ID: 679656
Sample Name:
SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:58:49
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Sigma Signatures 4
Snort Signatures 4
Joe Sandbox Signatures 5
AV Detection 5
System Summary 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 8
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
World Map of Contacted IPs 11
General Information 11
Warnings 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\73B779F7-DFB2-4207-86EE-503E84D76CFE 12
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0000.doc 13
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{095E6AB2-2F3E-400A-8AB1-757286E704FA}.tmp 13
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{9D89F239-4B3E-4452-8626-5B399ECB38A1}.tmp 13
C:\Users\user\AppData\Local\Temp\~DF01E2A729CC5FF1F3.TMP 13
C:\Users\user\AppData\Local\Temp\~DF4745CB5E195353BD.TMP 14
C:\Users\user\AppData\Local\Temp\~DFB49F3A3334AD4AFF.TMP 14
C:\Users\user\AppData\Local\Temp\~DFC3DCC4E415EA4647.TMP 14
C:\Users\user\AppData\Local\Temp\~DFCD0699F2B9716C34.TMP 15
C:\Users\user\AppData\Local\Temp\~DFD31E0F4A4C0282F1.TMP 15
C:\Users\user\AppData\Local\Temp\~DFFCD145A10D131B7E.TMP 15
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc.LNK 16
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat 16
C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm 16
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex 16
C:\Users\user\Desktop\~$curiteInfo.com.Trojan.GenericKD.61181694.26250.doc 17
Static File Info 17
General 17
File Icon 17
Static OLE Info 17
General 17
OLE File "SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc" 17
Indicators 17
Streams 18
Stream Path: \x1CompObj, File Type: data, Stream Size: 72 18
General 18
Stream Path: \x1Ole, File Type: data, Stream Size: 20 18
General 18
Stream Path: \x1Ole10Native, File Type: data, Stream Size: 202653 18
General 18
Stream Path: \x3ObjInfo, File Type: data, Stream Size: 6 18
General 18
Network Behavior 18
Statistics 19
System Behavior 19

Copyright Joe Security LLC 2022

Analysis Process: WINWORD.EXEPID: 4356, Parent PID: 756 19
General 19
File Activities 19
File Created 19
File Deleted 19
File Read 19
Registry Activities 20
Key Created 20
Key Value Created 20
Key Value Modified 21
Disassembly 24

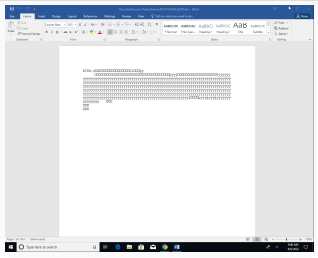
Windows Analysis Report

SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc

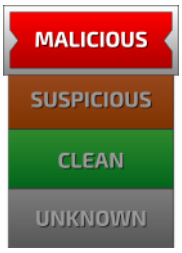
Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc
Analysis ID:	679656
MD5:	c14c4c6af1f9c42..
SHA1:	d4f4d0ee949a1a..
SHA256:	2386084b54b517.
Tags:	doc
Infos:	



Detection

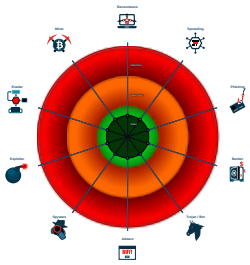


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Document contains OLE streams w…
- Document misses a certain OLE str…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 4356 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

Copyright Joe Security LLC 2022

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

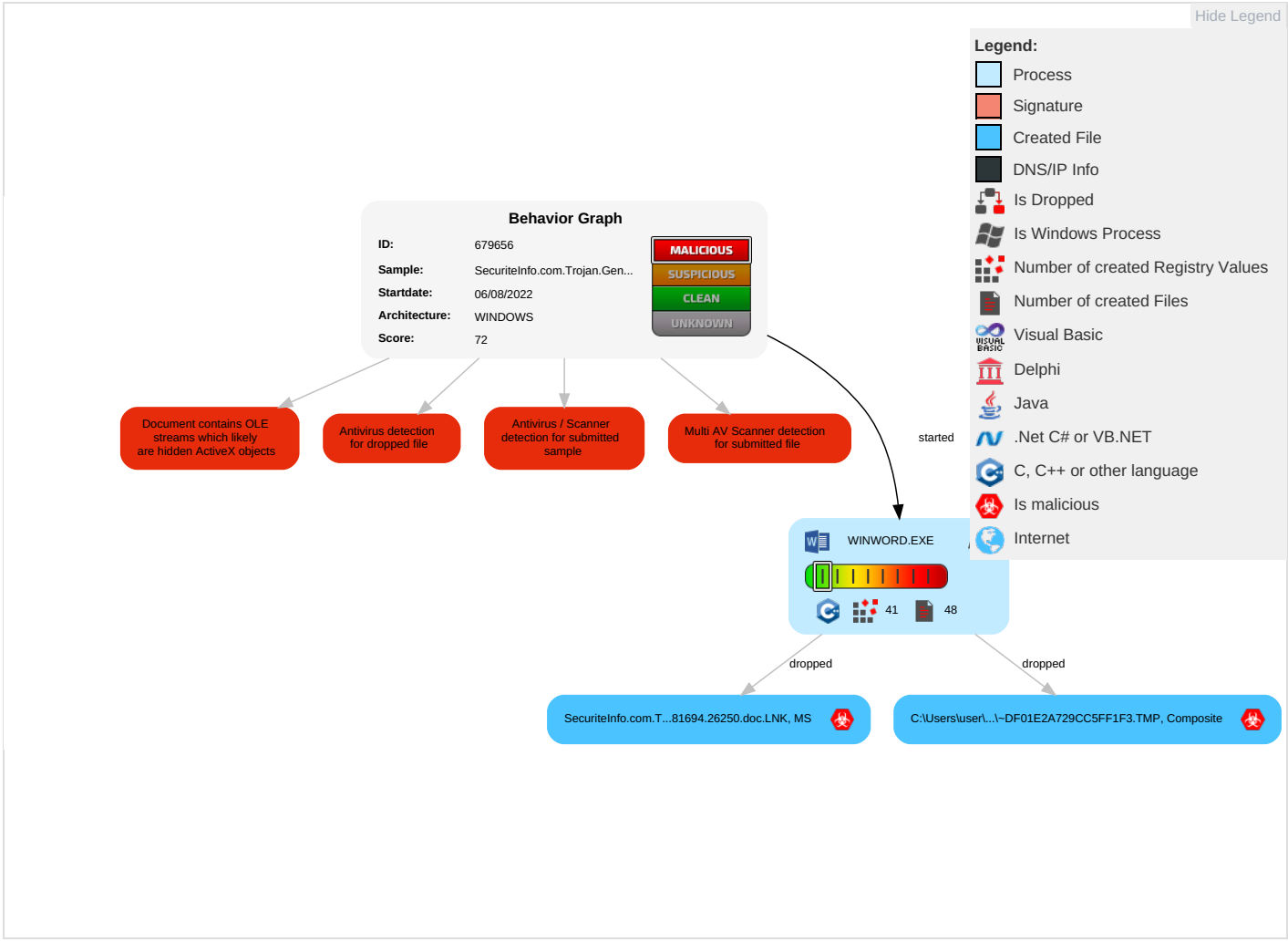
System Summary

Document contains OLE streams which likely are hidden ActiveX objects

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	1 Extra Window Memory Injection	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	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	1 Obfuscated Files or Information	LSASS Memory	2 System Information Discovery	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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Extra Window Memory Injection	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

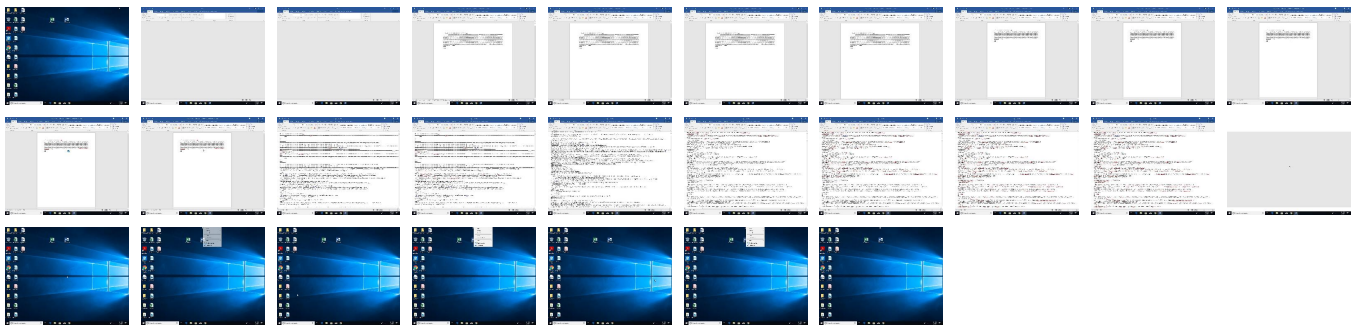
Behavior Graph

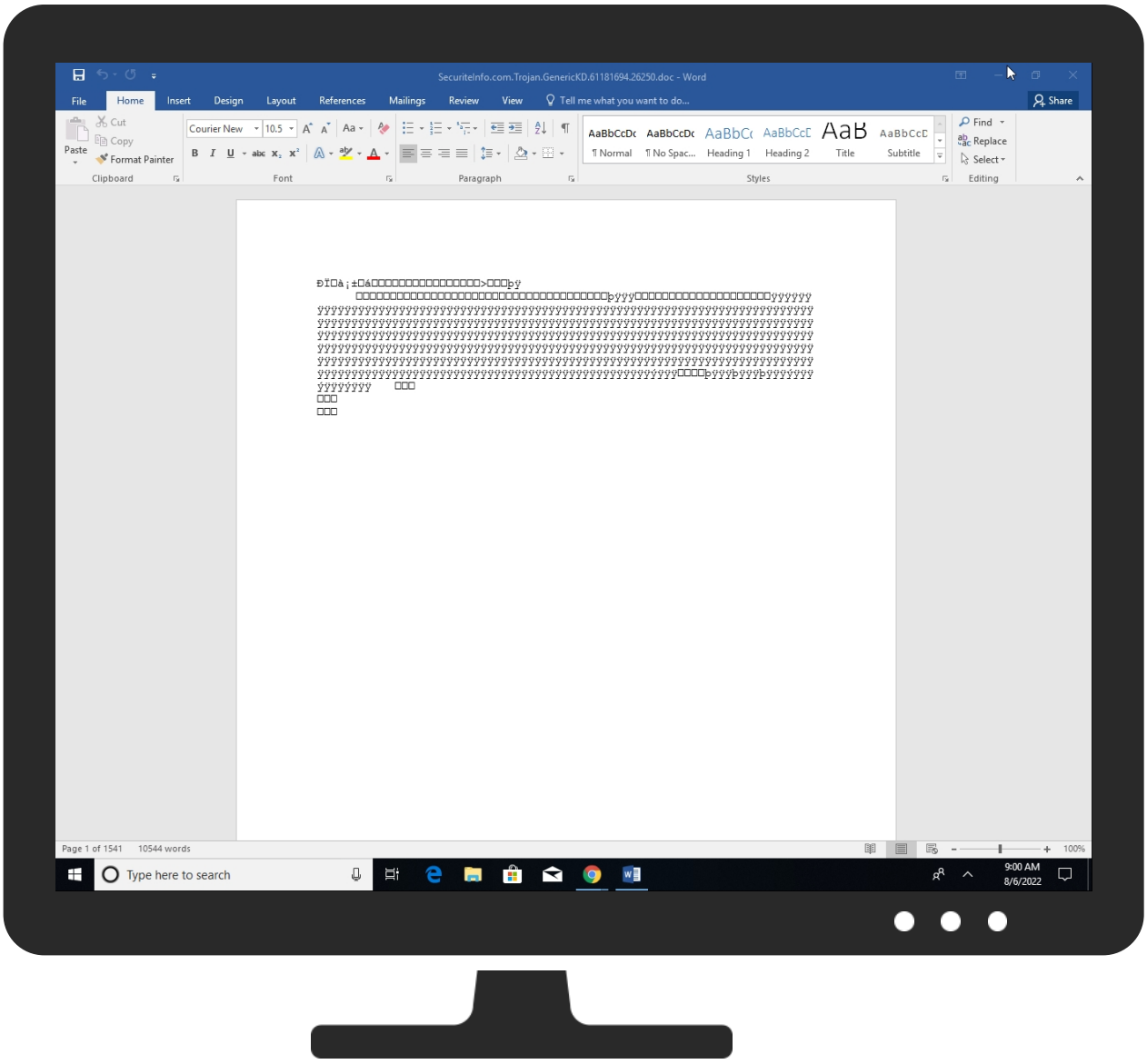


Screenshots

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
SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc	30%	Virustotal		Browse
SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc	33%	ReversingLabs	ByteCode-JAVA.Downloader.BanLoad	
SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc	100%	Avira	EXP/JAVA.Banload.VPDV.Gen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF01E2A729CC5FF1F3.TMP	100%	Avira	EXP/JAVA.Banload.VPDV.Gen	

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://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%	Avira URL Cloud	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://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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://login.microsoftonline.com/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://shell.suite.office.com:1443	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://autodiscover-s.outlook.com/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://roaming.edog.	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://cdn.entity.	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://powerlift.acompli.net	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lookup.onenote.com/lookup/geolocation/v1	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://cortana.ai	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://api.aadrm.com/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://api.microsoftstream.com/api/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://cr.office.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://graph.ppe.windows.net	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://my.microsoftpersonalcontent.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://messaging.engagement.office.com/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://web.microsoftstream.com/video/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://dataservice.o365filtering.com/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://ncus.contentsync.	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://weather.service.msn.com/data.aspx	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://apis.live.net/v5.0/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://messaging.lifecycle.office.com/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://management.azure.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://outlook.office365.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://wus2.contentsync.	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://api.office.net	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://entitlement.diagnostics.office.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://outlook.office.com/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://outlook.office365.com/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://webshell.suite.office.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://management.azure.com/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://graph.windows.net/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://devnull.onenote.com	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://messaging.action.office.com/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://ncus.pagecontentsync.	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://messaging.office.com/	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	73B779F7-DFB2-4207-86EE-503E84D76CFE.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679656
Start date and time: 06/08/202208:58:49	2022-08-06 08:58:49 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.GenericKD.61181694.26250.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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.winDOC@1/16@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.88.191, 52.109.76.35
- 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, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net

Copyright Joe Security LLC 2022

- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

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\73B779F7-DFB2-4207-86EE-503E84D76CFE

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):	5.3581546684794175
Encrypted:	false
SSDEEP:	1536:wcQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:j1Q9DQe+zuXYr
MD5:	B1E7CAFAB46D92C5B6794D5287677CEA
SHA1:	A058027B46B89273053952A91DA3FD8C1EDCFF6A
SHA-256:	AE4C11DD80DD86F303DECCA18A64EC0E1714673B9760FF02966C5239CBEC2315
SHA-512:	6923523DE54206F0C7156DC1E0B510D58B1717A4918BEFDE5F56E963F1B04A175D464EB18280110EF98053CF3C231432B6732E0F84030BF02D303DE0B9EA3958
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="2022-08-06T06:59:51">.. Build: 16.0.15601.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0000.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	414720
Entropy (8bit):	5.086778293300462
Encrypted:	false
SSDEEP:	6144:Fzg1Zdb0eFjrZCqKxJzvBZrEyk5vgkK/xGw3gNDjP4Bjz8huyFsan:1g39/v4b7/Hk5v18T3g+z8hu6
MD5:	18D932229A2A5DEA4B51BDD4B39A0768
SHA1:	135804A0ED7B86DC54404DC190DEA252218C74F0
SHA-256:	7D12D8D891EBEBCB269C2F9E9B454631AAF6DB24BBF9723D5785A8F9E339C479
SHA-512:	B8F4A319ED2B324868977F8B635B987EE8D84F0C199BB986F8E123243C28723BEE017D6F7A279865E878A4EC423440E5C5A324BC19697478B9FD62DD706F5067
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{095E6AB2-2F3E-400A-8AB1-757286E704FA}.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\Content.Word\~WRS{9D89F239-4B3E-4452-8626-5B399ECB38A1}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3676082633089806
Encrypted:	false
SSDEEP:	3:IiiiiiiiiiVeldI43lnl/bl//l/fl/9vvvvvvvvvvFl/l/lAqsDNjPl3lldHzlb5:Iiiiiiiiii8l+4cc8++lwG3qu
MD5:	AFDDA8CDFF4887A60DC8B478267D8A99
SHA1:	98CC8EC45ED062FB6315002E4123728B85DD0D90
SHA-256:	E209B417A91368042F6B9678ED20CE00CB5BF1497E467B8F27C4E059EE92F188
SHA-512:	B4271BF10CD0F15A89B3BFF6ADE9BCF657F7E785BF719507A257C5E629783FE84020AA01C01A4E50EF1A0B2CB743F56AAC1595D642098A21466173949699A792
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...(...p.r.a.t.e.s.h...p..... ...."...&...*.....>...B..... .....

C:\Users\user\AppData\Local\Temp\~DF01E2A729CC5FF1F3.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.969176466640856
Encrypted:	false
SSDEEP:	3072:O1FlTuC5EDTEEr1+1hkzQ4QKMg7B9Bpk6he6m78UakgaQ+vfr97/Xke:O1FlC2hkBrBiD9zXke
MD5:	C14C4C6AF1F9C4214691279C2F6FA13C
SHA1:	D4F4D0EE949A1AFF38DE302A3F5AA09749C4D89E
SHA-256:	2386084B54B517DFF1092496D4D4E5B558CF2EA50D51944BB8AC1F13FA1BBC05
SHA-512:	6416627E5E2488DC2A19C9F198BB813A159FD728986223DE4B210EA21687CDA3DF9284E3CDDF272AE48EADFAF288C30B7E7DFA1E98E88F779CE04C6A23D3B5C3
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DF4745CB5E195353BD.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFB49F3A3334AD4AFF.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFC3DCC4E415EA4647.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0

Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFCD0699F2B9716C34.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFD31E0F4A4C0282F1.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFFCD145A10D131B7E.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Trojan.GenericKD.61181694.26250.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 15:31:46 2022, mtime=Sat Aug 6 14:59:54 2022, atime=Sat Aug 6 14:59:48 2022, length=207360, window=hide
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	4.706698391088796
Encrypted:	false
SSDEEP:	24:8hpWIVt9f6qOpfkAISKV6HqOpfsDzr7aB6m:8hpSbxzISKAHbxKyB6
MD5:	C03E3C482236883D48124CD218B1C91D
SHA1:	859AC19F931D50BC8DAB04BA8E9EDF496067482E
SHA-256:	935882ED0DCBD2985716D16703CA863D765782EFD4579797C98E7DFA33B9E998
SHA-512:	F145E48874B9AB2B2EAFC8A6EE7F95A9BE2550AD2AB510B21CA55D1858EEB20672D5664D23C69ED3A80376857E69C58466A389866442A115478B2F5CDCAD298F
Malicious:	**true**
Preview:	L.....F.... .....3.."..... .....*.....+....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Ur.....:.....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..Ur.....S.....>...h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..Ur.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..*...Uy. .SECURI~1.DOC.....hT...Uy.....h.....<...S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D...6.1.1.8.1.6.9.4...2.6.2.5.0...d.o.c.....z.....-.....y.....>.S.....C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc..K.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D...6.1.1.8.1.6.9.4...2.6.2.5.0...d.o.c.....:...,.LB.)...As...`.....X.....992547.....!a..%.H.VZAj...6.....-..

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):	155
Entropy (8bit):	4.946678056348873
Encrypted:	false
SSDEEP:	3:bDuMJluscb3iALykTU9Tgj0aGCmX1n8b3iALykTU9Tgj0aGCv:bCVmsdoaGmmsdoaGs
MD5:	276484603B7E536B42A3AFB99563CD66
SHA1:	301AF6F3C88C7D2E50ABE8A4F251BC85E2F6C634
SHA-256:	64659BCDEEDBC678ED69203047818A4687642B94E249836C08680EF5308E6586
SHA-512:	A3D44EA7CB34FD9AB9A019CF6716A54D921A38FFBD72D0FD8D99E167D2C3E4DCE20321B8776E14AF13A722CF0E19CC73DA0F2FBB10D8610FCAD20CF84898A21B
Malicious:	false
Preview:	[folders]..Templates.LNK=0..SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc.LNK=0..[doc]..SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.132062010112871
Encrypted:	false
SSDEEP:	3:Rl/ZdctptBlqK0RlGltlllt7TJlp/l5:RtZ6tpUplG3tdrpr
MD5:	44CC4D1143B8FAC67A98705F1ECE3D75
SHA1:	8F2F79364AF92729E5100A36AB4FC49606DBC710
SHA-256:	995032F32828988FCF2A0D87F09CA803994BCBF4391CC28BCAE9316F6B2C57D3
SHA-512:	4FE53331695A74D3322DEA321B5D6283E202DA4B3827F13FA0328CD2F92590F346A58F412188DA4F1B8721C945BB8D48E0307822E811FD2E379AFA77306D7177
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....,A..".....H.....6C.....,]..#.....,Y..$.....$...

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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$curiteInfo.com.Trojan.GenericKD.61181694.26250.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.132062010112871
Encrypted:	false
SSDEEP:	3:Rl/ZdctptBlqK0RlGltlllt7TJlp/l5:RtZ6tpUplG3tdrpr
MD5:	44CC4D1143B8FAC67A98705F1ECE3D75
SHA1:	8F2F79364AF92729E5100A36AB4FC49606DBC710
SHA-256:	995032F32828988FCF2A0D87F09CA803994BCBF4391CC28BCAE9316F6B2C57D3
SHA-512:	4FE53331695A74D3322DEA321B5D6283E202DA4B3827F13FA0328CD2F92590F346A58F412188DA4F1B8721C945BB8D48E0307822E811FD2E379AFA77306D7177
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....,A..".....H.....6C.....]..#.....,Y..$.....$...

Static File Info

General

File type:	Composite Document File V2 Document, Cannot read section info
Entropy (8bit):	7.969176466640856
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc
File size:	207360
MD5:	c14c4c6af1f9c4214691279c2f6fa13c
SHA1:	d4f4d0ee949a1aff38de302a3f5aa09749c4d89e
SHA256:	2386084b54b517dff1092496d4d4e5b558cf2ea50d51944bb8ac1f13fa1bbc05
SHA512:	6416627e5e2488dc2a19c9f198bb813a159fd728986223de4b210ea21687cda3df9284e3cddf272ae48eadfaf288c30b7e7dfa1e98e88f779ce04c6a23d3b5c3
SSDEEP:	3072:O1FlTuC5EDTEEr1+1hkzQ4QKMg7B9Bpk6he6m78UakgaQ+vfr97/Xke:O1FlC2hkBrBiD9zXke
TLSH:	6A1423FE72B07535C52383361A844188D513CD6A171D736215B2B1D66CFB4CAFB3AAAC
File Content Preview:	.....>.....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc"

Indicators

Has Summary Info:	
Application Name:	None
Encrypted Document:	False

Contains Word Document Stream:	False
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:	False

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 72

General

Stream Path:	\x1CompObj
File Type:	data
Stream Size:	72
Entropy:	3.8231129765226823
Base64 Encoded:	False
Data ASCII:	. . . . / . { . . . Z @ . . . . P a c k a g e . . . . P a c k a g e . 9 q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 a7 0d f2 2f c0 ce 11 92 7b 08 00 09 5a e3 40 08 00 00 00 50 61 63 6b 61 67 65 00 00 00 00 00 08 00 00 00 50 61 63 6b 61 67 65 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x1Ole, File Type: data, Stream Size: 20

General

Stream Path:	\x1Ole
File Type:	data
Stream Size:	20
Entropy:	0.8475846798245739
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	01 00 00 02 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x1Ole10Native, File Type: data, Stream Size: 202653

General

Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	202653
Entropy:	7.996742729733093
Base64 Encoded:	True
Data ASCII:	. . . . . T V D N O S Y U K R B L U R M D H H G J C Y C Q W W F H I E Q Y U M D E O D F M R C I C V J U T H H A C P C I . J A R . C : \\ U s e r s \\ M I C R O S O F T \\ A p p D a t a \\ L o c a l \\ M i c r o s o f t \\ W i n d o w s \\ I N e t C a c h e \\ C o n t e n t . W o r d \\ T V D N O S Y U K R B L U R M D H H G J C Y C Q W W F H I E Q Y U M D E O D F M R C I C V J U T H H A C P C I . J A R . . . . . C : \\ U s e r s \\ M I C R O S ~ 1 \\ A p p D a t a \\ L o c a l \\ T e m p \\ { 7 2 D 4 C F D C - 4 8 2
Data Raw:	99 17 03 00 02 00 54 56 44 4e 4f 53 59 55 4b 52 42 4c 55 52 4d 44 48 48 47 4a 43 59 43 51 57 57 46 48 49 45 51 59 55 4d 44 45 4f 44 46 4d 52 43 49 43 56 4a 55 54 48 48 41 43 50 43 49 2e 4a 41 52 00 43 3a 5c 55 73 65 72 73 5c 4d 49 43 52 4f 53 4f 46 54 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 49 4e 65 74 43 61 63 68 65 5c 43

Stream Path: \x3ObjInfo, File Type: data, Stream Size: 6

General

Stream Path:	\x3ObjInfo
File Type:	data
Stream Size:	6
Entropy:	1.7924812503605778
Base64 Encoded:	False
Data ASCII:	@ . . . . .
Data Raw:	40 00 03 00 01 00

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 4356, Parent PID: 756

General

Target ID:	0
Start time:	08:59:48
Start date:	06/08/2022
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:	0x240000
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\tstC84C.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\tstC947.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\tstCA13.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\tstCADF.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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstC84C.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstC947.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstCA13.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstCADF.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\Desktop\~$curiteInfo.com.Trojan.GenericKD.61181694.26250.doc	success or wait	1	65925805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.6118 1694.26250.doc	unknown	14	success or wait	2	65B82FF3	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.61181694.26250.doc	unknown	4	success or wait	16	65B8253D	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0000.doc	unknown	512	success or wait	775	65925805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0000.doc	unknown	512	success or wait	1	65925805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0000.doc	unknown	512	success or wait	1	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\2551C	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\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Consolas	binary	02 0B 06 09 02 02 04 03 02 04	success or wait	1	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2551C	2551C	binary	04 00 00 00 04 11 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 54 2A DE A5 AD A9 D8 01 1C 55 02 00 1C 55 02 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	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 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	65925805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2022-08-06T09:00	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_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2551C	2551C	binary	04 00 00 00 04 11 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 54 2A DE A5 AD A9 D8 01 1C 55 02 00 1C 55 02 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 04 11 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 1C 55 02 00 1C 55 02 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	65925805	unknown

Copyright Joe Security LLC 2022

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

Copyright Joe Security LLC 2022

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 FF FF FF FF 00 00 00 00 00 00 00 00				

Disassembly

No disassembly

Copyright Joe Security LLC 2022