ID: 756308
Sample Name: SecuriteInfo.com.Exploit.CVE-2018-0798.4.1674.19041.rtf
Cookbook: default.jbs
Time: 00:32:08
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

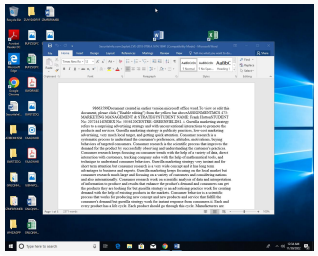
Windows Analysis Report

SecuriteInfo.com.Exploit.CVE-2018-0798.4.1674.19041.rtf

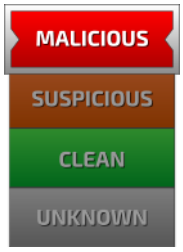
Overview

General Information

Sample Name:	SecuriteInfo.com.Exploit.CVE-2018-0798.4.1674.19041.rtf
Analysis ID:	756308
MD5:	651c9a6ce61867..
SHA1:	cd74ad99acc4c1..
SHA256:	de9a977c672758..
Tags:	rtf
Infos:	YARA



Detection

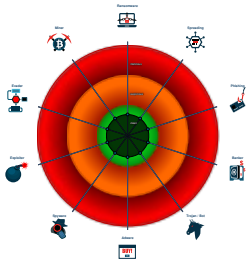


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through…
- Office document tries to convince v…
- Multi AV Scanner detection for subm…
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 1916 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-2018-0798.4.1674.19041.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	• 0x4723:$obj2: \objdata • 0x48f8:$obj3: \objupdate • 0x46fd:$obj5: \objautlink

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.CVE-2018-0798.4.1674.19041.rtf	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x4723:$obj2: \objdata • 0x48f8:$obj3: \objupdate • 0x46fd:$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

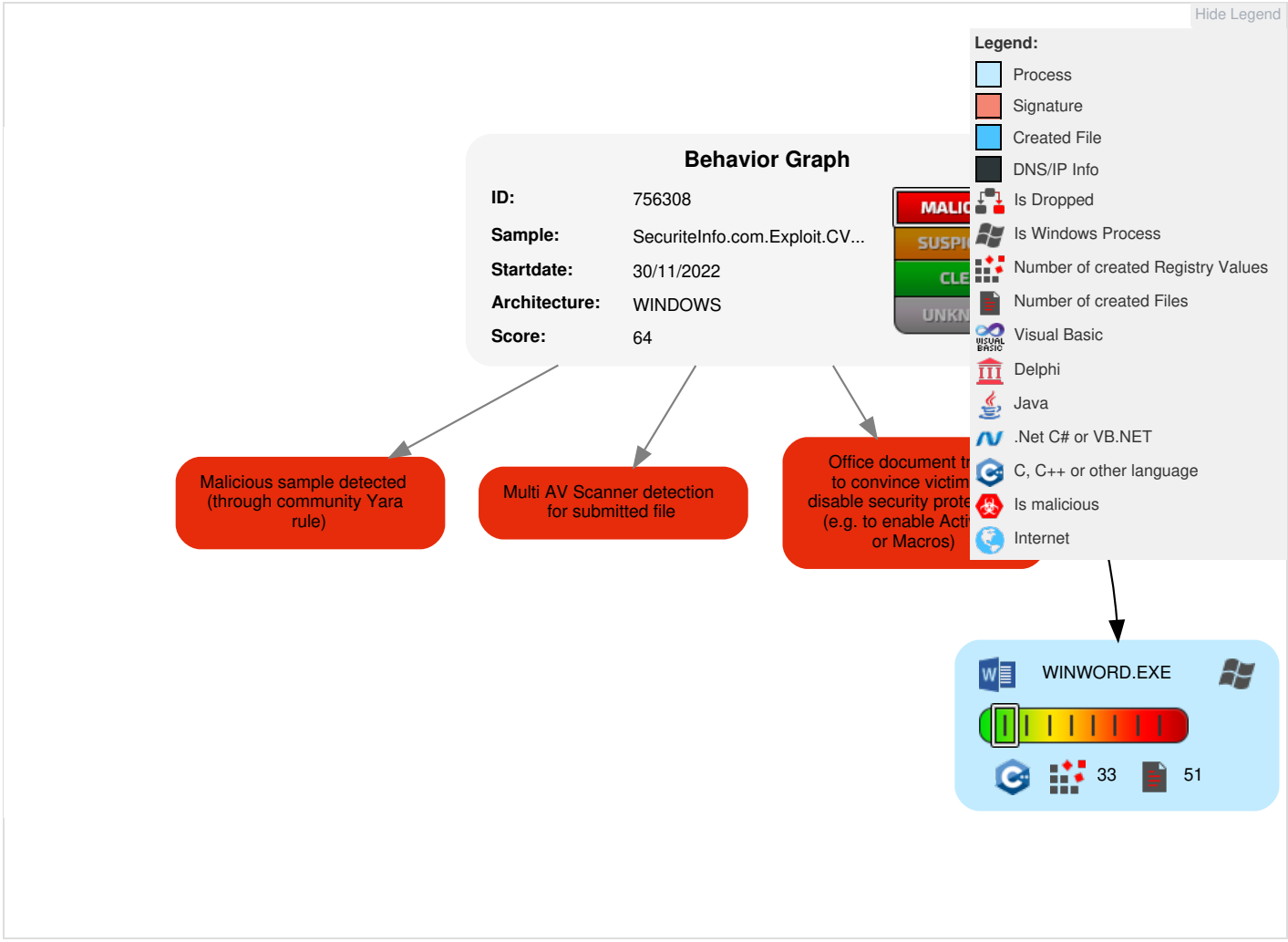
Malicious sample detected (through community Yara rule)

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

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	1 Disable or Modify Tools	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

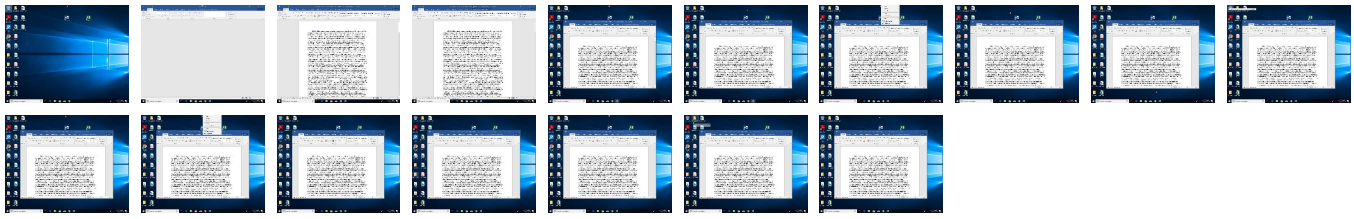
Behavior Graph

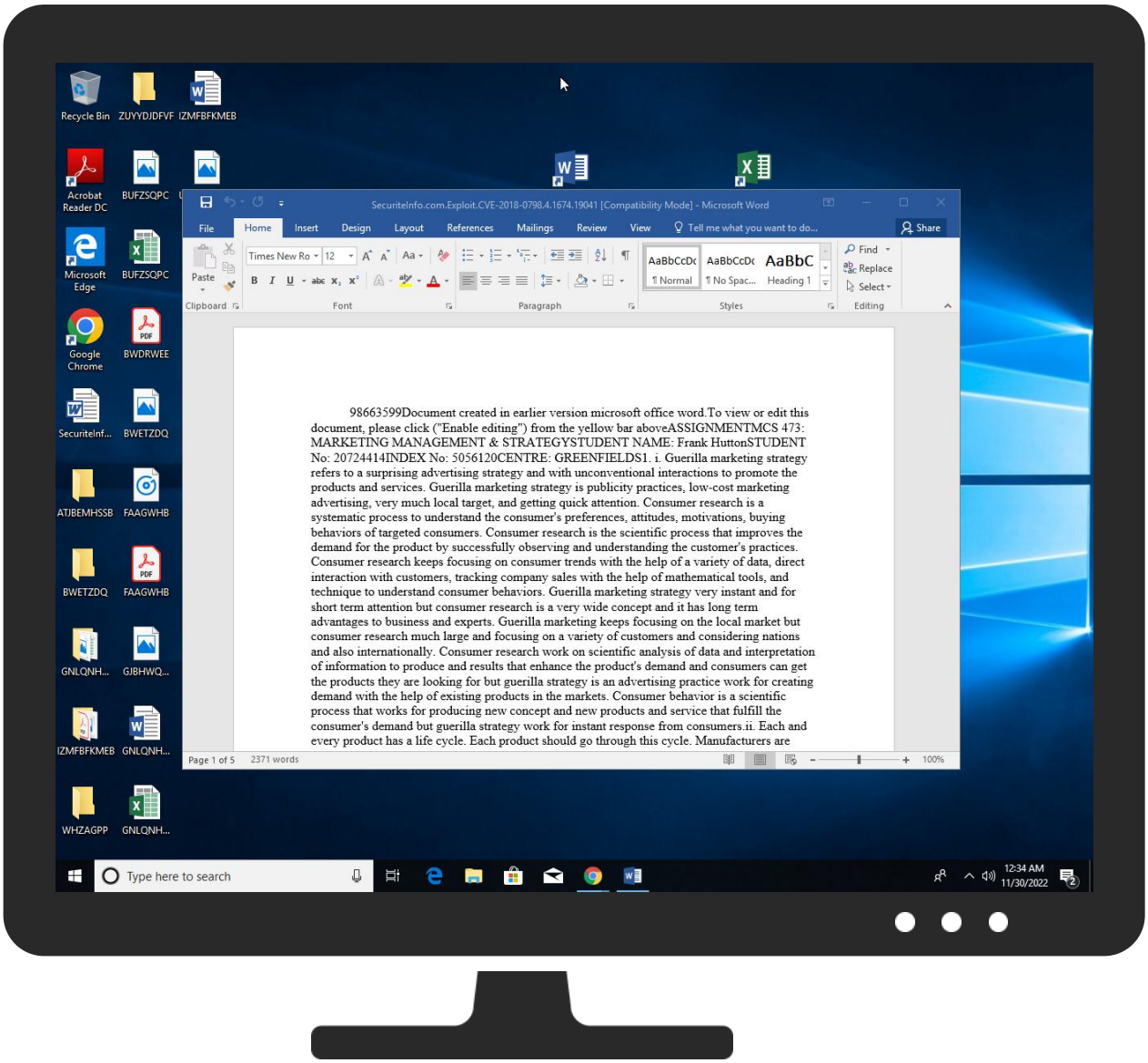


Screenshots

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-2018-0798.4.1674.19041.rtf	27%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	
SecuriteInfo.com.Exploit.CVE-2018-0798.4.1674.19041.rtf	26%	Virustotal		Browse

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	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	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://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	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://login.microsoftonline.com/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://shell.suite.office.com:1443	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://autodiscover-s.outlook.com/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://cdn.entity.	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://powerlift.acompli.net	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lookup.onenote.com/lookup/geolocation/v1	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://cortana.ai	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://api.aadrm.com/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://api.microsoftstream.com/api/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://cr.office.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://graph.ppe.windows.net	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://api.scheduler.	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://my.microsoftpersonalcontent.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://messaging.engagement.office.com/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://web.microsoftstream.com/video/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://dataservice.o365filtering.com/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://consent.config.office.com/consentcheckin/v1.0/consents	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://ncus.contentsync.	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://weather.service.msn.com/data.aspx	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://apis.live.net/v5.0/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://messaging.lifecycle.office.com/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://management.azure.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://outlook.office365.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://wus2.contentsync.	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://api.office.net	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://entitlement.diagnostics.office.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://outlook.office.com/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://outlook.office365.com/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://webshell.suite.office.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://management.azure.com/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://devnull.onenote.com	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://messaging.action.office.com/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://ncus.pagecontentsync.	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.0.dr	false		high
http://https://messaging.office.com/	1BC0D30C-906E-41DA-A53D-99EC4AE5726E.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:	756308
Start date and time:	2022-11-30 00:32:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.CVE-2018-0798.4.1674.19041.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:	10
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.winRTF@1/17@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, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.109.32.24, 20.25.84.51, 20.231.70.194
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, config.officeapps.live.com, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, nexus.officeapps.live.com, officeclient.microsoft.com, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\1BC0D30C-906E-41DA-A53D-99EC4AE5726E

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):	5.359451082546697
Encrypted:	false
SSDEEP:	1536:4L+C7/gUMB5BQguw/BQ9DQe+zQVk4F77nXmvid3XRcE6Lcz6S:Z5Q9DQe+zCXzJ
MD5:	B9DD3013D6D5AFB790AD26F5FCE92455
SHA1:	5D45643C7D2DDEBD211F8EB39D2A0DC1825F9211
SHA-256:	6D3BE75BDD3C55FBB3CD9B459377642639EC047CF3F480ED792BB6A9E01EBF75
SHA-512:	BFB5AEFB322E5200DB4896559736E3D1924DB7F4EA1D21FCF5FD7535DBFD59BA9696F20DD0BA3B4D187000999C3FBB5BD6748F4A374D27E5074F42729CFAA62
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="2022-11-29T23:33:04">.. 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\Bibliography\Style\APASixthEditionOfficeOnline.xsl

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):	333602

Entropy (8bit):	4.65455658727993
Encrypted:	false
SSDEEP:	6144:ybW83ob181+MKHZR5D7H3hgtfL/8mIDbEhPv9FHSVsioWUyGYmwxAw+GIfnUNv5J:Z
MD5:	58AAFDDC9C9FC6A422C6B29E8C4FCCA3
SHA1:	1A83A0297FE83D91950B71114F06CE42F4978316
SHA-256:	9095FE60C9F5A135DFC22B23082574FBF2F223BD3551E75456F57787ABC5797B
SHA-512:	1EBB116BAE9FE02CA942366C8E55D479743ABB549965F4F4302E27A21B28CDF8B75C8730508F045BA4954A5AA0B7EB593EE88226DE3C94BF4E821DBE4513118A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.. <xsl:output method="html" encoding="us-ascii"/>.... <xsl:template match="*" mode="outputHtml2">.. <xsl:apply-templates mode="outputHtml"/>.. </xsl:template>.... <xsl:template name="StringFormatDot">.. <xsl:param name="format" />.. <xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.. <xsl:when test="$format = ""></xsl:when>.. <xsl:when test="substring($format, 1, 2) = '%%'">.. <xsl:text>%</xsl:text>.. <xsl:call-template name="StringFormatDot">.. <xsl:with-param name="format" select="substring($format, 3)" />.. <xsl:with-param name=

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\CHICAGO.XSL

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	297017
Entropy (8bit):	5.000343845106573
Encrypted:	false
SSDEEP:	6144:GwprAtk0qvtfL/vF/bkWPz9yv7EOMBPitjASjTQQr7IwR0TnyDkJb78plJwf33iV:I
MD5:	0D0E65173F5AE6FE524DA09EEDDDCC84
SHA1:	C868617C86C1287B35875AE8D943457756B0B338
SHA-256:	787D1CBF076902B2568E8CFF1245E5FBEBA6AAD84240A54C4F9957084B93F90D
SHA-512:	E2FD5156BA707F6205B5CC52CC4FF8E1CDECB10B6C04E70EC4B3D3D0FA636AB9FDAE77F249D9D303D35CCCA8F8B399B60C602629B8803F708CFDAE8A112203D
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$p

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GB.XSL

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):	268670
Entropy (8bit):	5.054376958189988
Encrypted:	false
SSDEEP:	6144:JwprAJiR95vtfb8p4bgWPzDCvCmvQursq7vImej/yQzSS1apSiQhHDOruvoVeMUh:N4
MD5:	B17C7119B252FD46A675143F80499AA4
SHA1:	4445782BEC229727EE6F384EC29E0CBA82C25D22
SHA-256:	8535282A6E53FA4F307375BCEE99DD073A4E2E04FAF8841E51E1AA0EE351A670
SHA-512:	F9FB76A662DC6AB8DE22B87E817B4BAAC1AEEE08BA4F5090E6BC3060F42BC7CD15A71EB5B117554AEB395B22E5C2EEA7D0EFC36FF13BEC13B156879B87641505
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostName.XSL

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):	256358
Entropy (8bit):	5.104453150382283
Encrypted:	false
SSDEEP:	6144:gwprAB795vtfb8p4bgWPWEtTmtcRCDPThNPFQwB+26RxlsIBkAgRMBHcTCwsHe5a:BW
MD5:	4C7ECD0ED5ADCC30352E2C06931D290A
SHA1:	0E6A8E0EDDB5E67E26CF15692D1E8591F3D3D1DE
SHA-256:	40BACD32DB58799FA95B4707588ADEA1C9065CD804712B69B55DDD332C037D4E
SHA-512:	2C25363DCCDB718D427CE451963F1616344A59A57AF0A19F946B7C06536E773E0EA383AC48AAC35E109327B7B86432D608CB0490EBF9590A31AA87330D6F929E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select=

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostTitle.XSL

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):	251449
Entropy (8bit):	5.103599476769172
Encrypted:	false
SSDEEP:	6144:hwprA3R95vtfb8p4bgWPwW6/m26AnV9IBgIkqm6HITUZJcjUZS1XkaNPQTlvB2zr:XA
MD5:	234430F3D3032B9648671D3DF168D827
SHA1:	4B7606E1F7E8172EE74DE90EE4CA75E3F44A0A2B
SHA-256:	DC7160C2FE5939E82BFEEE180C1DA8176C4914C034CAE8938ED6C9F7A9144F3E
SHA-512:	943119B65B2017F8FAAD5EC6B490CC8E263EC6128DD3D274A54EFB826FBE4353C72D335F5708974F1624E9BAE971C9D112905638B3F2123FC384DB201DE5B26
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\HarvardAnglia2008OfficeOnline.xsl

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	284802
Entropy (8bit):	5.006325058456308
Encrypted:	false
SSDEEP:	6144:B9G5o7Fv0ZcxrStAtXWty8zRLYBQd8itHiYYPVJHMSo27hlwNR57johqBXlwNR2b:G
MD5:	08AD981C6D9BFD066BF29A77A62F0FEA
SHA1:	DBE60C2A2BC9A80EFBD6BE114BDF1416261C94E6
SHA-256:	BCFB2EF3D37F7DAFCB9FF4D92885C5F87B4BEC7A3045BC7208460DAE7DABAE31
SHA-512:	64A939705679AA9EBD66634059A63BE280DF197845F23334906EF419C891E1393700344EE8D200195B72509874AD6046495815B94C1BF998116C351BC483C6EB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".....xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.....<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="/">....<xsl:call-template name="Start"/>...</xsl:template>.....<xsl:template name="Start">....<xsl:choose>.....<xsl:when test="b:Version">.....<xsl:text>2010.2.02</xsl:text>.....</xsl:when>.....<xsl:when test="b:XslVersion">.....<xsl:text>2008</xsl:text>.....</xsl:when>.... <xsl:when test="b:StyleNameLocalized">.. <xsl:choose>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1033'">.. <xsl:text>Harvard - Anglia</xsl:text>.. </xsl:when>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1025'">.. <xsl:text>Harvard - Anglia</xsl:text>.. </xsl:when>.. <x

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\IEEE2006OfficeOnline.xsl

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, Unicode text, UTF-8 text, with CRLF line terminators

Category:	dropped
Size (bytes):	294525
Entropy (8bit):	4.978414555953716
Encrypted:	false
SSDEEP:	6144:ndkJ3yU0orh0SCLVXyMFsoiOjWIm4vW2uo4hfhf7v3uH4NYYP4BpBaZTTSSamEUD:Y
MD5:	96F3CCC20E23824F1904EDFDFE5CDA02
SHA1:	EF78E9B415A9FFD4094E525509D3AEB3E2A68EEE
SHA-256:	9970654851826C920261D52F8536B1305F7E582C7A2E892BAC344A95F909FE63
SHA-512:	1022D3E990B1A31361C9658C6C15DB9B41DA38E73319C93C62EE8E57E36333261F66897E1F0F6502EC28B780A9FC434E7F548178F3BC1D4463A44BCF508604E1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".....xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.....<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="/">....<xsl:call-template name="Start"/>...</xsl:template>.....<xsl:template name="Start">....<xsl:choose>.....<xsl:when test="b:Version">.....<xsl:text>2010.2.02</xsl:text>.....</xsl:when>.....<xsl:when test="b:XslVersion">.....<xsl:text>2006</xsl:text>.....</xsl:when>.. <xsl:when test="b:StyleNameLocalized">.. <xsl:choose>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1033'">.. <xsl:text>IEEE</xsl:text>.. </xsl:when>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1025'">.. <xsl:text>IEEE</xsl:text>.. </xsl:when>.. <xsl:when test="b:StyleNameL

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690.XSL

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):	270642
Entropy (8bit):	5.074829646335759
Encrypted:	false
SSDEEP:	6144:JwprAi5R95vtfb8pDbgWPzDCvCmvQursq7vImej/yQ4SS1apSiQhHDOruvoVeMUX:WL
MD5:	831E5489F3047AFF2EFDFF758FA42FEC
SHA1:	F27C9E96D726464E802AD007FE749B8F27FF4525
SHA-256:	7914A8B4ADFDC9A6589ED181DE46D3D735676A38AA61B8FAFC0F862B9EC3A1CD
SHA-512:	B84800FAB9FDF2AEFACBFC14527BC8361459E5138309E11C1025CF61A855C481E77EF14623182F485F3122A40BA4F873E4300B8D8209D924E3E16646FA34BCB8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690Nmerical.XSL

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):	217578
Entropy (8bit):	5.069961862348856
Encrypted:	false
SSDEEP:	6144:AwprA3Z95vtf58pb1WP2DCvCmvQursq7vIme5QyQzSS1apSiQhHDlruvoVeMUwFj:4P
MD5:	7777C0173259D8F4A4F5E69C1461CA14
SHA1:	9C83B87C098AECF3CDFC1B5C4C78B696BF14A5E6
SHA-256:	A343D61BAB2F25D138BDCC57D33C4A83FD494A54EAF3DF0F539E3B51CFE011F1
SHA-512:	77BFD6F7D21AB9771DF1993FB9AB82BA6D5E900F0B846F0F11578313E8A99C99E095612510CBB07590367EADE9B31CF396B26ABA5E8380F3ABC0886FA02858B9
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>..... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$parame

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\MLASeventhEditionOfficeOnline.xsl

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):	255219
Entropy (8bit):	5.004117790808506
Encrypted:	false
SSDEEP:	6144:MwprA8niNgtfbzbOWPuv7kOMBLitjAUjTQLrYHwR0TnyDkHqV3iPr1zHX5T6SSXj:x
MD5:	C9460BEAF863E337428518DAF5C09C5C
SHA1:	76BE7E80D117A73A4FFC96682345EECE9A5C4D2A
SHA-256:	A69368BE9AC843B088D739F1573007E634D1068DB0AD9937A95FE7A0690C05E0
SHA-512:	9E4A7D3E019D182CD6CFF4947364DCF435EF3B40BA004A360260EDA0712839875CB797DBFCCCD9E50885EB10AEF8695052899E4BAC16423D0EECCF025CF6B(3F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>...</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.....<xsl:variable name="prop_EndChars">.....<xsl:call-template name="templ_prop_EndChars"/>....</xsl:variable>.....<xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$parameters" />.....

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\SIST02.XSL

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):	251336
Entropy (8bit):	5.057713103491112
Encrypted:	false
SSDEEP:	6144:JwprA6sS95vtfb8p4bgWPzkhUh9I5/oBRSifJeg/yQzvapSiQhHZeruvoXMUw3im:u9
MD5:	DAE31FA14BC97723A87F126B5121BAE3
SHA1:	C6B5CFF442FCC8795A5AF0D69ACDA24497D9F4BE
SHA-256:	30F377F7AC24B022F52371ADA97CB057460265F4C8BDDBB521642B6E2462EE27
SHA-512:	AE6B8BB6FCF956E1973C9E40702CB1A86FD8AD6F87FA1C2D3A2113C2F8AEC2A495FE636D71786843496F37FF9DB3D2F0E034BC4014D9C379E4EA4CC9495BE907
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\TURABIAN.XSL

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):	344662
Entropy (8bit):	5.023256859004611
Encrypted:	false
SSDEEP:	6144:UwprAwnsqvtfL/vF/bkWPRMMv7EOMBPitjASjTQQr7IwR0TnyDk1b78plJwf33iD:F
MD5:	F82561FF802442D12B8B77EC6EDC027E
SHA1:	EE7ED23C6EF8DA4968BA969FC094203D61065C0E
SHA-256:	5B7A52DFAA9C3E9E340E081178B54E827ED591AC27DC098C3985C94BDE5CABE9
SHA-512:	FA205BCD1D61226A940EA333B3B3EC43FB461E7683669A344403B543B9F699677A9E332827EC0160E81A8FBFD43CA61735A5C414EE7C17143DC9819A137044B5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$pa

C:\Users\user\AppData\Roaming\Microsoft\Office\MSO1033.acl

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped

Size (bytes):	37730
Entropy (8bit):	3.1248667435282056
Encrypted:	false
SSDEEP:	768:+atNbFeZKdogeyHMOeYhIVi+iOFOqbPXdEmanb:5/eLAhIVJb2
MD5:	C8120F676FB4E7D77C22AD6A4A535212
SHA1:	7D281EAC08585C508A9FC6DA1A44E80CAB13D827
SHA-256:	0C7550F705FD9E087E3409946E17F2C81CBA39DAE4EE186194012C8D2963616F
SHA-512:	D65CB047C407A6B09F34163FFD7AF531D3EA632AE2A438AB3D336DB77C17804E42C2F7E5786E761553BE98D038FB6675F0FC2033D01523B25AD3F83E422A5E5
Malicious:	false
Preview:	.....b.....R.....(.c.).....(.e.)..... ....(.r.).....(.t.m.)....."!.....& ....a.b.b.o.u.t.....a.b.o.u.t.....a.b.o.t.u.....a.b.o.u.t.....a.b.o.u.t.a.....a.b.o.u.t. .a.....a.b.o.u.t.i.t.....a.b.o.u.t. .i.t.....a.b.o.u.t.t.h.e.....a.b.o.u.t. .t.h.e.....a.b.s.c.e.n.c.e.....a.b.s.e.n.c.e.....a.c.c.e.s.s.o.r.i.e.s.....a.c.c.e.s.s.o.r.i.e.s.....a.c.c.i.d.e.n.t.....a.c.c.i.d.e.n.t.....a.c.c.o.m.o.d.a.t.e.....a.c .c.o.m.m.o.d.a.t.e.....a.c.c.o.r.d.i.n.g.t.o.....a.c.c.o.r.d.i.n.g. .t.o.....a.c.c.r.o.s.s.....a.c.r.o.s.s.....a.c.h.e.i.v.e.....a.c.h.i.e.v.e.....a.c.h.e.i.v.e.d.....a.c.h.i.e.v.e.d.....a.c.h.e.i.v.i .n.g.....a.c.h.i.e.v.i.n.g.....a.c.n.....c.a.n.....a.c.o.m.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.o.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.t.u.a.l.y.l.....a.c.t.u.a.l.l.y.....a.d.d.i.t.i .n.a.l.....a.d.d.i.t.i.o.n.a.l.....a.d.d.t.i.o.n.a.l.....a.d.d.i.t.i.o.n.a.l.....a.d.e.q.u.i.t.....a.d.e.q.u.a.t.e.....a.d.e.q.u.i.t.e.....a.d.e.q.u.a.t.e.....a.d.n.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.CVE-2018-0798.4.1674.19041.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 21:54:42 2022, mtime=Wed Nov 30 07:33:06 2022, atime=Wed Nov 30 07:33:01 2022, length=23332, window=hide
Category:	dropped
Size (bytes):	1273
Entropy (8bit):	4.682406902235589
Encrypted:	false
SSDEEP:	24:8iggMizysCdNrAq8JhJwHCdNRDc6n7aB6m:8ZgM4CUqiJwHCm6WB6
MD5:	EB4FEF0BCDD2E6F18DFB74B7703BA9A3
SHA1:	999B25D5AC1B3509145C71A4743C70BDEC6FD12C
SHA-256:	D238489D44E14194E6D3519CF31FD7880A44DFD845928F5CEFE6D5438685ECCF
SHA-512:	7B2090015AEF0E42FED13994A818A88E5FFB571398E1AAC4FBB3F493EE8C578FE3C385F79FD9FD6AF1E09FBE89931DA3B7263E91FF1627430693AB703DE20D0D
Malicious:	false
Preview:	L.....F.... ....,.... .^.....B.[....$[.....;....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..~U.D.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....Z.1.....U...user..B.....N..~U.D.....S.....k..e.n.g.i.n.e.e.r.....~.1.....U...Desktop.h.....N..~U.D.....Y.....>.....f...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.$[..~U!D .SECURI~1.RTF.....U.~U!D.....%0..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...1.6.7.4...1.9.0.4.1...r.t.f. .....-.....>.S.....C:\Users\user\Desktop\SecuriteInfo.com.Exploit.CVE-2018-0798.4.1674.19041.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...1.6.7.4...1.9.0.4.1...r.t.f.....:.,.LB.)...A}...`.....X.....632922.....!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 [folders]
Category:	modified
Size (bytes):	143
Entropy (8bit):	5.035238645842531
Encrypted:	false
SSDEEP:	3:HIMov8bcK+KUer7xm4P8bcK+KUer7xv:H48wKhJnuwKhJnp
MD5:	C89814C6ADEBB9C96D7BEBE2C9043FB3
SHA1:	F5CBFDB429FD98961988877FD25652874ACF8A68
SHA-256:	D7AB5BCAD94D73406D3D2B6119460D6AC47101F666F22BF2982171D6251E7286
SHA-512:	D3E366E54D6E79F51E0F3A08C3CFE55E7E95F30B53F08253DC0EF534DA1348F8931FA7523CAD292735A738A10B4905E0C3331740EEFD5935E4CD9906EF48B7B
Malicious:	false
Preview:	[misc??????]..SecuriteInfo.com.Exploit.CVE-2018-0798.4.1674.19041.LNK=0..[folders]..SecuriteInfo.com.Exploit.CVE-2018-0798.4.1674.19041.LNK=0..

C:\Users\user\Desktop\~$curiteInfo.com.Exploit.CVE-2018-0798.4.1674.19041.rtf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.2284796143773873
Encrypted:	false
SSDEEP:	3:Rl/Zd3RlRxH/qlA5nRlGpiTdxldplXzBBbluxl:RtZZRlylkRlrTdxlrJ4j
MD5:	2C4DFC4C1FDCDB48EDA54752C3692FAF
SHA1:	3CEFF23CBAB2BC319424D7E1E47AC72643DD9CDF
SHA-256:	9245382A4F6DB21FDFFE2A91F800124BB3DDB45540A14332FDC675CB6E09180B

SHA-512:	3C250027622AEDAF868F82749FEC2FEE6C2BE9390A0134223DDD4518395887CCF260C017B8F2C93866A8ACDD61A658D956D22C4EAE24A77115F94641E6217AD
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....@.....".`...`^.....__len.....L.....d1~.d1~.APT.....H.....$~..$~.APT.

Static File Info

General

File type:	Rich Text Format data, version 1
Entropy (8bit):	5.348335644827323
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-2018-0798.4.1674.19041.rtf
File size:	23332
MD5:	651c9a6ce618676610f649779edc714b
SHA1:	cd74ad99acc4c1caf5e8379367b9df24f07746db
SHA256:	de9a977c672758a706c96568e202c075590bb60a848fb3b7680c2f83df7f203e
SHA512:	1cd373c30ebb11bed6a829cbd456b379e76ebe610ba85be75278e8874814e6f4bbb2cdce90c8dbf3850e2143eac53d77e8b01808f3a5fe30b9cdbe32114699d4
SSDEEP:	384:hQMmdOFNYY0aaaIswqPeOrka1+fHQJ+t3rQkRhZU78denfY5s8ecCOHMW1sCxWJ:vFx0XaIsnPRIa4fwJMGoUnw5ScpTH0
TLSH:	4BA22957FB9803BC439201A47B1F2BD8EB2EB539739054A12C6C923427968B643777EC
File Content Preview:	{\rtf1...{*\pnaiud788526351 \.}.{\498663599Document 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 & STRATEGYSTUDENT NAME: F

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000472Dh								no

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 1916, Parent PID: 800

General

Target ID:	0
Start time:	00:33:02
Start date:	30/11/2022

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:	0x1040000
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	664A977C	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	663E8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	663E8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	663E8A84	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