait	1	65D15805	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	65D15805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2021-05-06T17:55	success or wait	1	65D15805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	65D15805	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	1386610696	1386610697	success or wait	1	65D15805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1386610697	1386610698	success or wait	1	65D15805	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	65D15805	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	65D15805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	65D15805	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	65D15805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT632.CNV	success or wait	1	65D15805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	doc	wpd doc	success or wait	1	65D15805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\55C9F	55C9F	binary	04 00 00 00 6C 1B 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 6A 00 6F 00 6E 00 65 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 C4 B9 D5 43 90 42 D7 01 9F 5C 05 00 9F 5C 05 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 6C 1B 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 6A 00 6F 00 6E 00 65 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 9F 5C 05 00 9F 5C 05 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	65D15805	unknown

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

							Source	

Disassembly