ID: 753420
Sample Name: SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:59:58
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

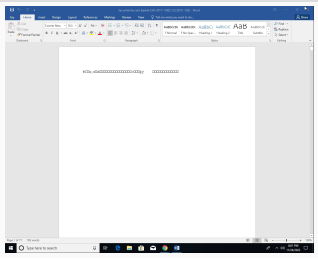
Windows Analysis Report

SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc

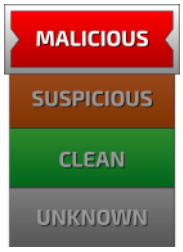
Overview

General Information

Sample Name:	SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc
Analysis ID:	753420
MD5:	d38967e524822d.
SHA1:	b2af456f879fba7..
SHA256:	5e458e56f23f18f..
Tags:	CVE-2017-11882 doc
Infos:	



Detection

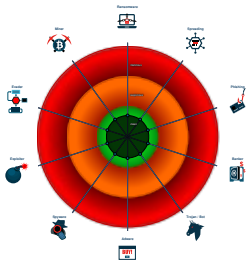


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 5020 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

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

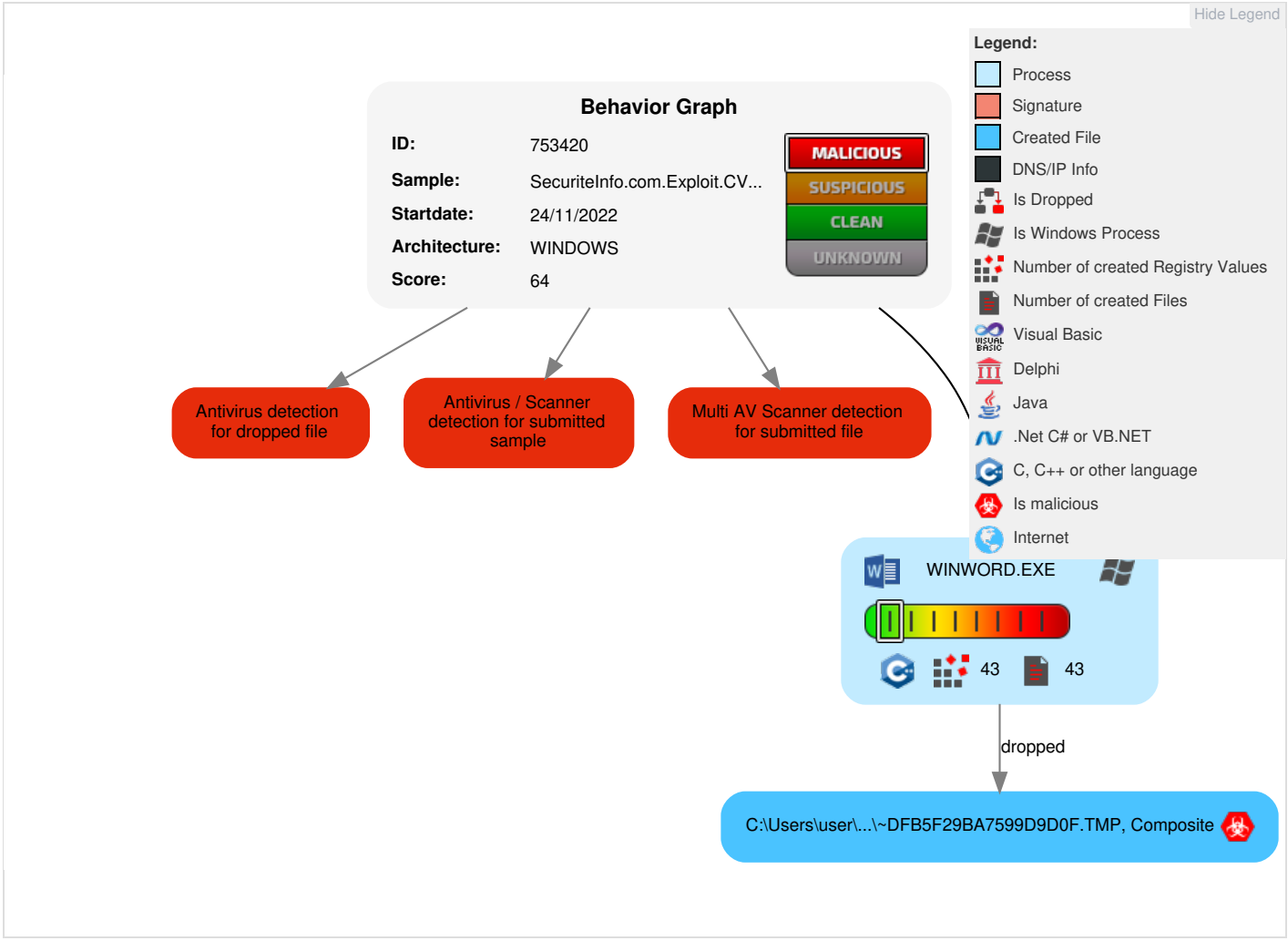
Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

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

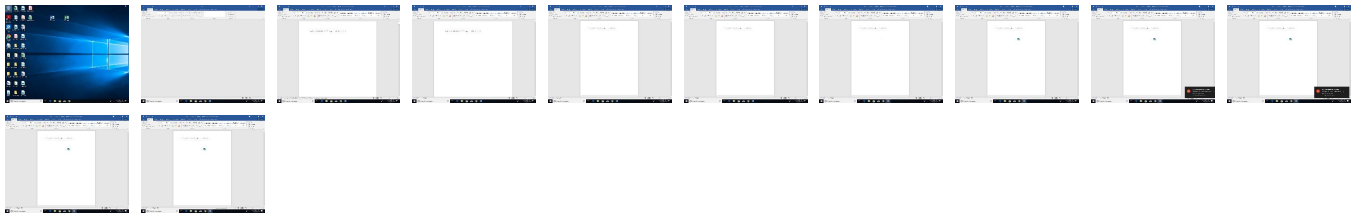
Behavior Graph

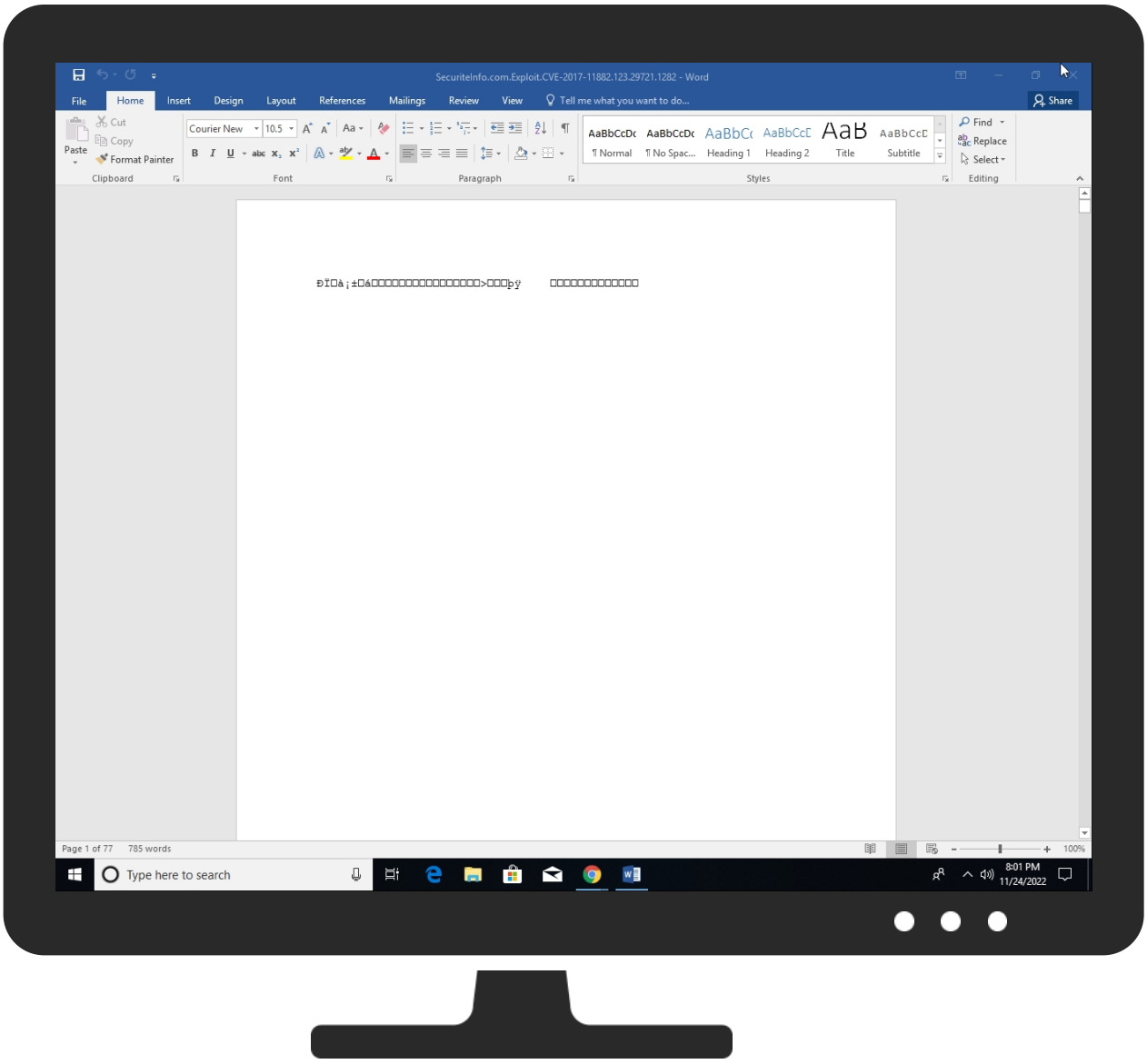


Screenshots

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-2017-11882.123.29721.1282.doc	54%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	
SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc	52%	Virustotal		Browse
SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc	100%	Avira	EXP/CVE-2017-11882.Gen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DFB5F29BA7599D9D0F.TMP	100%	Avira	EXP/CVE-2017-11882.Gen	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://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://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://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://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://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	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://login.microsoftonline.com/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://shell.suite.office.com:1443	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://autodiscover-s.outlook.com/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://cdn.entity.	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://cortana.ai	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://api.aadrm.com/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://api.microsoftstream.com/api/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://cr.office.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://graph.ppe.windows.net	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://api.scheduler.	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://my.microsoftpersonalcontent.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://messaging.engagement.office.com/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://web.microsoftstream.com/video/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://dataservice.o365filtering.com/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/autodiscover/autodiscover.json	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://consent.config.office.com/consentcheckin/v1.0/consents	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://ncus.contentsync.	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://weather.service.msn.com/data.aspx	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://apis.live.net/v5.0/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://messaging.lifecycle.office.com/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://management.azure.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://outlook.office365.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://wus2.contentsync.	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://api.office.net	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://entitlement.diagnostics.office.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://outlook.office.com/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://outlook.office365.com/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://webshell.suite.office.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://management.azure.com/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://devnull.onenote.com	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://messaging.action.office.com/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://ncus.pagecontentsync.	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high
http://https://messaging.office.com/	8DD21DB6-A354-43E1-AA05-383562B87248.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753420
Start date and time:	2022-11-24 19:59:58 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc
Cookbook file name:	defaultwindowsofficecookbook.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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	16
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:	mal64.winDOC@1/14@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 • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM

Warnings

- Max analysis timeout: 600s exceeded, the analysis took too long
- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, Microsoft.Photos.exe, MusNotifyIcon.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.109.76.141, 20.126.106.131, 20.223.225.174

- Excluded domains from analysis (whitelisted): www.bing.com, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, prod-w.nexus.live.com.akadns.net, login.live.com, config.officeapps.live.com, prod.configsvc1.live.com.akadns.net, settings-win.data.microsoft.com, nexus.officeapps.live.com, officeclient.microsoft.com, config.edge.skype.com, europe.configsvc1.live.com.akadns.net
- 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 NtReadVirtualMemory 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\8DD21DB6-A354-43E1-AA05-3835 62B87248

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):	5.359448137359727
Encrypted:	false
SSDEEP:	1536:DL+C7/gUMB5BQguw/BQ9DQe+zQVk4F77nXmvid3XRcE6Lcz6S:W5Q9DQe+zCXzJ
MD5:	9F524557C0D1416C15A2FFF45FEFC3B6
SHA1:	9AE5B80A5E3005C5BA39A5E9130CCB0A3226CD82
SHA-256:	CE92A8AC07BA95AFC263617A31A8EA3102AAA3F4E86C6681381E439CD910DB7F
SHA-512:	E9B3E61273679E7E9C516BF326FA0A5F240EAED1FFA369810BBA1585B49C3091A3FF300AC7EA1BF6F4C94CE515FACF64512C27254A2981CF3CDC4C02BA1FED23
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="2022-11-24T19:00:52">.. 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\Local\Temp\~DF20830712EE399E97.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\~DF22C9AF5F396B32E4.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\~DF3B50A295B66BD08B.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\~DF3F079023E26CE1AB.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\~DF7BF10879A29453F3.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\~DFB5F29BA7599D9D0F.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):	910336
Entropy (8bit):	6.01945829773662
Encrypted:	false
SSDEEP:	24576:5LMu/lUHGguNaUgjg+NkTgThiNkKBnv/E:51Kmg6RsOE
MD5:	D38967E524822D04257534078B0DC209
SHA1:	B2AF456F879FBA7DFFA694D9386F501883118822
SHA-256:	5E458E56F23F18FEB1E44F3EB3C15AB7D4D6CD9E937C72528DFCE9D5E195EA3C
SHA-512:	E6124B681EC75A45400EB822EA2F558B7B2D3CDFE6B3AFCCF4D03FE15E4934AD39AB8EF77DEE74ED4A20A506D3605DD606D5D91700013D8FD5419A51F1F98A5F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
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\~DFF0188A9052E2C15B.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.Exploit.CVE-2017-11882.123.29721.1282.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 12:41:30 2022, mtime=Thu Nov 24 18:01:01 2022, atime=Thu Nov 24 18:00:49 2022, length=910336, window=hide
Category:	dropped
Size (bytes):	1275
Entropy (8bit):	4.623082988143842
Encrypted:	false
SSDEEP:	24:8HLMKSa/KCdOmAqbcJHCdOwDQeFek7aB6m:8rMKVKC0qQHC9khB6
MD5:	80A9846FF8B7860B8360C6522C306F92
SHA1:	3DB08BF3813AC7F247C5A54C62822C71ACA7412B
SHA-256:	730343D2D4F9C88289A46D237203E77B82FBB9067AA018095E43459AE739892E
SHA-512:	EDB1473EDF3E75C55112E71FDC47C21C0AB8C5AA7A66A9B38532FD78FFBCA31B243C4FAF8B11E83D7489C64FC218180595697D5D01AC6280AD901D7B119963D
Malicious:	false
Preview:	L.....F.... .....(.u...7E..7.....$.7.....7....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..xU.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....U1m..user.<.....N..xU.....#J.....j.o.n.e.s.....~.1.....U2m..Desktop.h.....N..xU.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....xU.. .SECURI~1.DOC.....U0mxU.....P.....L.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.-.2.0.1.7.-.1.1.8.8.2...1.2.3...2.9.7.2.1...1.2.8.2...d.o.c.....-.....>.S.....C:\Users\user\Desktop\SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc..Q.....\.....\.....\.....\.....\.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.-.2.0.1.7.-.1.1.8.8.2...1.2.3...2.9.7.2.1...1.2.8.2...d.o.c.....:.,.LB.)...As...`.....X.....910646.....!a

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Generic INItialization configuration [doc]
Category:	dropped
Size (bytes):	159
Entropy (8bit):	4.9470059760402645
Encrypted:	false
SSDEEP:	3:bDuMJluscbcK+JiMXjEYdrXCmX1n8bcK+JiMXjEYdrXCv:bCVwKNcKwKNcl
MD5:	1EB5BE23C9F80FF12073FD8CC0905820
SHA1:	276033018F0E63FA3D0E544387276A6AA75905C7
SHA-256:	F8930A570B7580840EE7A3C469CEEBFC7DB7AAE538DF98FF22B7EE6D65A6AD8B
SHA-512:	001930C1A25BEA8EE8AD8820737DE73FC9431B67CD6DBC58595C94B18FB4441EAA302A496A72795CBCC0E7793120335B23B4562FE8266E1A5A42723FF9EEE7E7
Malicious:	false
Preview:	[folders]..Templates.LNK=0..SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.LNK=0..[doc]..SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.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):	2.406518452430825
Encrypted:	false
SSDEEP:	3:Rl/Zd15xd7ltl/tNLo/XolFH58lKzuKV:RtZ3v51LfV+2v
MD5:	EA97B7E1EDDA70476AD6C0001C4620AD
SHA1:	E5F90B01FE660C591C4384F345139295FC4300FB
SHA-256:	B80A405D74E591376F8C11E0F6E819A410E55090176BEE9723978E1F6F47CAED
SHA-512:	44F1EE3BA061D79D14F26B809E79494945FB363C7E13987FF2B213D70DF545BA82F0C0C759521A79E9D5015A871AAD96A232E9E7A40932FFD907EE70D27741D0

Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....A..8.....E. .....I.$.. .....scop

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:	dropped
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
Preview:	..p.r.a.t.e.s.h.....

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Unicode text, UTF-16, little-endian 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.Exploit.CVE-2017-11882.123.29721.1282.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.406518452430825
Encrypted:	false
SSDEEP:	3:Rl/Zd15xd7ltl/tNLo/XolFH58lKzuKV:RtZ3v51LfV+2v
MD5:	EA97B7E1EDDA70476AD6C0001C4620AD
SHA1:	E5F90B01FE660C591C4384F345139295FC4300FB
SHA-256:	B80A405D74E591376F8C11E0F6E819A410E55090176BEE9723978E1F6F47CAED
SHA-512:	44F1EE3BA061D79D14F26B809E79494945FB363C7E13987FF2B213D70DF545BA82F0C0C759521A79E9D5015A871AAD96A232E9E7A40932FFD907EE70D27741D0
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....A..8.....E. .....I.$.. .....scop

Static File Info

General

File type:	Composite Document File V2 Document, Cannot read section info
Entropy (8bit):	6.01945829773662
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc

File size:	910336
MD5:	d38967e524822d04257534078b0dc209
SHA1:	b2af456f879fba7dffa694d9386f501883118822
SHA256:	5e458e56f23f18feb1e44f3eb3c15ab7d4d6cd9e937c72528dfce9d5e195ea3c
SHA512:	e6124b681ec75a45400eb822ea2f558b7b2d3cdfe6b3afccf4d03fe15e4934ad39ab8ef77dee74ed4a20a506d3605dd606d5d91700013d8fd5419a51f1f98a5f
SSDEEP:	24576:5LMu/lUHGguNaUgjg+NkTgThiNkKBnv/E:51Kmg6RsOE
TLSH:	A2152340EE581F93C75A46396A1BC63C67D3BF5D831FC0F72BE2358A2A78B710886546
File Content Preview:	.....>.....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.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: \x1oLe10NatIVE, File Type: data, Stream Size: 900632

General

Stream Path:	\x1oLe10NatIVE
File Type:	data
Stream Size:	900632
Entropy:	5.969638510456594
Base64 Encoded:	True
Data ASCII:	I x . . T . . y . . V K M .) q = y # . x ; U . (- (7 C . * . 8 9 ~ . . : 3] . . e Q } . > w v ' H [= Z a . . j A . n . & \\ @ . p N . | s . 2 f 6 k) - V 1 8 " - # ~ F ' E b A 0 . D C * J _ M (^ I 9 b (P } T .) * _ * (~ J c . @ , . 3 r 9 . . } N . c y x . z y 7 = e . . . x Q O / E [. A . w u z + ! . 8 . . O _ e B . o . . # 7 . . . . . W > . . . e . . , . . . _ k . F . . . S W Q Y W _ R . V . . . . . V b Q & . . . . . Z W _ _ S b ` . . o . . $ D . . [[b . . . . S . . . . w . . [R S E . . :
Data Raw:	6c 78 f6 04 02 54 f2 f4 ab a0 01 08 99 79 bd 1a 14 91 94 81 ed b9 56 4b 94 8b 4d db 8b 29 bb d3 71 3d 79 81 eb 23 0a f7 78 8b 3b 55 ff d7 05 b0 f5 8a 28 2d 86 f4 8a 28 ff e0 fa 37 43 00 2a 1e 38 39 91 7e 9f cc 96 9d c2 0a 3a e6 f4 ec 33 5d d4 8b 0b 65 51 9d 8b 7d 14 3e ed 77 76 27 48 5b 3d 5a e2 61 16 02 ca 6a 9b ca 41 f0 ff 9a 06 f2 6e 09 fc 26 5c 40 bc 1b 70 4e fb 16 7c 88 ed b5

Stream Path: 5hLfxSDpMqWpnSELaMw6nQvvNrLo, File Type: empty, Stream Size: 0

General

Stream Path:	5hLfxSDpMqWpnSELaMw6nQvvNrLo
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 5020, Parent PID: 796

General	
Target ID:	0
Start time:	20:00:49
Start date:	24/11/2022
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:	0xd00000
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\tst29A6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	663D2F42	unknown
C:\Users\user\AppData\Local\Temp\tst29E5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	663D2F42	unknown
C:\Users\user\AppData\Local\Temp\tst2A15.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	663D2F42	unknown
C:\Users\user\AppData\Local\Temp\tst2A16.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	663D2F42	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	6624977C	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tst29A6.tmp	success or wait	1	663D2F42	unknown
C:\Users\user\AppData\Local\Temp\tst29E5.tmp	success or wait	1	663D2F42	unknown
C:\Users\user\AppData\Local\Temp\tst2A15.tmp	success or wait	1	663D2F42	unknown
C:\Users\user\AppData\Local\Temp\tst2A16.tmp	success or wait	1	663D2F42	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	1790976	29696	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	66175805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc	unknown	14	success or wait	2	663D2FF3	unknown
C:\Users\user\Desktop\SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc	unknown	4	success or wait	16	663D253D	unknown

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
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	66175805	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	66175805	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	66175805	unknown

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

Disassembly

No disassembly