ID: 356432
Sample Name:
855_28042020.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:49:10
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

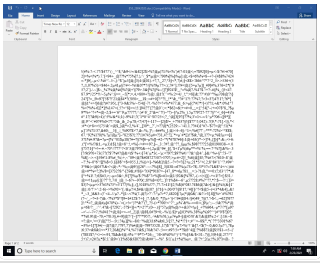
Analysis Report 855_28042020.doc

Overview

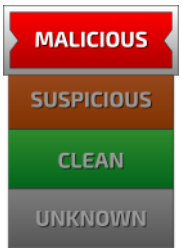
General Information

Sample Name:	855_28042020.doc
Analysis ID:	356432
MD5:	eda54697e6ab43..
SHA1:	fe3b1e8337728c7.
SHA256:	73bccef5c926cef…
Tags:	doc

Most interesting Screenshot:



Detection

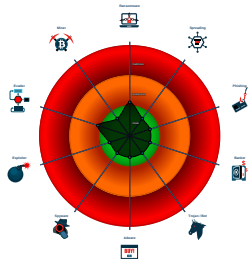


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub…

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 3448 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - splwow64.exe (PID: 6588 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
- **cleanup**

Malware Configuration

No configs have been found

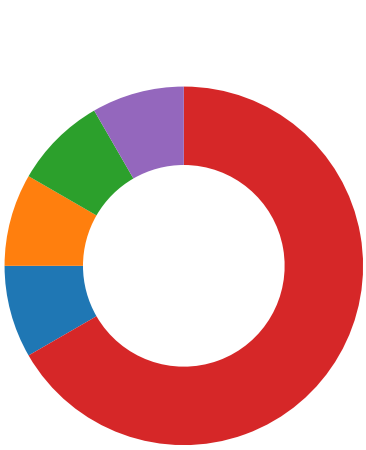
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

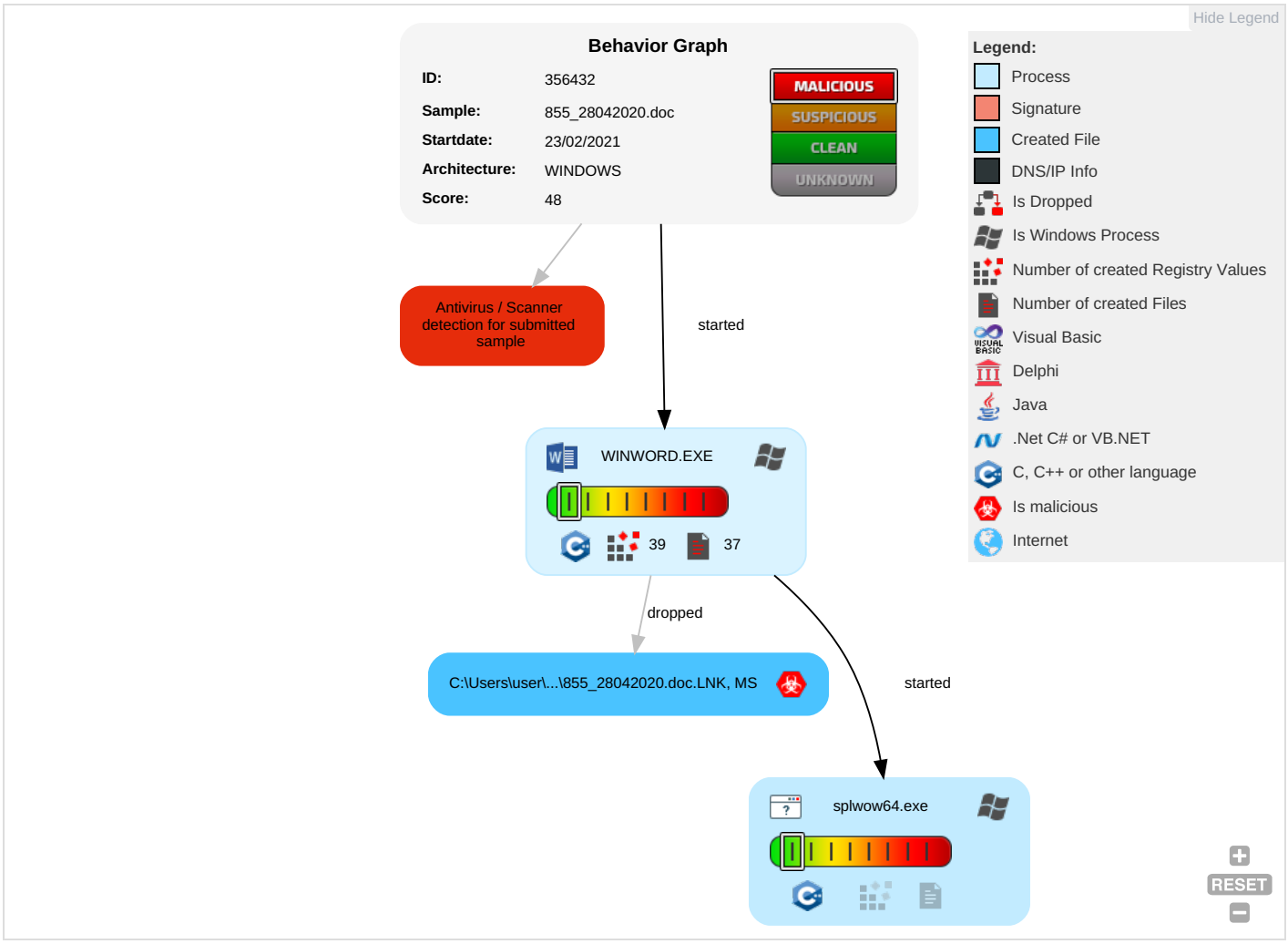
Compliance:

Uses new MSVCR Dlls

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	Process 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	Process 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

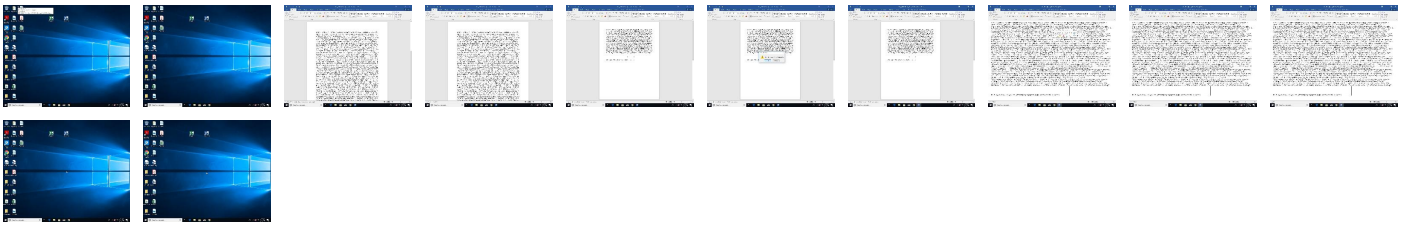
Behavior Graph

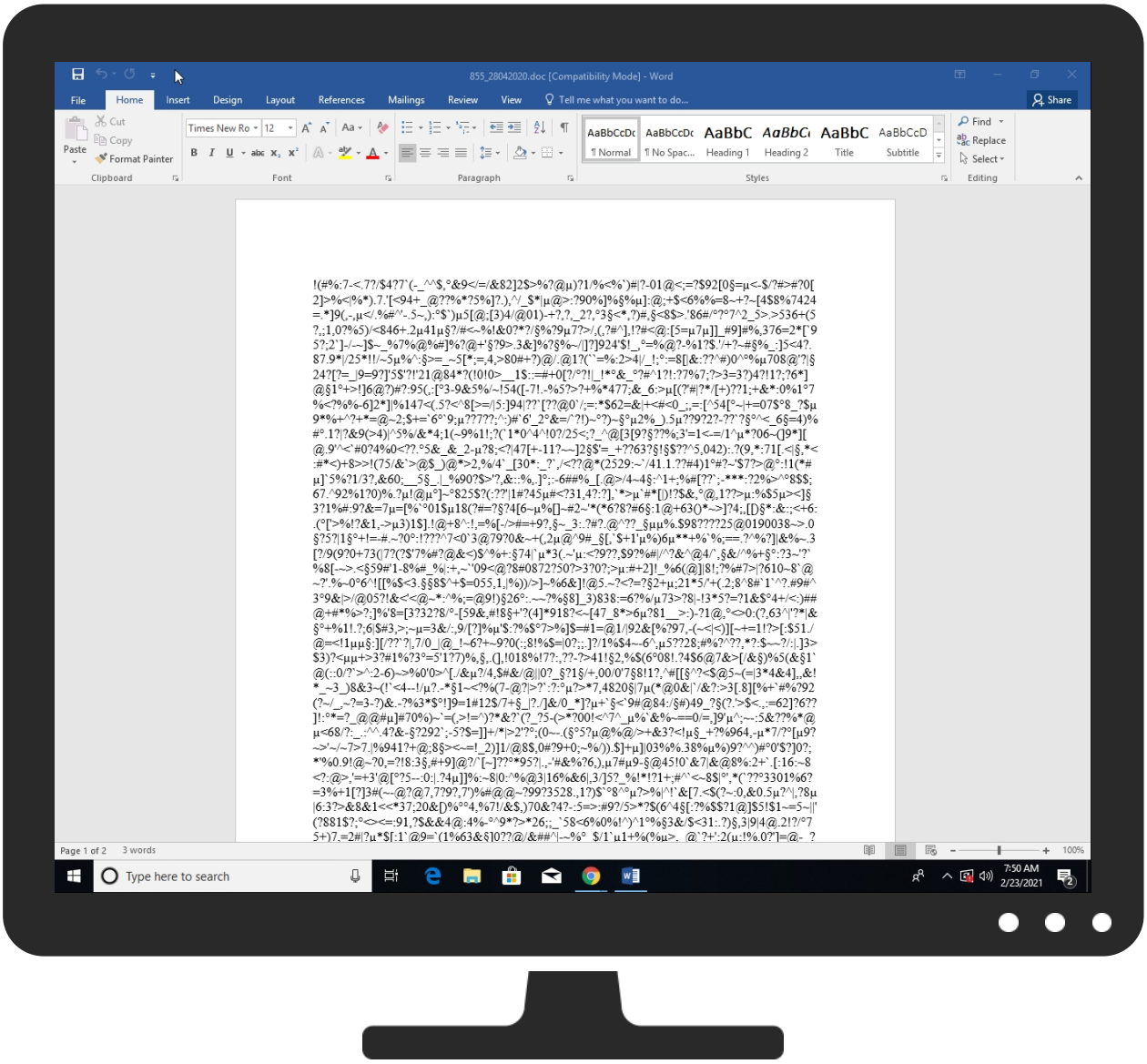


Screenshots

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
855_28042020.doc	100%	Avira	EXP/CVE-2017-11882.Gen	

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	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	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://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	

Source	Detection	Scanner	Label	Link
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://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://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Virustotal		Browse
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://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	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://login.microsoftonline.com/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://shell.suite.office.com:1443	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://autodiscover-s.outlook.com/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://cdn.entity.	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.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	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.contentsync.	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.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	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://powerlift.acompli.net	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://cortana.ai	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.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	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://api.aadrm.com/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://api.microsoftstream.com/api/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://cr.office.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://graph.ppe.windows.net	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://store.office.cn/addinstemplate	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.pagecontentsync.	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.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=	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.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	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://web.microsoftstream.com/video/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://graph.windows.net	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://dataservice.o365filtering.com/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://weather.service.msn.com/data.aspx	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://apis.live.net/v5.0/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.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	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://management.azure.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://incidents.diagnostics.office.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/odc/insertmedia	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://api.office.net	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://entitlement.diagnostics.office.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://outlook.office.com/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://templatelogging.office.com/client/log	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://outlook.office365.com/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://webshell.suite.office.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://management.azure.com/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://ncus-000.contentsync.	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://devnull.onenote.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://messaging.office.com/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://augloop.office.com/v2	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://skyapi.live.net/Activity/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.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	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://dataservice.o365filtering.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://directory.services.	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false		high
http://https://staging.cortana.ai	1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356432
Start date:	23.02.2021
Start time:	07:49:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	855_28042020.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	24
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.winDOC@3/7@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 40.88.32.150, 52.109.32.63, 52.109.88.37, 52.109.8.25, 51.104.139.180, 23.218.208.56, 8.248.143.254, 8.248.123.254, 8.248.139.254, 67.27.157.254, 8.248.119.254, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

Time	Type	Description
07:50:12	API Interceptor	12x Sleep call for process: splwow64.exe modified

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\1482DEE8-6AFF-4FA7-A5EC-FC31A1C9BCCB	
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):	132891
Entropy (8bit):	5.375880424470543
Encrypted:	false
SSDEEP:	1536:NcQceNquBXA3gBwJpQ9DQW+zA9H34ZldpKWXboOilXNErLdzEh:pcQ9DQW+z0XiK
MD5:	AC93374037B05ADCAC4D0EB0B87F4203
SHA1:	C05F8F664EF801E28C3AFC46E8842C6916DAED37
SHA-256:	C76F026C07C9C40439D276A7A513F813C3159538A6AD191431C5D199DD19C5C6
SHA-512:	B4F0A1AB68A751A4AD1782DAFBF6A57554F27665647221D252D698A8A18CC01C7F213028E499B9265F758BCA8E01E81136AABAAD47EDAC1C0566F6909DEB7A4A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-02-23T06:49:54">.. Build: 16.0.13822.30525-->.. <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{493A25AD-4274-46D2-B660-9B9CC5F79F69}.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{F0795CF8-46C6-4803-9D64-32515AF0A3BA}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	11800
Entropy (8bit):	3.5795173516548386
Encrypted:	false
SSDEEP:	192:jL02t8cCtzLMiD8VPVhGMl9qcdT3u6KKYzyk1PDKNXLgSVG2+:jLzcSPHiWTTKKEVD4XN+
MD5:	D2A019904C00B7B5D9C74FE6527733B7
SHA1:	2BD1BA4E410F8815B03621ECA569D0475BE41CF2
SHA-256:	721C67A88A24FF8E862622651BB328FDD93A71873A6A99C8E5AF70F9EA122ECD
SHA-512:	AA8B4AC9407AE5B4DB8E2A97BBC7FC5A603FAE1B74CED011A337272ACA5583F750E44E0F87D790EFD7EB6235BCE5B757DEFC60AB6A652F5A0077AC1EB15ACF0A
Malicious:	false
Reputation:	low
Preview:	!.(.#.%.:.7.-.<...7.?./.$.4.?.7.`.(.-._.^.^.$.,...&.9.<./.=./.&.8.2.].2.$.>.%.?.@...).?.1./.%.<.%.`.).#.|.?.-.0.1.@.<.;.=.?.$.9.2.[.0...=...<.-.$./.?.#.>.#.?.0.[.2.].>.%.<.|.%.*.)...7...'.[.<.9.4.+._.@.?.?.%.*.?.5.%.].?...),.,.^./._.$.*.|...@.>.:.?.9.0.%.].%...%...].:.@.;.+.$.<.6.%.%.=.8.~.+.?.~.[.4.$.8.%.7.4.2.4.=...*.].9.(.,.-.,...<./...%.#.^.'.-...5.~.,.):....$.`.)...5.[.@.;.[.3.).4./.@.0.1.).-.+.?.,.?.,._.2.?.,...3...<.*.,.?.).#.,...<.8.$.>...'.8.6.#./...?...7.^.2._.5.>...>.5.3.6.+.(.5.?.,.;.1.,.0.?.%.5.)./.<.8.4.6.+...2...4.1.....?./.#.<.~.%.!.&.0.?.*.?./...%.?.9...7.?.>./.,.(.,.?.#.^.],.,.!.?.#.<.@.:.[.5.=...7...].]._.#.9.].#.%.,.3.7.6.=.2.*.[.`.9.5.?.;.2.`.].-./.-.~.].$.~._.%.7.%.@.%.#.].%.?.@.+.'...?.9.>...3.&.].%.?...%.~./.|.].?.].9.2.4.'.$.!._.,...=.%.@.?.-.%.1.?.$...'./.+.?.~.#...%._.:.].5.<.4.?...8.7...9.*.|./.2.5.*.!.!./.~.5...%.^.:....>.=._.~.5.[.*.;.=.,.4.,.>.8.0.#.+.?.).@./...@.1.?.(.`.`.=.%.:.2.>.4.|./._.!.;,...:.=.8.[.|.&.:.?.?.^.#.).0.^...%...7.0.8.@.'.?.|...2.4.?.[.?.=.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\855_28042020.doc.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:41 2020, mtime=Tue Feb 23 14:49:54 2021, atime=Tue Feb 23 14:49:51 2021, length=233718, window=hide
Category:	dropped
Size (bytes):	2130
Entropy (8bit):	4.678382635187083
Encrypted:	false
SSDEEP:	24:8UaMuCKGAkWlYDUIb7aB6myUaMuCKGAkWlYDUIb7aB6m:8/0ekWWCB6p/0ekWWCB6
MD5:	F654A120857ADC8CE11947F311D83F7C
SHA1:	2639231BADD849C89E3F426A012FBD815A095313
SHA-256:	E69DA1D7BC1E31A20544E293FFE3AB0516EC7D065244C630AA785029E3CE206E
SHA-512:	B0D78A5558A6970DDF5C79F6A2E67AA5159BF5CC5AF571DF1CF26D68EDA5768A2A11535A44284027125CDF9174831F6219AC29CC746A99F5F32F2ABA68DB2E2
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ...I.G.:...NF.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..WR5~.....:.....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.WR5~.....S.....e..h.a.r.d.z.....~.1.....>Qwx..Desktop.h.....Ny.WR5~.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....n.2.....WR:~ .855_28~1.DOC..R.....>QuxWR:~....h.....\...8.5.5._.2.8.0.4.2.0.2.0...d.o.c.....V.....-.....U.....>.S.....C:\Users\user\Desktop\855_28042020.doc..'.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.8.5.5._.2.8.0.4.2.0.2.0...d.o.c.....:.,.LB.)...As...`.....X.....549163.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	86
Entropy (8bit):	4.0000353661000005
Encrypted:	false
SSDEEP:	3:M1dyXxVFLtCr8XxVFLtCmX1dyXxVFLtCv:MsBTBUBs
MD5:	1EAAF7B3978F4E4249554585391D6599
SHA1:	532EDB6FB412A13F87B5E0E9514E4C7FF6EB84B1
SHA-256:	3F286F8E9C782A59E5DABD48E19F42CE7ABBB06AA672EAD095D90430DB019F71
SHA-512:	1E1DF1DE5B09CF26C28B3F0A231F0F1F3A208965B8745FE9ACABEECBCB7F6BDD32E59333ED910F0AE4F061E03649484FED08608D073945ED7ECAC6CDC9444A07
Malicious:	false
Reputation:	low
Preview:	[doc]..855_28042020.doc.LNK=0..855_28042020.doc.LNK=0..[doc]..855_28042020.doc.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.672077668363927
Encrypted:	false
SSDEEP:	3:Rl/ZdCm4zll/9lqKfAltl1tlimb4R3N7F+dqP:RtZAQEAl/4L8dqP
MD5:	FC1DE3AA73CA41A9956F719B450F3AEC
SHA1:	5EFAC89691B2313C4DFDB1C652AB212294AE88F8
SHA-256:	4529FF40A828032741ACE0EA0F0F839BF9670100845E8E0B6BD9C0E6F1C70502
SHA-512:	4688B77728566DC7AC085D9FEDF8B60153D56DE86A89C75B5217AD69EDED0ADCCEBC4F5DBCC6D98BAD05C690B7ACFAD0B792DDFC8AC4A36A85D80B1CF8252E7
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....6....,.....$.....6C.....:....-.....>.....^.j@..jT..j

C:\Users\user\Desktop\~$5_28042020.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.672077668363927
Encrypted:	false
SSDEEP:	3:Rl/ZdCm4zll/9lqKfAltl1tlimb4R3N7F+dqP:RtZAQEAl/4L8dqP
MD5:	FC1DE3AA73CA41A9956F719B450F3AEC
SHA1:	5EFAC89691B2313C4DFDB1C652AB212294AE88F8

C:\Users\user\Desktop\~$5_28042020.doc	
SHA-256:	4529FF40A828032741ACE0EA0F0F839BF9670100845E8E0B6BD9C0E6F1C70502
SHA-512:	4688B77728566DC7AC085D9FEDF8B60153D56DE86A89C75B5217AD69EDED0ADCCEBC4F5DBCC6D98BAD05C690B7ACFAD0B792DDFC8AC4A36A85D80B1CF8252E7
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....6....,.....$.....6C.....:....-.....>.....^.j@..jT..j

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	2.358539580854024
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	855_28042020.doc
File size:	233718
MD5:	eda54697e6ab436600b8b74102833d7e
SHA1:	fe3b1e8337728c74600eab9cb5c9f073e7c04ced
SHA256:	73bccef5c926cefd41f82a329a8ba732bf59195f19c67498ccf162caa6410de1
SHA512:	a16951fc4600a2e3d468c1b82d05c657ffca41745c2fd91ac2a1449b4f87efe6eda1deb0e3b1c8fe573f0a44760f90a98628a431b81fbcae25bc33e1b55b87b0
SSDEEP:	6144:xLnHVKS3j8PtOPzOptaQE8qRQAX7NRNpo7s:Z
File Content Preview:	{\rtf7345!(#%:7-<.7?/$4?7`(-_^^$,.&9</=/&82]2$>%?@.)?1/%<%`)#|?-01@<;=?$92[0.=.<-$/?#>#?0[2]>%<|%*).7.'[<94+_@??%*?5%]?.),^/_$*\|.@>:?90%]%.%.]:@;+$<6%%=8~+?~[4$8%7424=.*]9(,-,.</.%#^'-.5~,):.$`).5[@;[3)4/@01)-+?,?,_2?,.3.<*,?)#,.<8$>.'86#/.?.7^2_5>.>536+(

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000152Eh	2	embedded	rJH7AOlLcfoAuNg7Sv3a	3584				no

Network Behavior

UDP Packets

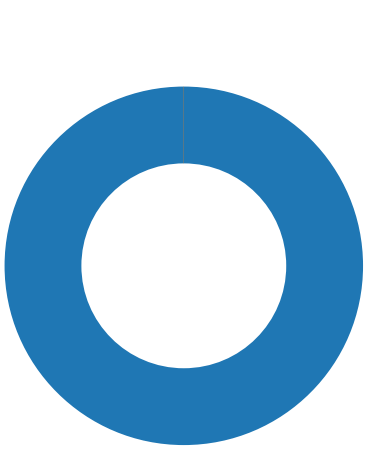
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 07:49:47.082614899 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:47.131302118 CET	53	50620	8.8.8.8	192.168.2.3
Feb 23, 2021 07:49:47.885247946 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:47.937375069 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 07:49:48.725214005 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:48.778696060 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 07:49:49.529930115 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:49.581005096 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 07:49:54.463937998 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:54.525861979 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 07:49:54.976887941 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:55.037965059 CET	53	64185	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 07:49:55.991853952 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:56.040684938 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 07:49:56.221067905 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:56.275150061 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 07:49:56.991839886 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:57.050733089 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 07:49:57.054027081 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:57.102861881 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 07:49:57.908535957 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:57.965487957 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 07:49:58.771482944 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:58.820323944 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 07:49:59.007225037 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:59.058435917 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 07:49:59.574090004 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:49:59.622910023 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 07:50:00.430264950 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:50:00.479000092 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 07:50:01.325335026 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:50:01.376348019 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 07:50:02.217580080 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:50:02.269618988 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 07:50:03.007731915 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:50:03.058753014 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 07:50:03.069091082 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:50:03.123348951 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 07:50:03.965982914 CET	51352	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:50:04.018023968 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 07:50:04.821099997 CET	59349	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:50:04.871782064 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 07:50:05.613234997 CET	57084	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:50:05.664455891 CET	53	57084	8.8.8.8	192.168.2.3
Feb 23, 2021 07:50:06.453061104 CET	58823	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:50:06.501843929 CET	53	58823	8.8.8.8	192.168.2.3
Feb 23, 2021 07:50:21.290867090 CET	57568	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:50:21.339737892 CET	53	57568	8.8.8.8	192.168.2.3
Feb 23, 2021 07:50:27.676306963 CET	50540	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:50:27.734680891 CET	53	50540	8.8.8.8	192.168.2.3
Feb 23, 2021 07:50:41.710563898 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:50:41.759320974 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 07:51:11.997292042 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:51:12.055838108 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 07:51:13.901324987 CET	57762	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:51:13.973232031 CET	53	57762	8.8.8.8	192.168.2.3
Feb 23, 2021 07:51:42.978579044 CET	55435	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:51:43.027165890 CET	53	55435	8.8.8.8	192.168.2.3
Feb 23, 2021 07:51:45.304361105 CET	50713	53	192.168.2.3	8.8.8.8
Feb 23, 2021 07:51:45.355740070 CET	53	50713	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 3448 Parent PID: 792

General

Start time:	07:49:52
Start date:	23/02/2021
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:	0xab0000
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	66AD977C	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$5_28042020.doc	success or wait	1	66A05805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	66A18A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	66A18A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	66A18A84	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1D0E8	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	66A05805	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	66A05805	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	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	66A05805	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	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1D0E8	1D0E8	binary	04 00 00 00 78 0D 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 60 FA FC 97 FB 09 D7 01 E8 D0 01 00 E8 D0 01 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	66A05805	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 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	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2021-02-23T07:50	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 3819	success or wait	1	66A05805	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	1381433359	1381433360	success or wait	1	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1381433360	1381433361	success or wait	1	66A05805	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	66A05805	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	66A05805	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	66A05805	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	66A05805	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	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	doc	wpd doc	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1D0E8	1D0E8	binary	04 00 00 00 78 0D 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 60 FA FC 97 FB 09 D7 01 E8 D0 01 00 E8 D0 01 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 78 0D 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E8 D0 01 00 E8 D0 01 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	66A05805	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 3819	0 0	success or wait	1	66A05805	unknown

Analysis Process: splwow64.exe PID: 6588 Parent PID: 3448

General

Start time:	07:50:12
Start date:	23/02/2021
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff65b2b0000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly