ID: 756114
Sample Name: SecuriteInfo.com.Exploit.CVE-2018-0798.4.29399.2797.rtf
Cookbook: default.jbs
Time: 16:49:09
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

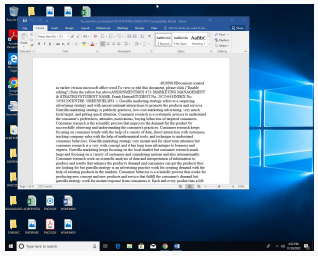
Windows Analysis Report

SecuriteInfo.com.Exploit.CVE-2018-0798.4.29399.2797.rtf

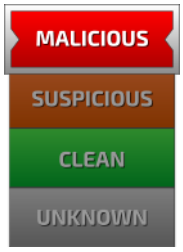
Overview

General Information

Sample Name:	SecuriteInfo.com.Exploit.CVE-2018-0798.4.29399.2797.rtf
Analysis ID:	756114
MD5:	9030afe25461e3..
SHA1:	a47f1de11c15e5..
SHA256:	b70c112ed968b0..
Tags:	rtf
Infos:	YARA



Detection

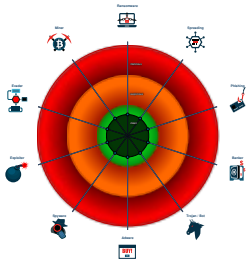


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through…
- Multi AV Scanner detection for subm…
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 6008 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.CVE-2018-0798.4.29399.2797.rtf	SUSP_INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embedding one of the object mostly observed in exploit (e.g. CVE-2017-11882) documents.	ditekSHen	• 0x5445:$obj2: \objdata • 0x5622:$obj3: \objupdate • 0x541e:$obj5: \objautlink

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.CVE-2018-0798.4.29399.2797.rtf	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x5445:$obj2: \objdata • 0x5622:$obj3: \objupdate • 0x541e:$obj5: \objautlink

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

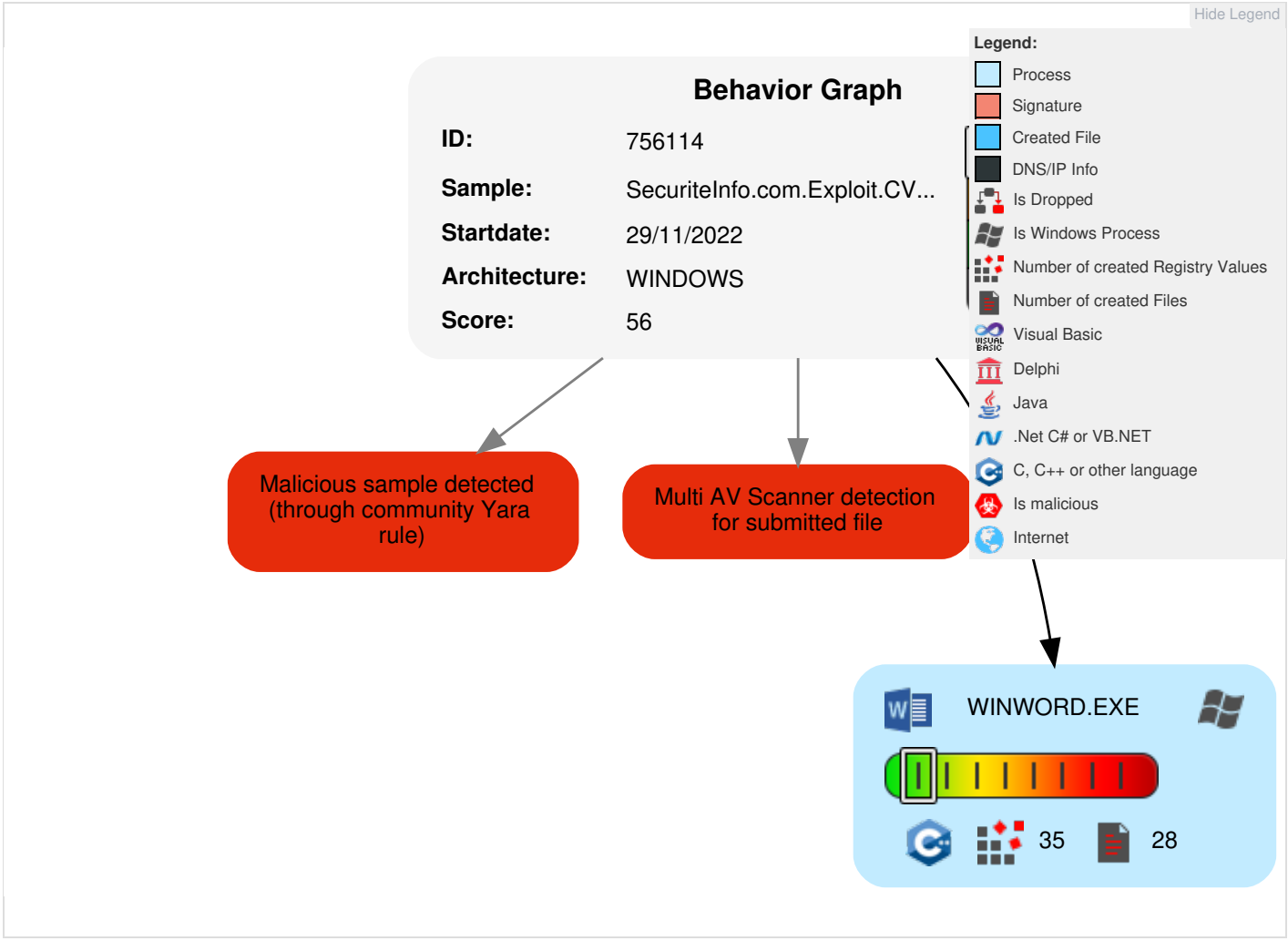
System Summary

Malicious sample detected (through community Yara rule)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	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	Rootkit	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

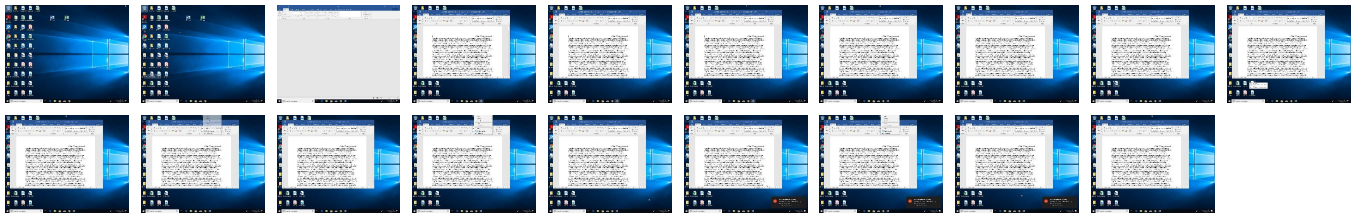
Behavior Graph

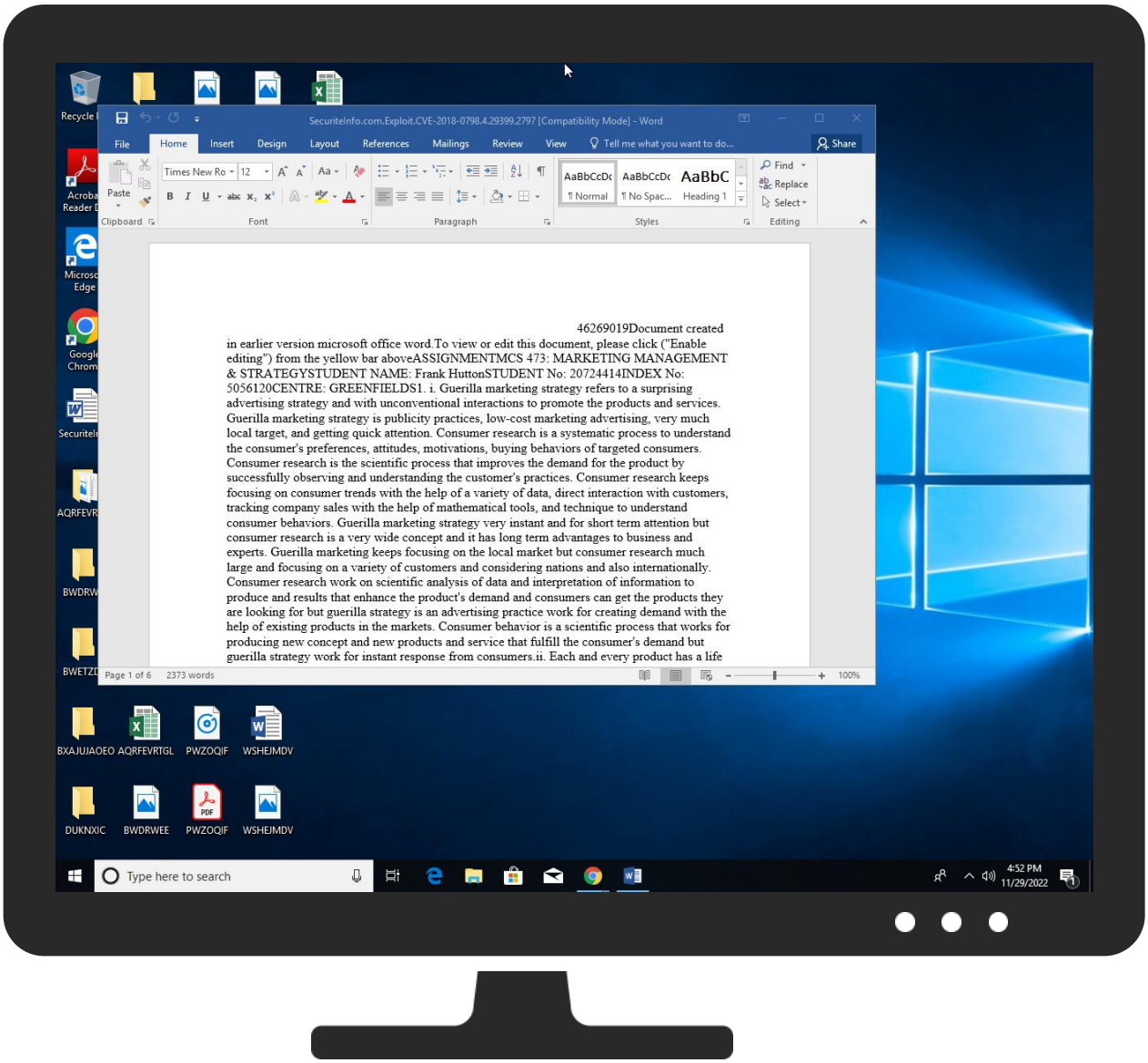


Screenshots

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.Exploit.CVE-2018-0798.4.29399.2797.rtf	31%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://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://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://api.scheduler.	0%	URL Reputation	safe	
http://https://my.microsoftpersonalcontent.com	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	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	

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	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://login.microsoftonline.com/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://shell.suite.office.com:1443	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://autodiscover-s.outlook.com/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://cdn.entity.	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://powerlift.acompli.net	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://cortana.ai	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cloudfiles.onenote.com/upload.aspx	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://api.aadrm.com/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://api.microsoftstream.com/api/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://cr.office.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://graph.ppe.windows.net	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://api.scheduler.	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://my.microsoftpersonalcontent.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://messaging.engagement.office.com/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://web.microsoftstream.com/video/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://dataservice.o365filtering.com/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://consent.config.office.com/consentcheckin/v1.0/consents	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://ncus.contentsync.	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://weather.service.msn.com/data.aspx	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://apis.live.net/v5.0/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://messaging.lifecycle.office.com/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://management.azure.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://outlook.office365.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://wus2.contentsync.	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://api.office.net	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://entitlement.diagnostics.office.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://outlook.office.com/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://outlook.office365.com/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://webshell.suite.office.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://management.azure.com/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://devnull.onenote.com	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messaging.action.office.com/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://ncus.pagecontentsync.	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high
http://https://messaging.office.com/	5C23899C-57D0-46BD-BBFE-0DB21569686F.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756114
Start date and time:	2022-11-29 16:49:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.CVE-2018-0798.4.29399.2797.rtf
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	6
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:	mal56.winRTF@1/6@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: .rtf

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- Excluded IPs from analysis (whitelisted): 52.109.76.141, 20.231.70.194, 20.224.201.79
- Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, config.officeapps.live.com, prod.configsvc1.live.com.akadns.net, nexus.officeapps.live.com, officeclient.microsoft.com, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: SecuriteInfo.com.Exploit.CVE-2018-0798.4.29399.2797.rtf

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\5C23899C-57D0-46BD-BBFE-0DB2 1569686F

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	149710
Entropy (8bit):	5.359454617114472
Encrypted:	false
SSDEEP:	1536:hL+C7/gUMB5BQguw/BQ9DQe+zQVk4F77nXmvid3XRcE6Lcz6S:w5Q9DQe+zCXzJ
MD5:	FEB719780ABDD7669810C28C66C938F7
SHA1:	6E63788A422BF66259A794725C347BD01084A328
SHA-256:	4FAA2B78852763410C3F2C9ACF5143CB7AA4C05B5AC430740F5ED22B4E7D4B70
SHA-512:	B5B0075E9F82659629949750CFAD871675A5905EC41A39372101379DCEE238F5DF43FFF6FAF81EDFF3579D1A10F4E7ADF9E59B5CF5BB66CB754EA139C54E422
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="2022-11-29T15:50:16">.. Build: 16.0.15913.30526-->.. <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:authentication="1">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. <o:ticket o:policy="MBI_SSL_SHORT" o:idprovider="1" o:target="[MAX.AuthHost]" o:headerValue="Passport1.4 from-PP='{}&p=''" />.. <o:ticket o:idprovider="3" o:headerValue="Bearer {}" o:resourceId="[MAX.ResourceId]" o:authorityUrl="[ADALAuthorityU

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.CVE-2018-0798.4.29399.2797.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 Aug 16 12:41:41 2022, mtime=Tue Nov 29 14:51:05 2022, atime=Tue Nov 29 14:51:00 2022, length=26570, window=hide
Category:	dropped
Size (bytes):	1260
Entropy (8bit):	4.673625813329463
Encrypted:	false
SSDEEP:	24:88b4ESRC5DCdPUAxbchcHCdBD4e5ek7aB6m:8Y4ES4CVjx0cHCzAhB6
MD5:	1B86048047F0B5DE84EB1DE1E80195C0
SHA1:	3E87F61F35E7C059EAFF47C4206C6F50E2927C23

SHA-256:	40DCC733BA62C689AE7548C9435DDDEFB101D94EDB7C0F939C196A3119647288
SHA-512:	37C8242BC6760974FDBC5694A266E01CEFC349ABA8CE44F0FD1BD1C96C4ED33E15ECE5EE32E468A45C930C112308E6E4FD172E7DAEC1B73A6AC2A4EDE794 0C5
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...L..u.....c....7M.`.....g.....1....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}UY~.....:.....:..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....U7m..user.<.....N..}UY~....#J.....j.o.n.e.s.....~.1.....U8m..Desktop.h.....N..}UY~.....Y.....>.....Ar..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....2..g..}Ua~ .SECURI~1.RTF.....U5m}Ua~....P.....)..S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...C.V.E.-.2.0.1.8.-.0.7.9.8...4...2.9.3.9.9...2.7.9.7... r.t.f.....}.....-.....|.....>.S.....C:\Users\user\Desktop\SecuriteInfo.com.Exploit.CVE-2018-0798.4.29399.2797.rtf..N.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e. I.n.f.o...c.o.m...E.x.p.l.o.i.t...C.V.E.-.2.0.1.8.-.0.7.9.8...4...2.9.3.9.9...2.7.9.7...r.t.f.....:..,.LB.)...As...`.....X.....210395.....!a..%.H.VZAj.....

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):	5.088217340833089
Encrypted:	false
SSDEEP:	3:bDuMJluscbcK+KX5C3FSmxWIMov8bcK+KX5C3FSv:bCVwKhXcJ8wKhXcm
MD5:	B5096C16B856E29A1E3FD0496AD7DE37
SHA1:	DDA79308DD6054E15CBC4B5BA9011BC2767CA5D5
SHA-256:	F60007FE1AFC15255C86F27BF4A096D056A3555756557C1CFA5ECF82FBDAC9EF
SHA-512:	CD75FAE398C9FF2062C9EAE9955E7678306B4902CA20703049CA13A02544C0532FD24CAC48902505C044BE2BEC5F84D833356353146B90A51E2D7B12621B152E
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..SecuriteInfo.com.Exploit.CVE-2018-0798.4.29399.2797.LNK=0..[misc??????]..SecuriteInfo.com.Exploit.CVE-2018-0798.4.29399.27 97.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):	2.1150565317044547
Encrypted:	false
SSDEEP:	3:Rl/Zdu4/Lt6/jp5lXlXtleKV/ttln:RtZ/Lt6/l5lXVt
MD5:	8D439B60EE3D036A98AE07C3B96A8201
SHA1:	5693F8FCCB47217E4A0AEA7FA3CFE98CDB0F9362
SHA-256:	A2AF9570E93C5F6576A18BC58418E1B0112DC0D190B49367EDFF69D68AB9C108
SHA-512:	E9E0DCF5D5F215B03446B745BAE28A651BBF567FF215E82AD5125205775D8498E385475D375E67D961E7C6251C2AF6796F0719BBC68E8B0774E6E0DF4D160FA5
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....|.....x.....|.....|.....

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	modified
Size (bytes):	20
Entropy (8bit):	2.8954618442383215
Encrypted:	false
SSDEEP:	3:QVNliGn:Q9rn
MD5:	C4F79900719F08A6F11287E3C7991493
SHA1:	754325A769BE6ECCC664002CD8F6BDB0D0B8CA4D
SHA-256:	625CA96CCA65A363CC76429804FF47520B103D2044BA559B11EB02AB7B4D79A8
SHA-512:	0F3C498BC7680B4C9167F790CC0BE6C889354AF703ABF0547F87B78FEB0BAA9F5220691DF511192B36AD9F3F69E547E6D382833E6BC25CDB4CD2191920970C5
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$curiteInfo.com.Exploit.CVE-2018-0798.4.29399.2797.rtf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1150565317044547
Encrypted:	false
SSDEEP:	3:Rl/Zdu4/Lt6/jp5lXlXtleKV/ttln:RtZ/Lt6/l5lXVt
MD5:	8D439B60EE3D036A98AE07C3B96A8201
SHA1:	5693F8FCCB47217E4A0AEA7FA3CFE98CDB0F9362
SHA-256:	A2AF9570E93C5F6576A18BC58418E1B0112DC0D190B49367EDFF69D68AB9C108
SHA-512:	E9E0DCF5D5F215B03446B745BAE28A651BBF567FF215E82AD5125205775D8498E385475D375E67D961E7C6251C2AF6796F0719BBC68E8B0774E6E0DF4D160FA5
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....|.....x.....|.....|.....

Static File Info

General

File type:	Rich Text Format data, version 1
Entropy (8bit):	5.597856428320499
TrID:	• Poser pose (12501/1) 58.12% • Rich Text Format (5005/1) 23.27% • Rich Text Format (4004/1) 18.61%
File name:	SecuriteInfo.com.Exploit.CVE-2018-0798.4.29399.2797.rtf
File size:	26570
MD5:	9030afe25461e39f11f8f7239217ca24
SHA1:	a47f1de11c15e5901110c29f318314ffbb65326a
SHA256:	b70c112ed968b0846a461d7d3c8e3681383fe28a8b5099c6201cb5bc263c2785
SHA512:	50b8108d0a23027cd59163784abeacb4a3cce4e9b160176786b420d0febcbd1046b24ca38061bc4bb0cd466a9fddf84e7fa0e3eb68866c7b18a01c717793e47e
SSDEEP:	384:6QMmdOFNYY0aaaIswqPeOrka1+fHQJ+t3rQkRhZfAlnjXYtG2eQkp5wDBhPjZ:WFx0XaIsnPRIa4fwJMKlnjXf2e54DDZ
TLSH:	6DC24C67F798133D478301D1765F2BE8EB2EA53923A095612C6C92782385CBA43377ED
File Content Preview:	{\rtf1.....{*\adjust2Value201371486 \;}.{\146269019Document created in earlier version microsoft office word.To view or edit this document, please click ("Enable editing") from the yellow bar aboveASSIGNMENTMCS 473: MARKETING MANAGEMENT & STRATEGY

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000544Fh								no

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 6008, Parent PID: 796

General

Target ID:	0
Start time:	16:51:01
Start date:	29/11/2022
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:	0xd0000
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	6624977C	unknown

File Path	Completion	Count	Source Address	Symbol

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	66188A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	66188A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	66188A84	RegCreateKeyExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

No disassembly