

JoeSandbox Cloud BASIC



**ID:** 680530

**Sample Name:**

SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf

**Cookbook:**

defaultwindowsofficecookbook.jbs

**Time:** 18:51:07

**Date:** 08/08/2022

**Version:** 35.0.0 Citrine

## Table of Contents

Table of Contents	2
Windows Analysis Report SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Initial Sample	3
Sigma Signatures	4
Snort Signatures	4
Joe Sandbox Signatures	4
AV Detection	4
Exploits	4
Software Vulnerabilities	4
System Summary	4
Mitre Att&ck Matrix	4
Behavior Graph	5
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
URLs from Memory and Binaries	7
World Map of Contacted IPs	10
General Information	10
Warnings	10
Simulations	11
Behavior and APIs	11
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASNs	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\F79DE4CE-3D38-4A51-B300-A0A52CA0A936	11
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Content.Word\~WRS{C94F2438-4712-4EDB-BA13-F546C0F4C19F}.tmp	11
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Content.Word\~WRS{D3E63778-DEB8-4D19-866C-1D5344BC51ED}.tmp	12
C:\Users\user\AppData\Local\Temp\Client.exe	12
C:\Users\user\AppData\Local\Temp\Client.exe:Zone.Identifier	12
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf.LNK	13
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	13
C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm	13
C:\Users\user\Desktop\~\$curiteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf	14
Static File Info	14
General	14
File Icon	14
Static RTF Info	14
Objects	14
Network Behavior	14
Statistics	15
System Behavior	15
Analysis Process: WINWORD.EXEPID: 5144, Parent PID: 756	15
General	15
File Activities	15
File Created	15
File Deleted	15
Registry Activities	15
Key Created	15
Key Value Created	16
Key Value Modified	17
Disassembly	20

# Windows Analysis Report

SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf

## Overview

### General Information

Sample Name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf
Analysis ID:	680530
MD5:	a5b0c571197ee2..
SHA1:	a4355fe45e321b..
SHA256:	00915bcbff87b2e..
Tags:	rtf
Infos:	

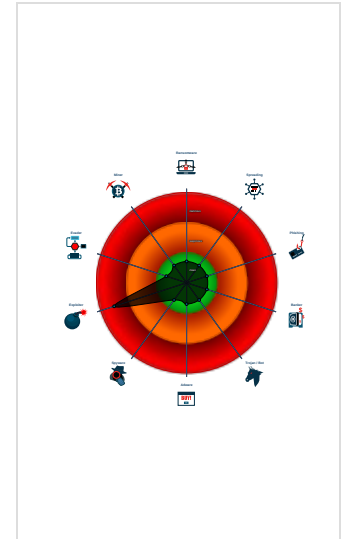
### Detection

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

### Signatures

Document exploit detected (creates...
Document exploit detected (drops P...
Malicious sample detected (through...
Office process drops PE file
PE file has nameless sections
Machine Learning detection for drop...
Found suspicious RTF objects
Found potential equation exploit (CV...
PE file contains section with specia...
Yara signature match
Drops PE files
PE file contains sections with non-s...

### Classification



## Process Tree

- System is w10x64
- WINWORD.EXE (PID: 5144 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- cleanup

## Malware Configuration

No configs have been found

## Yara Signatures

### Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf	MAL_RTF_Embedded_OLE_PE	Detects a suspicious string often used in PE files in a hex encoded object stream	Florian Roth	<ul style="list-style-type: none"><li>0x178c:\$a1: 546869732070726f6772616d2063616e6e6f742062652072756e20696e204444f53206d6f6465</li><li>0x16f0:\$m1: 4d5a90000300000004000000ffff</li></ul>
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embedding one of the object mostly observed in exploit documents.	ditekSHen	<ul style="list-style-type: none"><li>0x1276:\$obj2: \objdata</li><li>0x1e867e:\$obj2: \objdata</li><li>0x2c8c94:\$obj3: \objupdate</li><li>0x8e3:\$obj4: \objemb</li><li>0x1e7ceb:\$obj4: \objemb</li></ul>

## Sigma Signatures

 No Sigma rule has matched

## Snort Signatures

 No Snort rule has matched

## Joe Sandbox Signatures

### AV Detection



Machine Learning detection for dropped file

### Exploits



Found potential equation exploit (CVE-2017-11882)

### Software Vulnerabilities



Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

### System Summary



Malicious sample detected (through community Yara rule)

Office process drops PE file

PE file has nameless sections

Found suspicious RTF objects

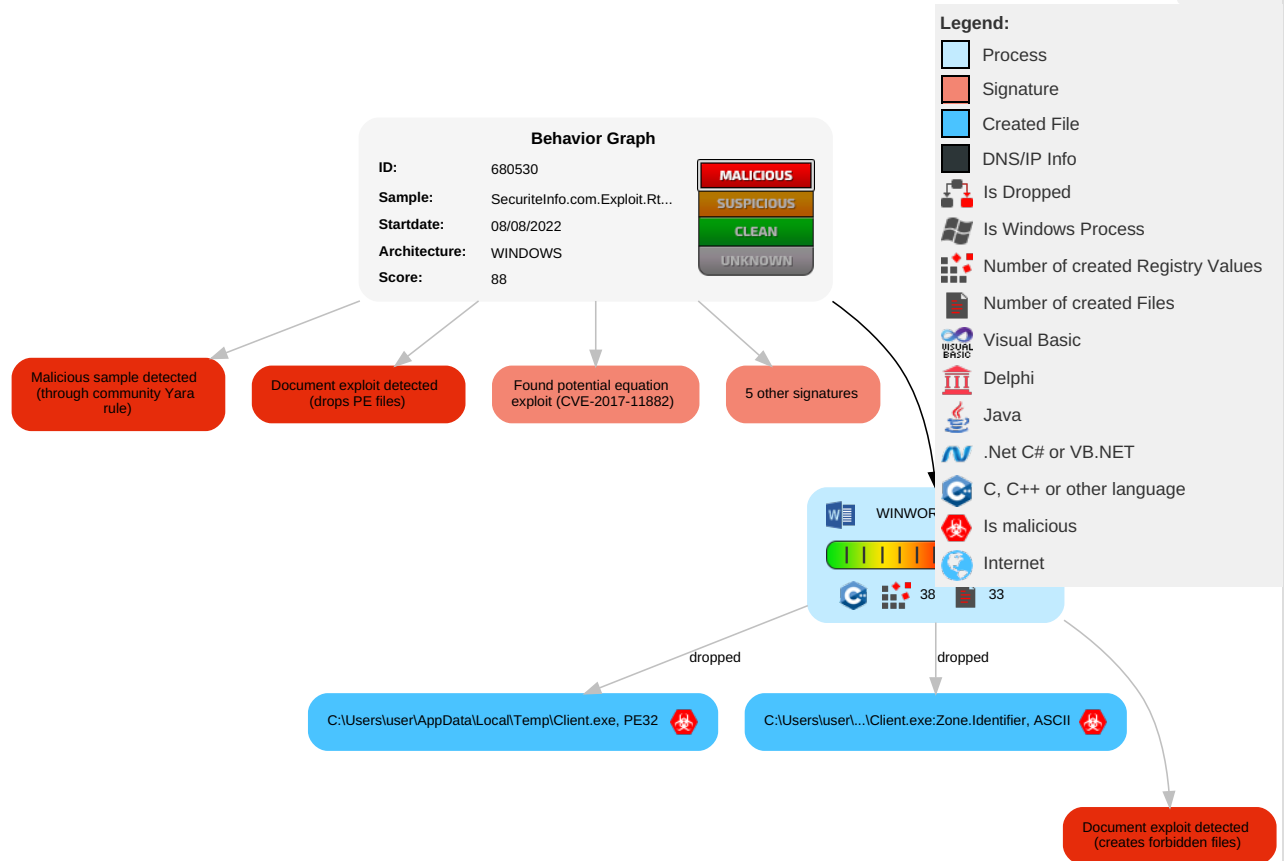
PE file contains section with special chars

## 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	<b>3</b> <a href="#">Exploitation for Client Execution</a>	Path Interception	Path Interception	<b>1</b> <a href="#">Masquerading</a>	OS Credential Dumping	<b>1</b> <a href="#">File and Directory Discovery</a>	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	<b>2</b> <a href="#">Software Packing</a>	LSASS Memory	<b>2</b> <a href="#">System Information Discovery</a>	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)	<b>1</b> <a href="#">Obfuscated Files or Information</a>	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

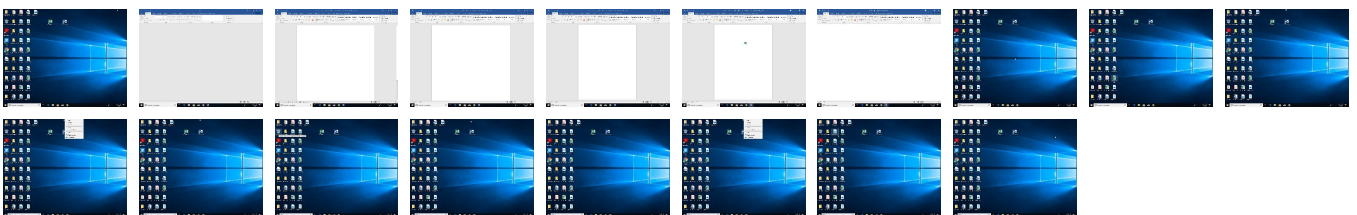
Hide Legend

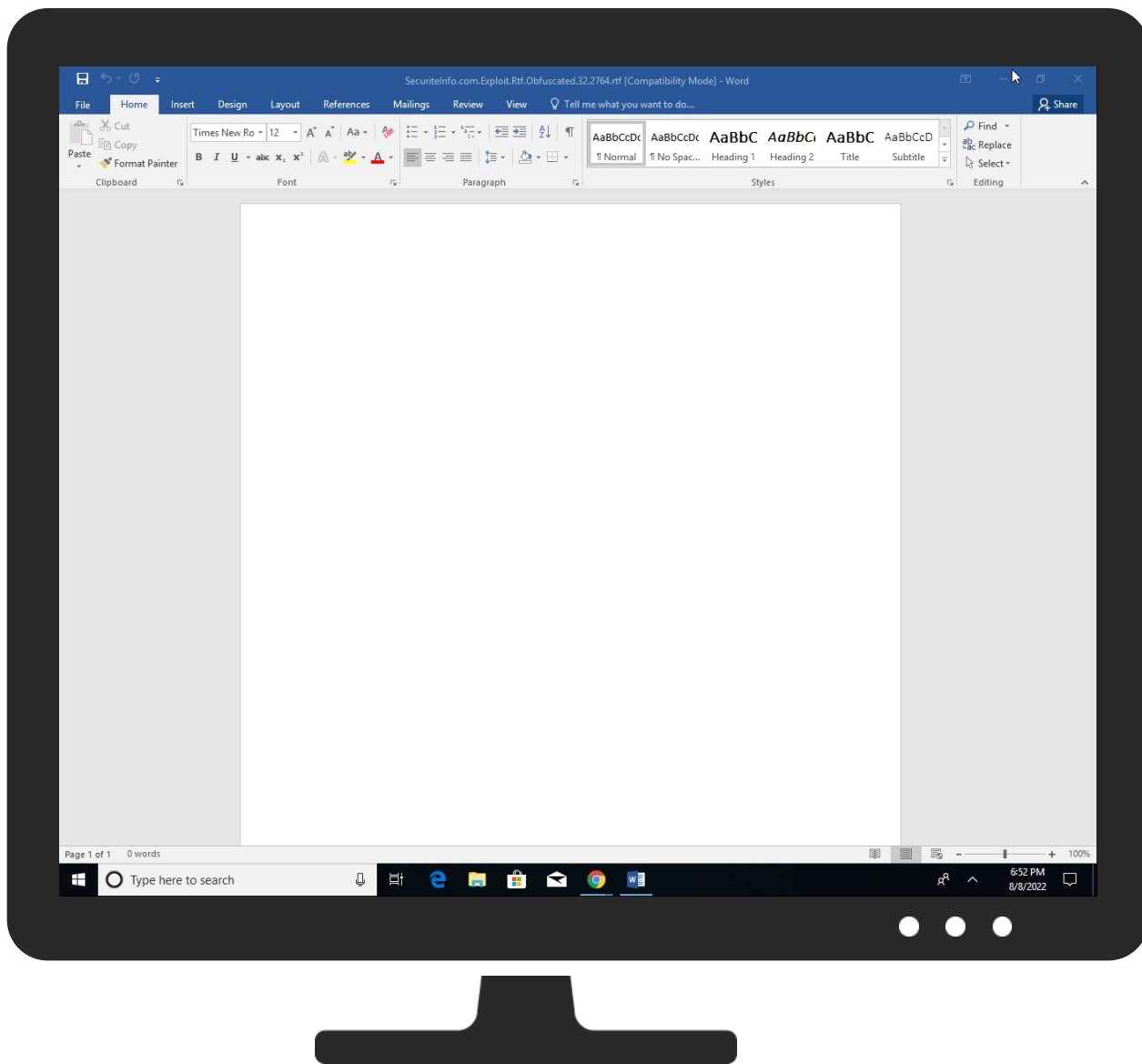


## Screenshots

### Thumbnails

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





## Antivirus, Machine Learning and Genetic Malware Detection


### Initial Sample

 No Antivirus matches

### Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Client.exe	100%	Joe Sandbox ML		

### 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	

Source	Detection	Scanner	Label	Link
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://asgsmproxyapi.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.diagnosticsddf.office.com	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
http://https://login.microsoftonline.com/	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
http://https://shell.suite.office.com:1443	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
http://https://autodiscover-s.outlook.com/	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
http://https://roaming.edog.	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
http://https://cdn.entity.	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
http://https://api.addins.omex.office.net/appinfo/query	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
http://https://powerlift.acompli.net	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
http://https://cortana.ai	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
<a href="http://https://cloudfiles.onenote.com/upload.aspx">http://https://cloudfiles.onenote.com/upload.aspx</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile">http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://entitlement.diagnosticsdf.office.com">http://https://entitlement.diagnosticsdf.office.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy">http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://api.aadrm.com/">http://https://api.aadrm.com/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• URL Reputation: safe	unknown
<a href="http://https://ofcrecsvcapi-int.azurewebsites.net/">http://https://ofcrecsvcapi-int.azurewebsites.net/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• URL Reputation: safe	unknown
<a href="http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies">http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://api.microsoftstream.com/api/">http://https://api.microsoftstream.com/api/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://insertmedia.bing.office.net/images/hosted?host=office&amp;adt=strict&amp;hostType=Immersive">http://https://insertmedia.bing.office.net/images/hosted?host=office&amp;adt=strict&amp;hostType=Immersive</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://cr.office.com">http://https://cr.office.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h">http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• Avira URL Cloud: safe	low
<a href="http://https://portal.office.com/account/?ref=ClientMeControl">http://https://portal.office.com/account/?ref=ClientMeControl</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://graph.ppe.windows.net">http://https://graph.ppe.windows.net</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://res.getmicrosoftkey.com/api/redemptionevents">http://https://res.getmicrosoftkey.com/api/redemptionevents</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• URL Reputation: safe	unknown
<a href="http://https://powerlift-frontdesk.acompli.net">http://https://powerlift-frontdesk.acompli.net</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• URL Reputation: safe	unknown
<a href="http://https://tasks.office.com">http://https://tasks.office.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://officeci.azurewebsites.net/api/">http://https://officeci.azurewebsites.net/api/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• URL Reputation: safe	unknown
<a href="http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work">http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://my.microsoftpersonalcontent.com">http://https://my.microsoftpersonalcontent.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• Avira URL Cloud: safe	unknown
<a href="http://https://store.office.cn/addinstemplate">http://https://store.office.cn/addinstemplate</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• URL Reputation: safe	unknown
<a href="http://https://api.aadrm.com">http://https://api.aadrm.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• URL Reputation: safe	unknown
<a href="http://https://outlook.office.com/autosuggest/api/v1/init?cvid=">http://https://outlook.office.com/autosuggest/api/v1/init?cvid=</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://globaldisco.crm.dynamics.com">http://https://globaldisco.crm.dynamics.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://messaging.engagement.office.com/">http://https://messaging.engagement.office.com/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech">http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://dev0-api.acompli.net/autodetect">http://https://dev0-api.acompli.net/autodetect</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• URL Reputation: safe	unknown
<a href="http://https://www.odwebp.svc.ms">http://https://www.odwebp.svc.ms</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• URL Reputation: safe	unknown
<a href="http://https://api.diagnosticsdf.office.com/v2/feedback">http://https://api.diagnosticsdf.office.com/v2/feedback</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://api.powerbi.com/v1.0/myorg/groups">http://https://api.powerbi.com/v1.0/myorg/groups</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://web.microsoftstream.com/video/">http://https://web.microsoftstream.com/video/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://api.addins.store.officeppe.com/addinstemplate">http://https://api.addins.store.officeppe.com/addinstemplate</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• URL Reputation: safe	unknown
<a href="http://https://graph.windows.net">http://https://graph.windows.net</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://dataservice.o365filtering.com/">http://https://dataservice.o365filtering.com/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• URL Reputation: safe	unknown
<a href="http://https://officesetup.getmicrosoftkey.com">http://https://officesetup.getmicrosoftkey.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• URL Reputation: safe	unknown
<a href="http://https://analysis.windows.net/powerbi/api">http://https://analysis.windows.net/powerbi/api</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://prod-global-autodetect.acompli.net/autodetect">http://https://prod-global-autodetect.acompli.net/autodetect</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	• URL Reputation: safe	unknown
<a href="http://https://outlook.office365.com/autodiscover/autodiscover.json">http://https://outlook.office365.com/autodiscover/autodiscover.json</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios">http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech">http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices">http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high



Name	Source	Malicious	Antivirus Detection	Reputation
<a href="https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json">http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://https://ncus.contentsync">http://https://ncus.contentsync</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false">http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://webdir.online.lync.com/autodiscover/autodiscover/service.svc/root/">http://https://webdir.online.lync.com/autodiscover/autodiscover/service.svc/root/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="http://weather.service.msn.com/data.aspx">http://weather.service.msn.com/data.aspx</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://apis.live.net/v5.0/">http://https://apis.live.net/v5.0/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks">http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios">http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://messaging.lifecycle.office.com/">http://https://messaging.lifecycle.office.com/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml">http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://management.azure.com">http://https://management.azure.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://outlook.office365.com">http://https://outlook.office365.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://wus2.contentsync">http://https://wus2.contentsync</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="https://incidents.diagnostics.office.com">http://https://incidents.diagnostics.office.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://clients.config.office.net/user/v1.0/ios">http://https://clients.config.office.net/user/v1.0/ios</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://insertmedia.bing.office.net/odc/insertmedia">http://https://insertmedia.bing.office.net/odc/insertmedia</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://o365auditrealtimeingestion.manage.office.com">http://https://o365auditrealtimeingestion.manage.office.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://outlook.office365.com/api/v1.0/me/Activities">http://https://outlook.office365.com/api/v1.0/me/Activities</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://api.office.net">http://https://api.office.net</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://incidents.diagnosticsdf.office.com">http://https://incidents.diagnosticsdf.office.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://asgmsproxyapi.azurewebsites.net/">http://https://asgmsproxyapi.azurewebsites.net/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="https://clients.config.office.net/user/v1.0/android/policies">http://https://clients.config.office.net/user/v1.0/android/policies</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://entitlement.diagnostics.office.com">http://https://entitlement.diagnostics.office.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json">http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://substrate.office.com/search/api/v2/init">http://https://substrate.office.com/search/api/v2/init</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://outlook.office.com/">http://https://outlook.office.com/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://storage.live.com/clientlogs/uploadlocation">http://https://storage.live.com/clientlogs/uploadlocation</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://outlook.office365.com/">http://https://outlook.office365.com/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://webshell.suite.office.com">http://https://webshell.suite.office.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive">http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://substrate.office.com/search/api/v1/SearchHistory">http://https://substrate.office.com/search/api/v1/SearchHistory</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://management.azure.com/">http://https://management.azure.com/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://messaging.lifecycle.office.com/getcustommessage16">http://https://messaging.lifecycle.office.com/getcustommessage16</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://clients.config.office.net/c2r/v1.0/InteractiveInstallation">http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://login.windows.net/common/oauth2/authorize">http://https://login.windows.net/common/oauth2/authorize</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile">http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="https://graph.windows.net/">http://https://graph.windows.net/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://api.powerbi.com/beta/myorg/imports">http://https://api.powerbi.com/beta/myorg/imports</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://devnull.onenote.com">http://https://devnull.onenote.com</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://messaging.action.office.com/">http://https://messaging.action.office.com/</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
<a href="https://ncus.pagecontentsync">http://https://ncus.pagecontentsync</a>	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://r4.res.office365.com/footprintconfig/v1.7/scripts/ fpconfig.json	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
http://https://messaging.office.com/	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high
http:// https://dataservice.protection.outlook.com/PolicySync/ PolicySync.svc/SyncFile	F79DE4CE-3D38-4A51-B300-A0A52CA0A936.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information	
Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680530
Start date and time: 08/08/202218:51:07	2022-08-08 18:51:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.expl.winRTF@1/9@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 100%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>
Cookbook Comments:	<ul style="list-style-type: none"><li>• Found application associated with file extension: .rtf</li><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found Word or Excel or PowerPoint or XPS Viewer</li><li>• Attach to Office via COM</li><li>• Scroll down</li><li>• Close Viewer</li></ul>

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, 52.109.32.24, 52.109.88.39
- 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, cdn.onenote.net, eur ope.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- 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\F79DE4CE-3D38-4A51-B300-A0A52CA0A936

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):	5.358133405421376
Encrypted:	false
SSDEEP:	1536:UcQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:/1Q9DQe+zuXYr
MD5:	524DEB669CBD12BFA0E862F9FB78CCDC
SHA1:	4FAC81AE9AD7B129C238661E0E4F781E9ABC91B3
SHA-256:	BDD825B56D52BE60C4D50616B97EB23E3DE3BCB9D883AF7ED68395685AF4507B
SHA-512:	35C6BD6E1DFE62F89124107E8F75773C10025164A3C9D0D9ECECF84078240F5D9B73E1E3FB54084EA093855FDBCC559B20A7699A275855D905F44B662EB56341C
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="2022-08-08T16:52:11">.. 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.aspx</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="CIViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="CIViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="CIViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{C94F2438-4712-4EDB-BA13-F546C0F4C19F}.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:	DBB11419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..... ..... ..... .....

<b>C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{D3E63778-DEB8-4D19-866C-1D5344BC51ED}.tmp</b>	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	1.1393247452705433
Encrypted:	false
SSDEEP:	6:beKnc1EICIXiKNwDOxRAJgm7KmrRmvlw5Fr+ur8FrK:beOc1MCIXiO6Ox2JF5Rmvq5ZP8ZK
MD5:	2508CC81F5E9247B80C4FB3781394285
SHA1:	453AC54E5038EF8D30A585EB885652468B0992A4
SHA-256:	5A1936A4E61EFDC38F71EE6AE93A7537F589F2A2B2B71D898B2877ECE3374FC
SHA-512:	08A7D69CF5ADD926CB304D49A5B97757FE3CF7EFEB957654EB7718ADF69B46F2A1C40F9973197E71300419ECBD3F1B5EBE40F63C228B6E92EA0075C11E7A86AD
Malicious:	false
Reputation:	<b>moderate, very likely benign file</b>
Preview:	.).(.).(.).(.).5=..... .P.a.c.k.a.g.e.E.M.B.E.D.5=..... .U.n.k.n.o.w.n.E.M.B.E.D..... ..... ....."....<...>...@...F..... .....CJ..OJ..QJ..^J.....j....CJ..OJ..QJ..U..^J...<..CJ..OJ..QJ..^J...O J..QJ..^J.

C:\Users\user\AppData\Local\Temp\Client.exe  	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	979456
Entropy (8bit):	7.255901249909526
Encrypted:	false
SSDEEP:	12288:t1fPLY2Y841v3xqdanStZpGZh75x6OFMqnUDv2GTHPx2TZX5OHpCu9qvle:thDY2d4kE1x+qeZTZAZJcpv9W
MD5:	599BB05227A88A5C83E36E05D67DA0EA
SHA1:	663EBDC243BDF990D2950A0BCAB08CF316BDDFF50
SHA-256:	2D63CA0053F446B5531AA5703C136586CEC0635994FD5DEE51DF7FE51DF58EB4
SHA-512:	5E1826F4EB4BD831A02DD705E2DF1ED1C082BB7E7D4486F6A4F34E6323F2942448EC3D2C56F516AA9A65AF71A2F4411D5BDA4764656E3C7B9776C0DF44DB7AE1
Malicious:	true
Antivirus:	<ul style="list-style-type: none"><li>Antivirus: Joe Sandbox ML, Detection: 100%</li></ul>
Reputation:	low
Preview:	MZ.....@.....!.L!This program cannot be run in DOS mode...\$.PE.L.....b.....".....0.....R.....@.....@..... ..@..... ..O.....`.....@.....H.....s.n=><v..F.....H.....@....._text...H.....L.....`rsr c.....@..@.....@......reloc.....@..B..... ..... .....

C:\Users\user\AppData\Local\Temp\Client.exe:Zone.Identifier 	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBC85A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443f98
Malicious:	true
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf.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=Tue Aug 9 00:52:12 2022, atime=Tue Aug 9 00:52:07 2022, length=2920194, window=hide
Category:	dropped
Size (bytes):	1240
Entropy (8bit):	4.746811657719839
Encrypted:	false
SSDEEP:	24:8pFo7u8/Pa/kfJoCn9U+QA95HCn9UkDrT7aB6m:8p69qvCna+n95HCnaSKB6
MD5:	1F66D0046017517FBB298B785E458174
SHA1:	0763BC76E9899DEC36D8826F7F3292883DF62A87
SHA-256:	D7D8FD1FD7E7918E65B21C3DE6BC78E74E0B01154E28815821D2184C47A0333D
SHA-512:	5B761C964501072DEA7C2236992BBDC65717F2F77C408F43230B958D05B44338344A54C1590D6764AAC76C7B7D03E5D160DDA097C3C09194CEFAEFCDEDFDE4
Malicious:	false
Preview:	L.....F....9[...3...M....m.....)....P.O. ....+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.....h.T....user.<.....Ny..U{.....S.....}.h.a.r.d.z.....~.1.....h.T....Desktop.h.....Ny..U{.....Y.....>.....Y6..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....2.....U...SECURI~1.RTF.....h.T...U...h.....b.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...R.t.f...O.b.f.u.s.c.a.t.e.d...3.2...2.7.6.4...r.t.f.....y......x.....>.S.....C:\Users\user\Desktop\SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf.J.....\.....\.....\D.e.s.k.t.o.p\l.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...R.t.f...O.b.f.u.s.c.a.t.e.d...3.2...2.7.6.4...r.t.f.....;..LB.)...As...`.....X.....284992.....!a.%H.VZAj.....-!a.%


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):	160
Entropy (8bit):	4.975057392169532
Encrypted:	false
SSDEEP:	3:bDuMJluscBcTLqjQWC0LXSdNFFomxWIMov8bcTLqjQWC0LXSdNFFov:bCVvTeS0LXS7N8wTeS0LXS7y
MD5:	3E8AC3467A1477A539CDEA8189236AAB
SHA1:	B66B713170E5B6356C249C6B0FDDBA263BA536C8
SHA-256:	F3DAE50CE58EF48DA30BD29C3450F9E9F6A9D86DBD807630025B85F767A3CC3B
SHA-512:	DE4754D2A05F58593AEC8B9BE5181A50289253E3EA5A4D2AE98F5C2A93CFA562B18D7BC3EBB56CE7603251F42882AC633B8E29B8DC50A0AA77D9F2C4602C8599
Malicious:	false
Preview:	[folders]..Templates.LNK=0..SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf.LNK=0..[misc?????]?..SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf.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):	2.0466224483025317
Encrypted:	false
SSDEEP:	3:RI/Zd9vM43ttLvKrBv/9nv2xCllXoIn:RtZ/R3tFSNtuUIWn
MD5:	667567BDE1E565AE3CCC8C2482092094
SHA1:	701815E43A23F2B76A9ED83E489BCA8EB3616D86
SHA-256:	FD5B9F8A37DB674A9EBE5D295443329E72DD1EA9F9B37E41A724652FF6F74C84


SHA-512:	1139FCEC9EA59E6640A6B9FA359CCE71270B6DBFE25BF6EB612716A54D5D4D1B1641A5414E8161A1B70B9704B3BC1814039115F0DB6E66ABB53F9D17CA213853
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....J+N.....J/N.....J.N.....

C:\Users\user\Desktop\~\$curiteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.0466224483025317
Encrypted:	false
SSDEEP:	3:RI/Zd9vM43tt7LvKrBv/9nv2xCllXoIn:RtZ/R3tFSNtuUIWn
MD5:	667567BDE1E565AE3CCC8C2482092094
SHA1:	701815E43A23F2B76A9ED83E489BCA8EB3616D86
SHA-256:	FD5B9F8A37DB674A9EBE5D295443329E72DD1EA9F9B37E41A724652FF674C84
SHA-512:	1139FCEC9EA59E6640A6B9FA359CCE71270B6DBFE25BF6EB612716A54D5D4D1B1641A5414E8161A1B70B9704B3BC1814039115F0DB6E66ABB53F9D17CA213853
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....J+N.....J/N.....J.N.....

Static File Info	
General	
File type:	Rich Text Format data, version 1, unknown character set
Entropy (8bit):	4.7600452351752605
TrID:	<ul style="list-style-type: none"><li>Rich Text Format (5005/1) 55.56%</li><li>Rich Text Format (4004/1) 44.44%</li></ul>
File name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf
File size:	2920194
MD5:	a5b0c571197ee2931e12f11caf138eff
SHA1:	a4355fe45e321b99274f8000c5ac9c08f7146b28
SHA256:	00915bcbff87b2e195e1547df8e1944cadcdc6aa46beb130bd5a960dff01c7e3
SHA512:	eff4fadba11f02724628b950cfe815347c019759f2b40ea8ce4c9dcbf13964ac3fdf76230a2a685b0a6c68d33fff24fa3f43f026b365e0efb7a4cbf992834b6c
SSDEEP:	24576:0u0HN0y/U6FoR5bjoPL/GWEuwJpiGOR2QGBI0s5mp1BRX56XRsH9dBwK3UFHzZ:z
TLSH:	07D5A67071B535C6E26F0172429FBC59521738C3B3C62D88815DEAF62ED4B7A7B81A0E
File Content Preview:	{\rtf1{\*\pnseclvl3\pndec\pnstart1\pnindent720\pnhang {\pntxta .}}{\*\pnseclvl4\pncltr\pnstart1\pnindent720\pnhang {\pntxta .}}}{\*\pnseclvl5\pndec\pnstart1\pnindent720\pnhang {\pntxtb ({\pntxta .})}}{\*\pnseclvl6\pncltr\pnstart1\pnindent720\pnhang {\pnt

File Icon	
	
Icon Hash:	74f4c4c6c1cac4d8

Static RTF Info									
Objects									
Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000129Ah	2	embedded	Package	979623	Client.exe	C:\Path\Client.exe	C:\Path\Client.exe	no
1	001E86A2h	2	embedded	Equation.3	3072				no

Network Behavior	
 No network behavior found	

# Statistics

No statistics

# System Behavior

Analysis Process: WINWORD.EXE PID: 5144, Parent PID: 756

## General

Target ID:	0
Start time:	18:52:08
Start date:	08/08/2022
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:	0x13a0000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

## File Activities

### File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory   synchronize	device	directory file   synchronous io non alert   open for backup ident   open reparse point	success or wait	1	659D977C	unknown

### File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\-\$curiteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf	success or wait	1	65905805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

## Registry Activities

### Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	65918A84	RegCreateKeyEx A
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	65918A84	RegCreateKeyEx A
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	65918A84	RegCreateKeyEx A
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	65905805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	65905805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\247BE	success or wait	1	65905805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	65905805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	65905805	unknown

Key Value Created
<ul style="list-style-type: none"> <li>• <b>Revenue Growth:</b> Increased sales volume and revenue.</li> <li>• <b>Customer Satisfaction:</b> Improved customer loyalty and repeat business.</li> <li>• <b>Operational Efficiency:</b> Streamlined processes and reduced costs.</li> <li>• <b>Market Penetration:</b> Expanded reach into new markets.</li> <li>• <b>Brand Reputation:</b> Enhanced brand image and credibility.</li> </ul>

[illegible]









