ID: 404291
Sample Name: Bio-Solid Feed Stock Evaluation_.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:51:24
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

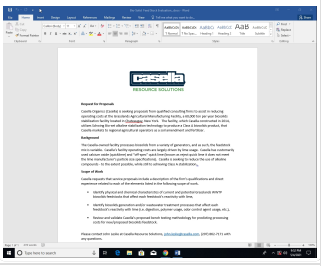
Analysis Report Bio-Solid Feed Stock Evaluation_.docx

Overview

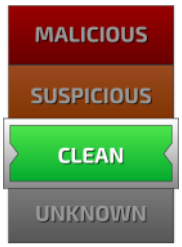
General Information

Sample Name:	Bio-Solid Feed Stock Evaluation_.docx
Analysis ID:	404291
MD5:	a829fa8a85650dd.
SHA1:	22964385dc0064..
SHA256:	08bcf8510cbfb3a..
Infos:	

Most interesting Screenshot:



Detection

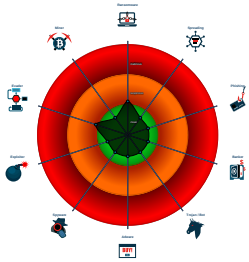


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 5992 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

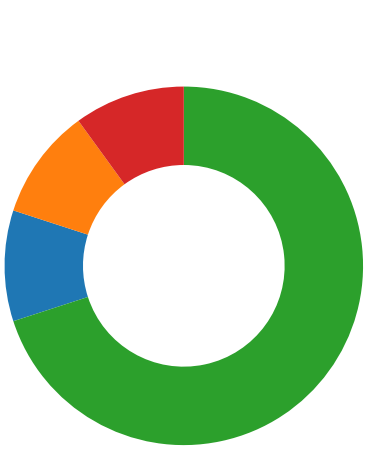
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



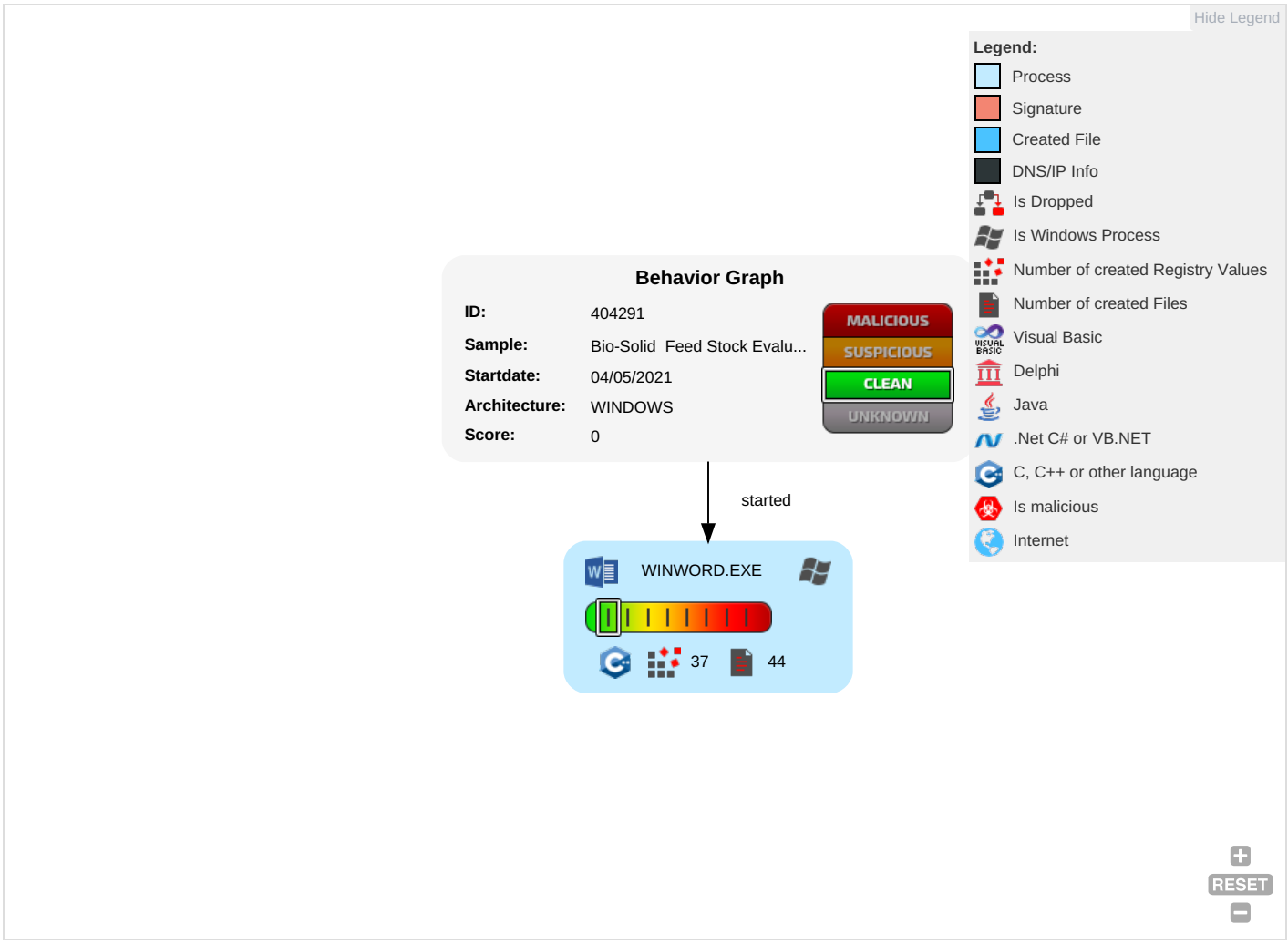
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

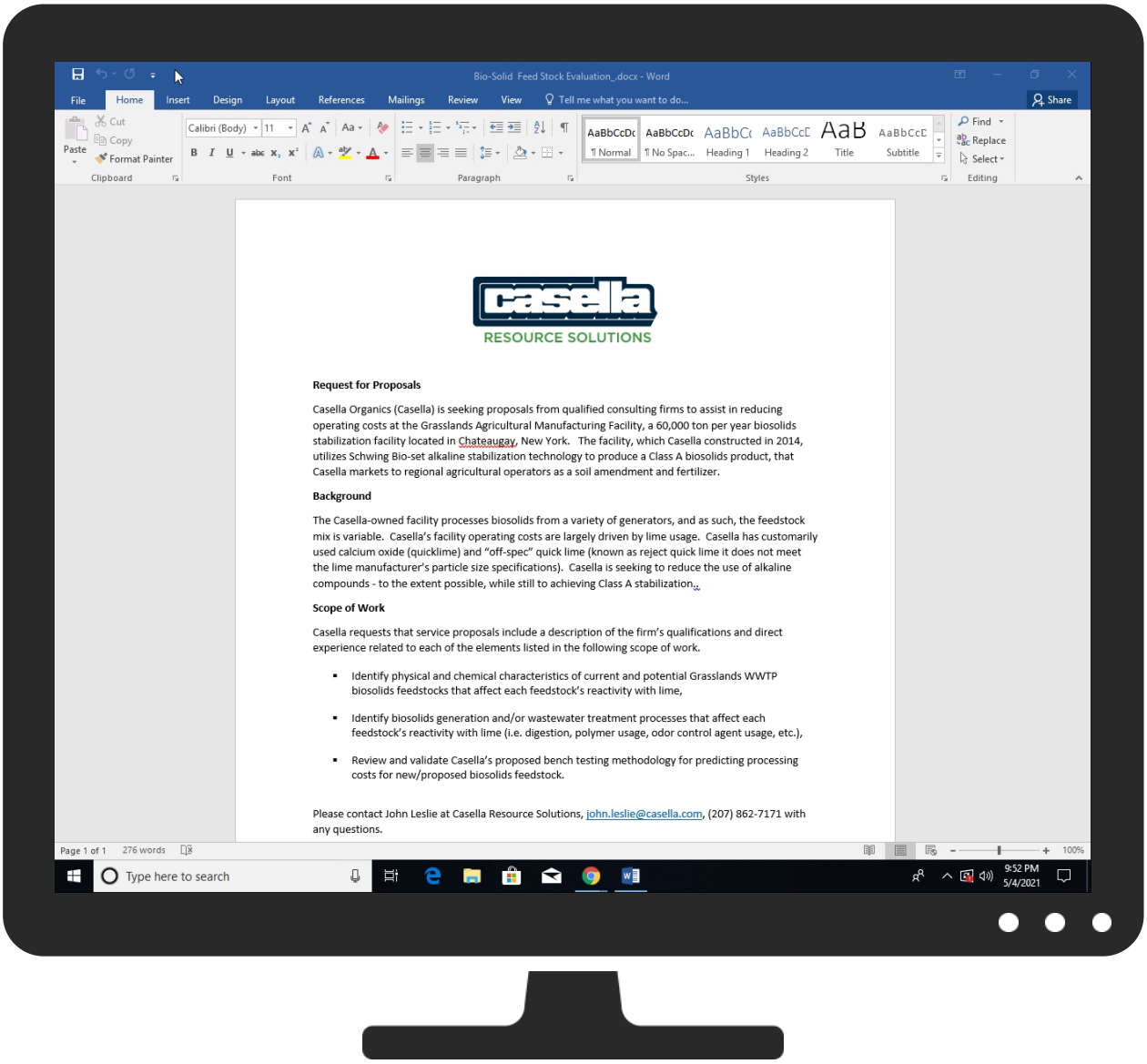
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	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	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://login.microsoftonline.com/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://shell.suite.office.com:1443	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://autodiscover-s.outlook.com/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://cdn.entity.	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://cortana.ai	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.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	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://api.aadrm.com/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://api.microsoftstream.com/api/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://cr.office.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://ecs.office.com/config/v2/Office	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://graph.ppe.windows.net	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://officeci.azurewebsites.net/api/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://store.office.cn/addinstemplate	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.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=	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://globaldisco.crm.dynamics.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://store.officeppe.com/addinstemplate	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev0-api.acompli.net/autodetect	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://web.microsoftstream.com/video/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://graph.windows.net	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://dataservice.o365filtering.com/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://ncus.contentsync.	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://weather.service.msn.com/data.aspx	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://apis.live.net/v5.0/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.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	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://management.azure.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://wus2.contentsync.	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/api/v1.0/me/Activities	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://api.office.net	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://incidents.diagnosticssdf.office.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://entitlement.diagnostics.office.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://outlook.office.com/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://templatelogging.office.com/client/log	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://outlook.office365.com/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://webshell.suite.office.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://management.azure.com/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://devnull.onenote.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://ncus.pagecontentsync.	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://messaging.office.com/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://augloop.office.com/v2	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://skyapi.live.net/Activity/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.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	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://dataservice.o365filtering.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://visio.uservoice.com/forums/368202-visio-on-devices	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://directory.services.	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.dr	false		high
http://https://staging.cortana.ai	DF1C0634-A091-48ED-8FF2-AF628B96BF81.1.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:	32.0.0 Black Diamond
Analysis ID:	404291
Start date:	04.05.2021
Start time:	21:51:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bio-Solid Feed Stock Evaluation_.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winDOCX@1/11@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

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\DF1C0634-A091-48ED-8FF2-AF628B96BF81	
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):	5.368391659266551
Encrypted:	false
SSDEEP:	1536:UcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:TEQ9DQW+zPXO8
MD5:	16D01D9D8F2B0DCEC42940B25E6B2106
SHA1:	D954FAE7A2B3464F22FCB670C3BBCB8DC3ACF43A
SHA-256:	B37DAE2CA61EDF4821D46ABF6A919750B34E3AB1B2AE9E81D89AF022B95917E6
SHA-512:	2120F4CF40C9710BADDF6F1631009A5C70C0FD4977E0C4F56FA06A2811B4F05E8CB436FAB3186A5FE8755EE6DE17108A902138D0B14A026C5427687019D31465
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-05-04T19:52:17">.. Build: 16.0.14102.30525-->.. <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.MSO\88D6A842.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 228 x 81, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	12912
Entropy (8bit):	7.980657944433155
Encrypted:	false
SSDEEP:	192:t/mdfXGmMfhQ7E0FyUm177+dZlivT4moRWzLGwk9o4fGXjER/U7:Uh22FyidZIMURWzHYGTz7
MD5:	91251E9C2886771106FA67FA469EC2D2
SHA1:	F10256D1480FB009A2AC58F80A6BDDD6269A2FBE
SHA-256:	67A26E18A62AA8C2E7919BDA7B1DA3089DD262993AD7C88B0ACBAB9F8A265C3A
SHA-512:	2D34B014640350DEA9B913661744149E053C0901F465DFD4F236010BD521C55E842923463CEA51A6009411A65D4AD37CB1C767C25FA6C9C547F831E4E1025781
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\88D6A842.png	
Preview:	.PNG.....IHDR.....Q.....P.K....sRGB.....pHYs.....+.....tEXtSoftware.Microsoft Office..5q..1.IDATx^.}.|SU.....t....e...ED\.D`*.X.bE.....od.!n.[...D*v.....a.Ed.D....Ji.6{.....$]..M.;..4...s..{.....-.w..AD._.+.J..].D0.....[Ex.6"a.A\.....2...n..xA.....%r....,>...@..=..V.j..D.5G.fnw....4....<.`..y\..#.....z...,(.G..._....".F..\.F.s.v.}0..6.6=\...pzx.~+.S.rXw...s"" .....D,.....e...v.....".4.....p..u.....N..W3...,R..1 .9.]r.B...(..~.-..3...PA.#..s....!...e.....3..&..y..8..a...l.;.HD.....&.....y..Tx...^.,.!...:,`....[7.XL\.w....D...1..=m.e.m.Z.j.....R`F.... ...n.qV.....'.K...k:y..T.N.....9..)...Q._.Z.....T8P.:...[..?a).....8.E...i4...;.-"...B....H4.0..].....JW..oHK.t#.!..V..\C M;fH..!...o.V.. ..b..A.v.....:".s....q...B ...%.c..6.....A.v,.../T0Pf... <I.~..m8.....{..2b.....p...J..."'"f'..:A`9.."h+n..;ep..U.....F.C...JIJ.A.....o.....q.fH.;..&b.Y.{g...z.6!.32.K... .O"..c..ID..K...z"D.[.....I..uE[.H...IZ....fy

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\mso8672.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 1024 x 768, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	9084
Entropy (8bit):	6.066243465397226
Encrypted:	false
SSDEEP:	96:ESBBav8ThoL9Jd+saEmB9IS9W/bvtWzd/JEdtgYTwetWyLrfvqk+U25qD3MsuTqy:ESdKvVmB9Ls8JqdtWCebkcU+
MD5:	84EA1CD08BE8E4BB6D8FA8BA0530FB13
SHA1:	B5FF79D7B5EE6C4F47F754A11B34302AD99C84DB
SHA-256:	5CDB826CC6DDF754FF543B77A3D12276B7B21DA81B7E197D5653B3B1574CC1AC
SHA-512:	013419EEA891A25976CCA53293BD8883AFBDAFA557E279E8D918CF12D0B169FD905CA93E412E50A61BA90E9E803E6895E121AEFFF2ED3B3CFBC60552770F3A4 4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....pHYs.....tEXtSoftware.Adobe ImageReadyq.e<..#.IDATx....q.G...9....H..E*.....@T..".0.*.....M.@e E..>..tw.W.....B....y?h..^....?..C.u'... ....V.1....Z..Q....zJ.....?.....H....9.....c.(D.... ..<^.>....{..._..za$...)_D.SJ?.....@..C.I.... .....E..1.....M).....P#@./.... .).Kc..s..J.p< ..Q.L)....8.....`)..|aT...y.x@...ww.t.. ..nw$...D.....O...w... ...:._P.....r.x@.....'...+...0..[#.. .I~....0..../.3Y7F..@..zl5....5...rf|....;T..F....+'.....A...zc..v.....`..#c.. @9.z].X....;..z..~.....Qc=...}....Jm.....08..`...F..| ..%..A..1..9...0..;... *.....g...."_n.... .).+c.....W.ny.....d[.P.....;... ....1..o.~.@Q.b...SY..`n..u=...}.....Q...'.....#.. H."vJ.'...c...`..1....<..... ...`...0.....R.4.@..Gy.. .....fJ.7.`..v.....0z....|.Z...,.w....|..nw$...D..GV.,.w...~..n....._...*.Ex...4....8....(.'.c..*.....0..ko...AN.k0.@..'.\u.... ./SJ"...!...../g.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{B75B9AA0-2C2A-42AF-99FA-1A1373CEF798}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{DE6EC9FB-3337-48EC-BC41-5E8E77CEDBD8}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	5558
Entropy (8bit):	3.2100491303624255
Encrypted:	false
SSDEEP:	96:chjmS4+HTIw8suFs53hgMNXhc+QUAu777+FKb6:cdHT3ys5fRhHiV
MD5:	A60DB88EF4FFB9F449F3E51D43168EE7
SHA1:	6A2E3B8C49C438B68AE9601C8C4EA371321C848D
SHA-256:	0B81F0B817CAD98516763E79B4E774E8EC2972AC3C957408173D3D1D96D21197
SHA-512:	BFDAD2ADBA0796F6BDB831F493C841FE7F0F5B5641F9D8A331B06C63990CE32236417591CBAE90E64AF91B86D71B5759D756BB2843A47A041392A7E4515FBAC A
Malicious:	false
Reputation:	low
Preview:	../.....R.e.q.u.e.s.t. .f.o.r. .P.r.o.p.o.s.a.l.s.....

C:\Users\user\AppData\Local\Temp\mso8538.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlrojAxh4bxdtT/CS3wkxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWKbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A
SHA-512:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA878 41
Malicious:	false
Reputation:	high, very likely benign file
Preview:	GIF89a....w..!..MSOFFICE9.0.....sRGB.....!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3.!..MSOFFICE9.0.....cmPPJCmp0712.....!.....,.....'.;..b...RQ.xx.... .....,+.....yy..;..b.....qp.bb.....uv.ZZ.LL.....xw.jj.NN.A@....zz.mm.^_.....yw.....yx.xw.RR.,*.++..... .....8....>.....4567...=..../0123.....<9:.()*+,-.B.@...."#$%&'..... !..... .....C.?....A;<...HT(..;

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Bio-Solid Feed Stock Evaluation_.docx.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:46 2020, mtime=Wed May 5 03:52:18 2021, atime=Wed May 5 03:52:15 2021, length=28469, window=hide
Category:	dropped
Size (bytes):	2350
Entropy (8bit):	4.707968364236359
Encrypted:	false
SSDEEP:	24:8opNK/E4AIZRx4AyNo2QvZRxCDhRh7aB6myopNK/E4AIZRx4AyNo2QvZRxCDhRh2:8opnWXfG6BXIMB6popnWXfG6BXIMB6
MD5:	3636098DDB5C361119C3D9900C1969CC
SHA1:	94B3D7C57C9DA2151E287F241C66F6D45F8ACB00
SHA-256:	F72633FFDB9B8AC500E38A760B7BDA3FF702F5E140770C804EE35E7C0344A4B0
SHA-512:	1561C3412E702A52584ED0C56DF397E731A2A330DC65C380C273DA687FD7422DDBEC85E8226984E693640FD70B4C97AFBA202C2AA49C41B216968AEF57950D3
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...k...:....=.mjA...S.kjA..5o.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.&.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Qyx..user.<.....Ny..R.&.....S.....h.a.r.d.z.....~.1.....>Q{x..Desktop.h.....Ny..R.&.....Y.....>.....d...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.- 2.1.7.6.9.....2.5o...R.& .BIO-SO~1.DOC..~.....>Qxx.R.&....h.....l..B.i.o.-.S.o.l.i.d. . .F.e.e.d. .S.t.o.c.k. .E.v.a.l.u.a.t.i.o.n._...d.o.c.x.....l.....-.....k.....>.S.. ....C:\Users\user\Desktop\Bio-Solid Feed Stock Evaluation_.docx..=.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.B.i.o.-.S.o.l.i.d. . .F.e.e.d. .S.t.o.c.k. .E.v.a.l.u.a.t.i.o.n._...d.o.c.x. .....:.,.LB.)...As...`.....X.....830021.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q.....

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):	154
Entropy (8bit):	4.748557805188019
Encrypted:	false
SSDEEP:	3:HsMT21MREg0Q4MQWS/n1MREg0Q4MQWSmxWsMT21MREg0Q4MQWSv:HtT21zVQ4MnWn1zVQ4MnaT21zVQ4Mnc
MD5:	52D7C16EB6DB8326A3D103C4F06CD57D
SHA1:	789704C304038A34D60E42FC5769838AF33376A2
SHA-256:	81197DCB14624A313257D0272276987AD2C6195C0FE476A2399F92061849319F
SHA-512:	D7EDA7E5E9D57113D4EE10D360F54B83E3CE4F2D41EB26C3CA4969DD3291B00C38A3FD18E0B522B4651D2C7F3DBC2FACD45BA5738B86898C4DD24767E6099 2D
Malicious:	false
Reputation:	low
Preview:	[misc]..Bio-Solid Feed Stock Evaluation_.docx.LNK=0..Bio-Solid Feed Stock Evaluation_.docx.LNK=0..[misc]..Bio-Solid Feed Stock Evaluation_.docx.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	1.8270399412171197
Encrypted:	false
SSDEEP:	3:Rl/ZdzcCVl//tlclkXlolRhlXln:RtZxWk14P

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
MD5:	066EAF455BB4CBC23C499AF83D7C92EB
SHA1:	75AC762773A704B3E890CD02B7B8F89EE068DDC2
SHA-256:	47EE684F6BD787F6FDDCDDBBCC12DBD2E3568F9EE6A2AC9796B54AD0DF95AA62
SHA-512:	A081711E5DAC8E77014023C042C84616F84F2AA8DC93F94A7995812CE2D5A3B067077C483E703CF7C4AD317B1FF4B12C3060FC33C727252CE5B7672EABBA4DF
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....4.Y.=.....*\.....

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$o-Solid Feed Stock Evaluation_.docx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	1.8270399412171197
Encrypted:	false
SSDEEP:	3:Rl/ZdzcCVl//tlclkXlolRhlXln:RtZxWk14P
MD5:	066EAF455BB4CBC23C499AF83D7C92EB
SHA1:	75AC762773A704B3E890CD02B7B8F89EE068DDC2
SHA-256:	47EE684F6BD787F6FDDCDDBBCC12DBD2E3568F9EE6A2AC9796B54AD0DF95AA62
SHA-512:	A081711E5DAC8E77014023C042C84616F84F2AA8DC93F94A7995812CE2D5A3B067077C483E703CF7C4AD317B1FF4B12C3060FC33C727252CE5B7672EABBA4DF
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....4.Y.=.....*\.....

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.711910442031405
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:	Bio-Solid Feed Stock Evaluation_.docx
File size:	28469
MD5:	a829fa8a85650dde608ada79d3ba4f11
SHA1:	22964385dc00646b24d1203b8d7c4520c8e7704c
SHA256:	08bcf8510cbfb3a81777399682e35f05046d285e7c401b9 7874f9149113ddc88
SHA512:	c2388a4b6a087f10a35bbba71958b8b3e3342ca818bfdb2 f6a3f4d04f1b42e696b4c294cab07cf55b75d1ff4d66852b ed35e08f89255a3798a259f1db4bf4a70
SSDEEP:	384:r+B8tLLwWWAh22FyidZIMURWzHYGTzvNxt/ZtNN 4CRc4/NodMyXTzf:rBLLws82FrlPRKTpxllN4GNbe
File Content Preview:	PK.....!..!.]p.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:52:08.624069929 CEST	60152	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:08.696279049 CEST	53	60152	8.8.8.8	192.168.2.3
May 4, 2021 21:52:09.015103102 CEST	57544	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:09.065540075 CEST	53	57544	8.8.8.8	192.168.2.3
May 4, 2021 21:52:10.219959974 CEST	55984	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:10.271389961 CEST	53	55984	8.8.8.8	192.168.2.3
May 4, 2021 21:52:10.427999973 CEST	64185	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:10.498090982 CEST	53	64185	8.8.8.8	192.168.2.3
May 4, 2021 21:52:11.457957983 CEST	65110	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:11.506858110 CEST	53	65110	8.8.8.8	192.168.2.3
May 4, 2021 21:52:12.525136948 CEST	58361	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:12.573875904 CEST	53	58361	8.8.8.8	192.168.2.3
May 4, 2021 21:52:14.179151058 CEST	63492	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:14.227716923 CEST	53	63492	8.8.8.8	192.168.2.3
May 4, 2021 21:52:16.153858900 CEST	60831	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:16.203943968 CEST	53	60831	8.8.8.8	192.168.2.3
May 4, 2021 21:52:17.550607920 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:17.610881090 CEST	53	60100	8.8.8.8	192.168.2.3
May 4, 2021 21:52:18.137170076 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:18.208787918 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 21:52:19.166042089 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:19.222877979 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 21:52:19.927901030 CEST	50141	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:19.980820894 CEST	53	50141	8.8.8.8	192.168.2.3
May 4, 2021 21:52:20.176446915 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:20.233649969 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 21:52:21.487370968 CEST	53023	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:21.537960052 CEST	53	53023	8.8.8.8	192.168.2.3
May 4, 2021 21:52:22.194715023 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:22.253542900 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 21:52:23.024149895 CEST	49563	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:23.086242914 CEST	53	49563	8.8.8.8	192.168.2.3
May 4, 2021 21:52:24.025109053 CEST	51352	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:24.086288929 CEST	53	51352	8.8.8.8	192.168.2.3
May 4, 2021 21:52:26.208239079 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:26.267613888 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 21:52:28.377373934 CEST	59349	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:28.426177025 CEST	53	59349	8.8.8.8	192.168.2.3
May 4, 2021 21:52:29.336983919 CEST	57084	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:29.385871887 CEST	53	57084	8.8.8.8	192.168.2.3
May 4, 2021 21:52:30.848551035 CEST	58823	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:30.897841930 CEST	53	58823	8.8.8.8	192.168.2.3
May 4, 2021 21:52:33.650832891 CEST	57568	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:33.699486971 CEST	53	57568	8.8.8.8	192.168.2.3
May 4, 2021 21:52:34.779993057 CEST	50540	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:34.836891890 CEST	53	50540	8.8.8.8	192.168.2.3
May 4, 2021 21:52:35.957417965 CEST	54366	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:36.006494045 CEST	53	54366	8.8.8.8	192.168.2.3
May 4, 2021 21:52:37.128276110 CEST	53034	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:37.180418015 CEST	53	53034	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:52:38.255739927 CEST	57762	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:38.308357000 CEST	53	57762	8.8.8.8	192.168.2.3
May 4, 2021 21:52:43.173784018 CEST	55435	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:43.235239029 CEST	53	55435	8.8.8.8	192.168.2.3
May 4, 2021 21:52:46.948877096 CEST	50713	53	192.168.2.3	8.8.8.8
May 4, 2021 21:52:46.998903990 CEST	53	50713	8.8.8.8	192.168.2.3
May 4, 2021 21:53:04.843822002 CEST	56132	53	192.168.2.3	8.8.8.8
May 4, 2021 21:53:04.903740883 CEST	53	56132	8.8.8.8	192.168.2.3
May 4, 2021 21:53:21.584486008 CEST	58987	53	192.168.2.3	8.8.8.8
May 4, 2021 21:53:21.658561945 CEST	53	58987	8.8.8.8	192.168.2.3
May 4, 2021 21:53:27.835124016 CEST	56579	53	192.168.2.3	8.8.8.8
May 4, 2021 21:53:27.835844040 CEST	60633	53	192.168.2.3	8.8.8.8
May 4, 2021 21:53:27.884354115 CEST	53	60633	8.8.8.8	192.168.2.3
May 4, 2021 21:53:27.893630981 CEST	53	56579	8.8.8.8	192.168.2.3
May 4, 2021 21:53:29.448121071 CEST	61292	53	192.168.2.3	8.8.8.8
May 4, 2021 21:53:29.500988960 CEST	53	61292	8.8.8.8	192.168.2.3
May 4, 2021 21:53:34.958740950 CEST	63619	53	192.168.2.3	8.8.8.8
May 4, 2021 21:53:35.017502069 CEST	53	63619	8.8.8.8	192.168.2.3
May 4, 2021 21:54:05.237024069 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 21:54:05.299891949 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 21:54:07.219696045 CEST	61946	53	192.168.2.3	8.8.8.8
May 4, 2021 21:54:07.286463976 CEST	53	61946	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 5992 Parent PID: 792

General

Start time:	21:52:15
Start date:	04/05/2021
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:	0xfc0000
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

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	66B6977C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\88D6A842.png	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	66A95805	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$o-Solid Feed Stock Evaluation_.docx	success or wait	1	66A95805	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\88D6A842.png	0	12912	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 e4 00 00 00 51 08 06 00 00 00 c2 50 0a 4b 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 7f ed 35 71 00 00 31 f0 49 44 41 54 78 5e ed 7d 09 7c 53 55 f6 ff cd cb cb be 74 a3 1b a5 0b 65 17 c4 a5 94 45 44 5c 18 44 60 2a 8a 58 a5 62 45 11 19 07 9d fe fc c9 6f 64 c6 bf 21 6e b8 5b 15 15 19 44 2a 76 98 0e d6 81 02 05 11 61 dc 45 64 14 44 14 81 b2 17 4a 69 d3 36 7b f2 f2 f2 ff de 97 a6 24 5d 93 b4 4d eb 98 3b 9f 8c 34 b9 cb b9 e7 9e 73 ee b9 e7 9c 7b 2e ab d7 eb 09 2d ba 77 b6 dd 41 44 fc 5f 09 2b 1b 4a dc bc f0 5d a4 44 30 10 14 06 18 96 10 9e 5b 45 78	.PNG........IHDR.......Q.....P.K....sRGB.........pHYs.....+.....tEXtSoftware.Microsoft Office..5q..1.IDATx^.}.|SU.....t....e....ED\.D`*.X.bE.....od..!n.[...D*v.....a.Ed.D....Ji.6{.....$]..M..;..4.....s....{.....-.w..AD._.+.J..].D0.....[Ex	success or wait	1	66A95805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Bio-Solid Feed Stock Evaluation_.docx	5372	12912	success or wait	1	66A95805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	66AA8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	66AA8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	66AA8A84	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	66A95805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	66A95805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1FAB7	success or wait	1	66A95805	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	66A95805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	66A95805	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	66A95805	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	66A95805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	66A95805	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	66A95805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1FAB7	1FAB7	binary	04 00 00 00 68 17 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 C4 A4 B7 7E 6A 41 D7 01 B7 FA 01 00 B7 FA 01 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	66A95805	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 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	66A95805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2021-05-04T21:52	success or wait	1	66A95805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	1955539754 0	success or wait	1	66A95805	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	1386479631	1386479632	success or wait	1	66A95805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1386479632	1386479633	success or wait	1	66A95805	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	66A95805	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	66A95805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	66A95805	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	66A95805	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	66A95805	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	wpd doc	success or wait	1	66A95805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1FAB7	1FAB7	binary	04 00 00 00 68 17 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 C4 A4 B7 7E 6A 41 D7 01 B7 FA 01 00 B7 FA 01 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 68 17 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 B7 FA 01 00 B7 FA 01 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	66A95805	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 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 FF FF FF FF 00 00 00 00 00 00 00 00				

Disassembly