ID: 715093
Sample Name:
l6C8uDXVRN.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 16:18:56
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

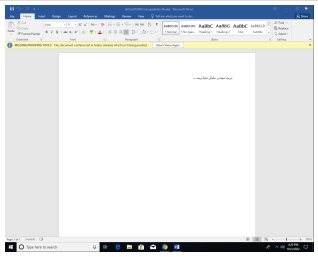
Windows Analysis Report

l6C8uDXVRN.doc

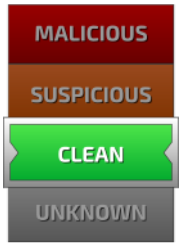
Overview

General Information

Sample Name:	l6C8uDXVRN.doc
Analysis ID:	715093
MD5:	36839293424d99.
SHA1:	67292dea75e5e6.
SHA256:	aea2494a833a1a.
Infos:	



Detection

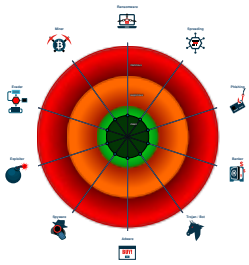


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- WINWORD.EXE (PID: 6124 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

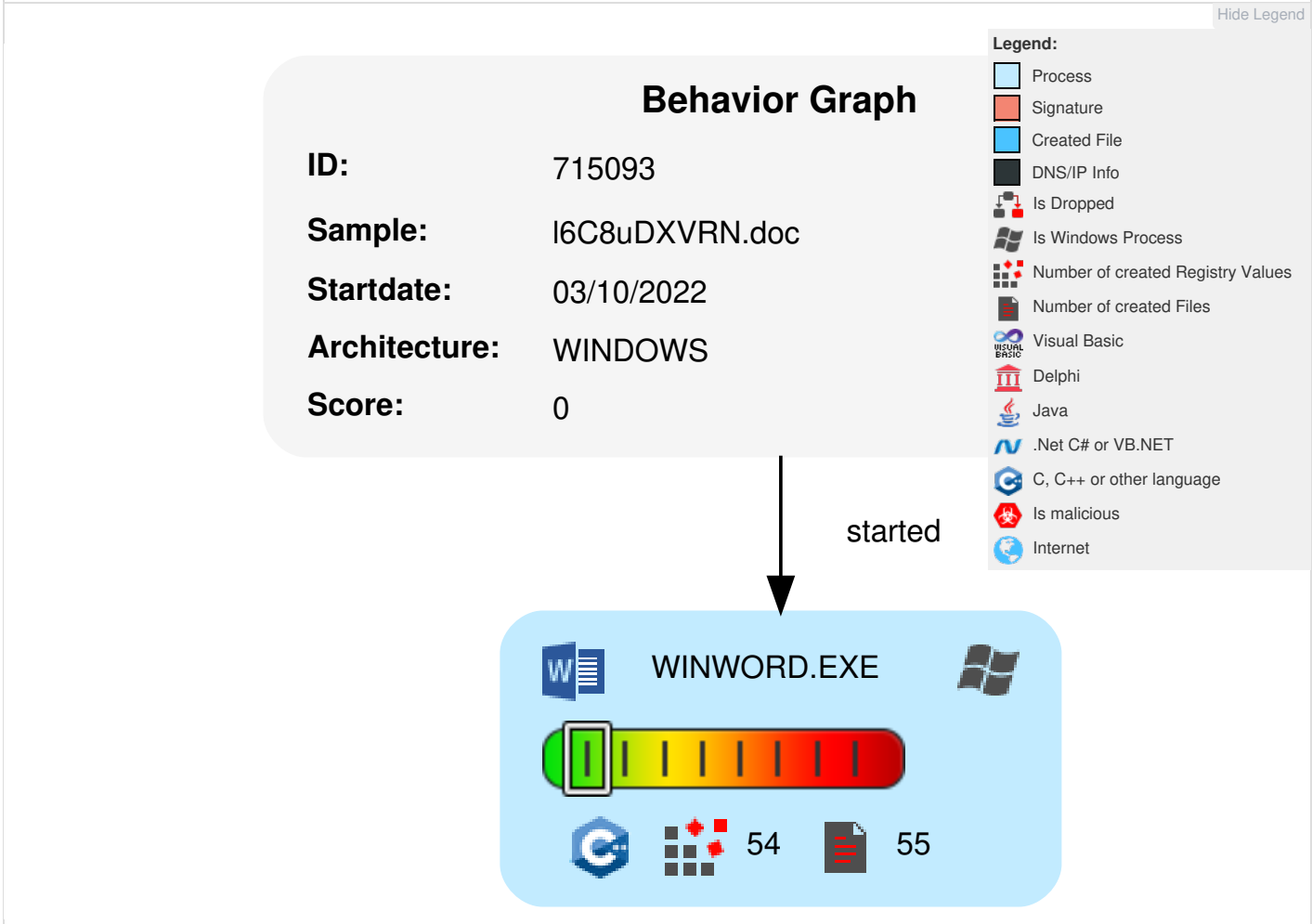
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

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

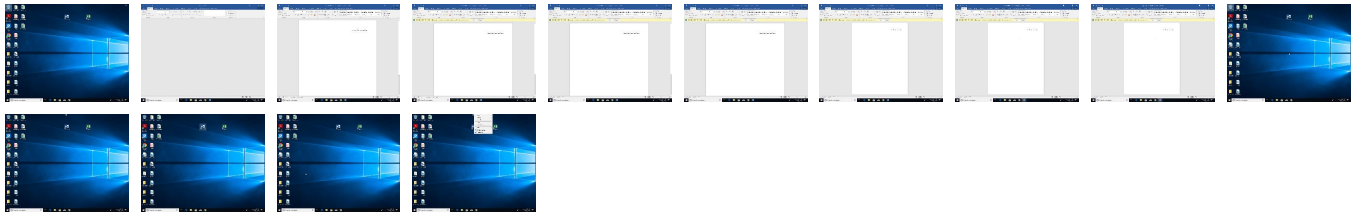
Behavior Graph

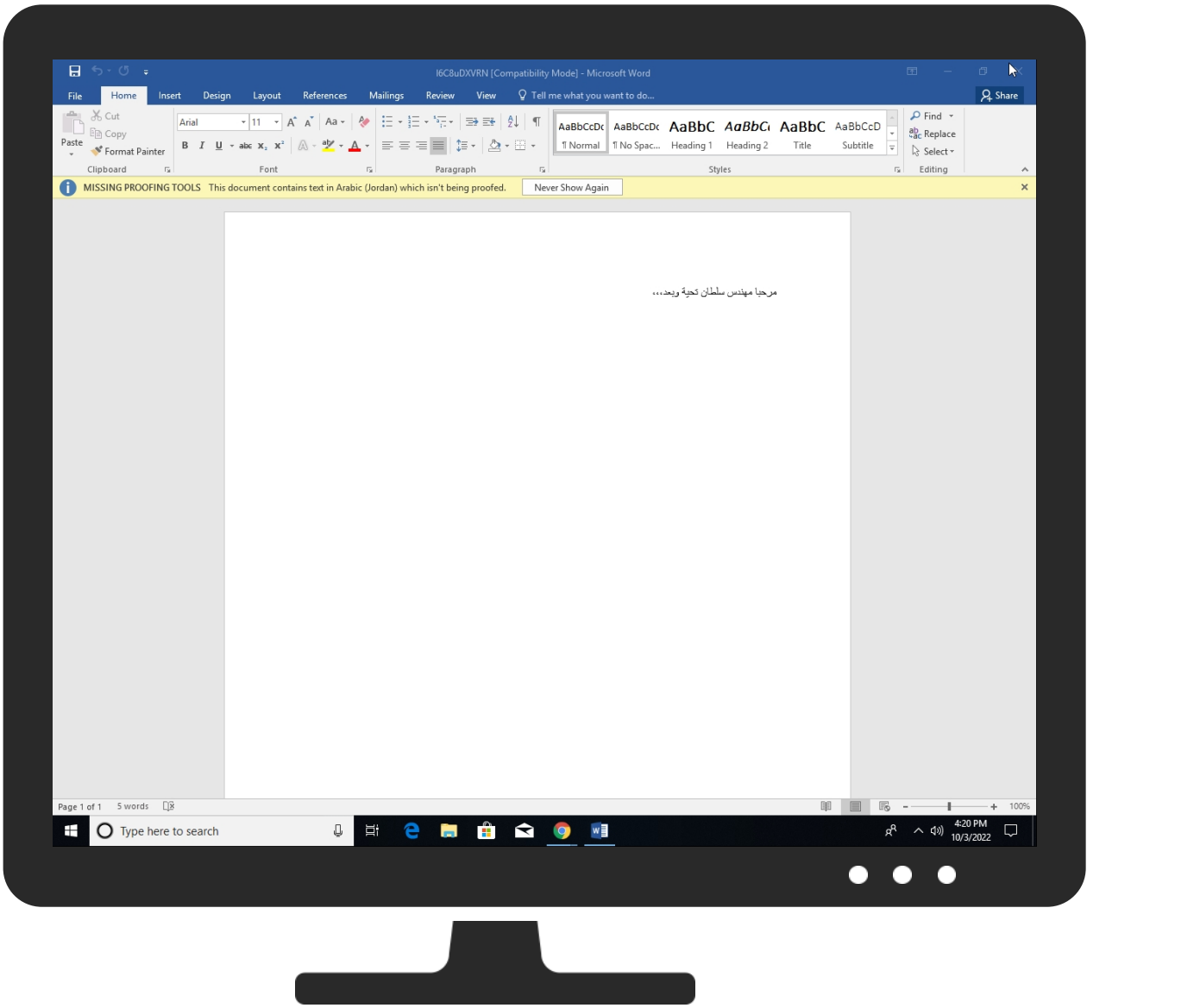


Screenshots

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
I6C8uDXVRN.doc	2%	ReversingLabs		
I6C8uDXVRN.doc	5%	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://roaming.edog.	0%	URL Reputation	safe	
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	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://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	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://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://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	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://login.microsoftonline.com/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://shell.suite.office.com:1443	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://autodiscover-s.outlook.com/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://roaming.edog.	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://cdn.entity.	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://powerlift.acompli.net	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://cortana.ai	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://api.aadrm.com/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://api.microsoftstream.com/api/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://cr.office.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://graph.ppe.windows.net	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://api.scheduler.	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://my.microsoftpersonalcontent.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.aadrm.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://globaldisco.crm.dynamics.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://messaging.engagement.office.com/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://web.microsoftstream.com/video/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://dataservice.o365filtering.com/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://ncus.contentsync.	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://weather.service.msn.com/data.aspx	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://apis.live.net/v5.0/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://messaging.lifecycle.office.com/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://management.azure.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://outlook.office365.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://wus2.contentsync.	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://api.office.net	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://entitlement.diagnostics.office.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://outlook.office.com/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://outlook.office365.com/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://webshell.suite.office.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://management.azure.com/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://devnull.onenote.com	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://messaging.action.office.com/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://ncus.pagecontentsync.	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high
http://https://messaging.office.com/	65637C51-BF51-4763-A2DC-E19CAF4209B1.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715093
Start date and time:	2022-10-03 16:18:56 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	l6C8uDXVRN.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:	12
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:	CLEAN
Classification:	clean0.winDOC@1/22@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 • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.109.76.141, 20.126.106.131, 20.231.71.84
- Excluded domains from analysis (whitelisted): fs.microsoft.com, 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
- Report size getting too big, too many NtQueryAttributesFile 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\65637C51-BF51-4763-A2DC-E19CAF4209B1

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):	148001
Entropy (8bit):	5.358566546592772
Encrypted:	false
SSDEEP:	1536:jcQW/gx5B5BQguw//Q9DQe+zQhk4F77nXmvid3XRWE6Lcz6S:PHQ9DQe+zWXJJ
MD5:	2CB30F376D5A36131039CB0A2AB7FD39
SHA1:	0786831CAE9653048760969321086E190F5E5AE5
SHA-256:	22D9393896BD57957EF27C0C10BCDFA9717584EBB4DD40348F93554F9336598F
SHA-512:	9692876400C84E2091377F0A6072CDA6A3E62B5DA1F9AD644270457DCD3DA23F6A82C31F6BEF5E7248B438A40E92B6D73194A37CBB565BB41D3AD3F83888E41
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="2022-10-03T14:19:57">.. Build: 16.0.15730.30528-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Temp\~DFB6637BAE1EB82BAB.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\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:	E2FD5156BA707F6205B5CC52CC4FF8E1CDECB10B6C04E70EC4B3D3D0FA636AB9FDAE77F249D9D303D35CCCA8F8B399B60C602629B8803F708CFDAE8A1122603D
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($format, 3)" />.....<xsl:with-param name="parameters" select="$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
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:ndkJ3yU0orh0SCLVXyMFsoiOjWlm4vW2uo4hfhf7v3uH4NYYP4BpBaZTTSSamEUD: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:	9E4A7D3E019D182CD6CFF4947364DCF435EF3B40BA004A360260EDA0712839875CB797DBFCCCD9E50885EB10AEF8695052899E4BAC16423D0EECCF025CF6B03F
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:	AE6B8BB6FCF956E1973C9E40702CB1A86FD8AD6F87FA1C2D3A2113C2F8AEC2A495FE636D71786843496F37FF9DB3D2F0E034BC4014D9C379E4EA4CC9495BE9 07
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:xs lt".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="StringFormat Dot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_En dChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</x sl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" sel ect="$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-co m:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encodi ng="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringForm atDot">....<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($format, 3)" />.....<xsl:with-param name="parameters" s elect="$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:jatNbFeZKdogeyHMOeYhIVi+iOFOqbPXdEmanb:S/eLAhIVJb2
MD5:	88448C03D04FE3D905245C7C41F5ADC2
SHA1:	2132AED6679AE86E867ED4934DB65A6BC373EA83
SHA-256:	D926AB6EADFF355329C6AD79DF4E5CDF82E83D71CC823FD0D80A7525942BDF7F
SHA-512:	FDA7C1616B3AFF95DC3C944393766575869737F7BE57C4B4C05E0D1028849EFA3A75641CE08167CA72C472A46F0AF36EF7D72B53A1E392366B620C9AA0F16DC
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.a.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\Templates.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, Directory, ctime=Mon Oct 3 22:19:56 2022, mtime=Mon Oct 3 22:21:01 2022, at ime=Mon Oct 3 22:21:01 2022, length=0, window=hide

Category:	dropped
Size (bytes):	1177
Entropy (8bit):	4.695290020550004
Encrypted:	false
SSDEEP:	12:8DXCyUuWCHoDoBh/ceQsv9YH3/cqSoELw2TDY9qXIxlqjA+/E+HSuT1lilGsbNft:8B0Cc30Vome96A+8buTYa/7aB6m
MD5:	321E7BA6BDCA94D24D9EDB3BD232BCCA
SHA1:	CC6B68D26DE631106D4D7678A01319917C7BDC7F
SHA-256:	990112966E6542EDACC3545BCFC280467E347B32524DACAC2632E59E02789F64
SHA-512:	C2DDC8A3EF4E4DC048A371A69116F6537334E39A4C87851AB986F5274B7AC2E601B6D9BD4533D6C88B5756E4436C0974DDE0328B0B4F23F36B9783CCFFDB24 0
Malicious:	false
Preview:	L.....F.....S.~....q'.~.....%.~.....e....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..CUv.....:.....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..CUv.....S.....V...e.n.g.i.n.e.e.r.....V.1.....N....AppData.@.....N..CUv.....Y.....t..A.p.p.D.a.t.a.....V.1.....N ....Roaming.@.....N..CUv.....Y.....D...R.o.a.m.i.n.g.....\.1.....CU....MICROS~1..D.....N..CU.....Y.....M.i.c.r.o.s.o.f.t.....\.1.....CU....TEMPLA~1.. D.....CU}.CU.....T.....K.T.e.m.p.l.a.t.e.s.....d.....-.....c.....>.S.....C:\Users\user\AppData\Roaming\Microsoft\Templates.....\....\.T.e.m.p.l.a.t.e.s..... .....>.e.L.:..er.=....`.....X.....648351.....!a..%.H.VZAj...%.c2.....-$..!a..%.H.VZAj...%.c2.....-$.....1SPS.XF.L8C....&.m.q....

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:	dropped
Size (bytes):	71
Entropy (8bit):	4.778504211951284
Encrypted:	false
SSDEEP:	3:M1dqa3rpFom41qa3rpFopnbJlv:M33e3iv
MD5:	43362E612B198FA3412C7A2FAF3FE959
SHA1:	99484E3C1ACD1DE64ED2E07E8007518E62ABED3E
SHA-256:	5A490C3B6524D3C69C464A53A9415D4DF9EA49ED3197F929F42A13C8E4E30E2B
SHA-512:	EB6192950A3BB2A3BC65E0032A4E07C86C0B63E3FCA97F4453B9D9A714B8B6169F6E71CE87896B5AA461C37F348D1E4BA0EFA404FA1DBE3209C3085B5786340 E
Malicious:	false
Preview:	[doc]..l6C8uDXVRN.LNK=0..[folders]..l6C8uDXVRN.LNK=0..Templates.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\l6C8uDXVRN.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 21:54:47 2022, mtime=Mon Oct 3 22:19:59 2022, atime=Mon Oct 3 22:19:55 2022, length=22528, window=hide
Category:	dropped
Size (bytes):	1068
Entropy (8bit):	4.6777037948449225
Encrypted:	false
SSDEEP:	12:87tRU0UuWCHoDoBBDhDv7e+WNJv3SXOjAH/E2DAm2S5D8/LQLUk44t2Y+xIBjKZm:8I6hjyAH8UASDu7aB6m
MD5:	293B05AD826E9B0B2C25CF90BF595D25
SHA1:	6CAAECB03B8D397FFAA185DFDB5A8902EF023C42
SHA-256:	004D1BDA11DE45FEB28826DEC2203E59A190E34CA585231512C5A2A232C30DA4
SHA-512:	EC871471C79D20157C76B4F46768FEBFE6A236DB8556E1C4B4A5E89E8038961B10E0F3902C43BA596350D1146355798C164E2233DC4463367CBDA2F2AD3715DE
Malicious:	false
Preview:	L.....F.... .....1/.....V.~...6D..~....X.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..CUv.....:.....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..CUv.....S.....V...e.n.g.i.n.e.e.r.....~.1.....U...Desktop.h.....N..CUv.....Y.....>.....H.6.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,- .2.1.7.6.9.....j.2..X..CU|. .L6C8UD~1.DOC..N.....U.CU|.....l.6.C.8.u.D.X.V.R.N...d.o.c.....W.....-.....V.....>.S.....C:\Users\user\Desktop\ l6C8uDXVRN.doc..%.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.l.6.C.8.u.D.X.V.R.N...d.o.c.....:.,.LB.)...A}...`.....X.....648351.....!a..%.H.VZAj....c2.....-$..!a..%.H.V ZAj....c2.....-$.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\AppData\Roaming\Microsoft\Templates\Normal.dotm (copy)

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	17938
Entropy (8bit):	7.4052962065553265
Encrypted:	false
SSDEEP:	384:Jg+SiC78rS5RLxK4C556akwLWdxd0pfBsMhEh4:cV8WNK4rakw6L0pf9k4
MD5:	B5D9D23E6B4B5BBE7716829698DCD98F

SHA1:	8127C1E08F14AC88882504190300C35788911B11
SHA-256:	EACBB51D2F1ECA32C08E244860A44DC6484E88E3904D9CA54B8FD2D2BA87EAD9
SHA-512:	B3EBE0987BFA910358F808C02F3B7964D2C41C366B89E34DBA91F76E80F69441C13BE9DA21297FB89C0DBFB1F91EEDAFEA1B05FF0B8CB876AE868501FCDB6AC4
Malicious:	false
Preview:	PK.....!.Q3.p.....[Content_Types].xml ...(..... ....N.0.E.H.C.-J\X .....J..0....K.....H...R*.D.g..3.H....M!`.l.....J.j;*...>.b.Fa...B....wz...<`F..K6.._s.r.F`.<X.T....7....U.._t:.\:...<&....A%&:f.9.. H.hd..*1y.Lx.k)".....e..k.g.....)....&.....A...3..WNN.U..e...<....'4(.....x.....nh.t.....p7..j..s...I@.w6.X..C.Tp...r+..^..F.N...".az...h.[!F.!...g...i"...C..n9.~I...3.....H..V..9.2.,)s ..GZD..mo6M..a.!...q$.....O..r-.....PK.....!.....N.....

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):	3.0376871165346113
Encrypted:	false
SSDEEP:	3:Rl/ZdnK2kdKdnSE/NTT22lzlTn:RtZgKH/pT22lzhn
MD5:	1B442339680B6CF793980F10D4AC3418
SHA1:	54D82D4F327E23D4E697E4FC726526B930275855
SHA-256:	31B889EDCB6699DFD5F0E79E2CB450C7B64A330388BBCD60BED7D44AA5D1A1FE
SHA-512:	EA3D692F5A2716B0AEA0983835185780828C41E879CA2252A04F5C77400EB783B240D65D20AFEA2597C56E722683DB6A37DDCDE63F708F12707551F58CAE03F
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h...8.....JOv.....p.r.a.t.e.s.h...8.....JKv.....LMEM....T.....JGv....o.l.e.3.2...

C:\Users\user\AppData\Roaming\Microsoft\Templates\~WRD0000.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	17938
Entropy (8bit):	7.4052962065553265
Encrypted:	false
SSDEEP:	384:Jg+SiC78rS5RLxK4C556akwLWdxd0pfBsMhEh4:cV8WNK4rakw6L0pf9k4
MD5:	B5D9D23E6B4B5BBE7716829698DCD98F
SHA1:	8127C1E08F14AC88882504190300C35788911B11
SHA-256:	EACBB51D2F1ECA32C08E244860A44DC6484E88E3904D9CA54B8FD2D2BA87EAD9
SHA-512:	B3EBE0987BFA910358F808C02F3B7964D2C41C366B89E34DBA91F76E80F69441C13BE9DA21297FB89C0DBFB1F91EEDAFEA1B05FF0B8CB876AE868501FCDB6AC4
Malicious:	false
Preview:	PK.....!.Q3.p.....[Content_Types].xml ...(..... ....N.0.E.H.C.-J\X .....J..0....K.....H...R*.D.g..3.H....M!`.l.....J.j;*...>.b.Fa...B....wz...<`F..K6.._s.r.F`.<X.T....7....U.._t:.\:...<&....A%&:f.9.. H.hd..*1y.Lx.k)".....e..k.g.....)....&.....A...3..WNN.U..e...<....'4(.....x.....nh.t.....p7..j..s...I@.w6.X..C.Tp...r+..^..F.N...".az...h.[!F.!...g...i"...C..n9.~I...3.....H..V..9.2.,)s ..GZD..mo6M..a.!...q$.....O..r-.....PK.....!.....N.....

C:\Users\user\Desktop\~$C8uDXVRN.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.0376871165346113
Encrypted:	false
SSDEEP:	3:Rl/ZdnK2kdKdnSE/NTT22lzlTn:RtZgKH/pT22lzhn
MD5:	1B442339680B6CF793980F10D4AC3418
SHA1:	54D82D4F327E23D4E697E4FC726526B930275855
SHA-256:	31B889EDCB6699DFD5F0E79E2CB450C7B64A330388BBCD60BED7D44AA5D1A1FE
SHA-512:	EA3D692F5A2716B0AEA0983835185780828C41E879CA2252A04F5C77400EB783B240D65D20AFEA2597C56E722683DB6A37DDCDE63F708F12707551F58CAE03F
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h...8.....JOv.....p.r.a.t.e.s.h...8.....JKv.....LMEM....T.....JGv....o.l.e.3.2...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Author: ayman alkhateeb, Template: Normal.dotm, Last Saved By: ayman alkhateeb, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Sun Oct 2 11:52:00 2022, Last Saved Time/Date: Sun Oct 2 11:53:00 2022, Number of Pages: 1, Number of Words: 4, Number of Characters: 27, Security: 0
Entropy (8bit):	2.9464620025743873
TrID:	• Microsoft Word document (32009/1) 54.23% • Microsoft Word document (old ver.) (19008/1) 32.20% • Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	l6C8uDXVRN.doc
File size:	22528
MD5:	36839293424d99142586e6afd07b3260
SHA1:	67292dea75e5e63254cbe39e6a8d0b60479270b2
SHA256:	aea2494a833a1ad438574250b3132746a0055a84ee9c09964a6776c2d18dd427
SHA512:	503b477daac01f0c3f0e7b50bac7cd589f9b64c335ea4f2f373d0d99c9706b254734f3e08289a5d54dbc7e984799376efe904b76ee88a9dc05184c55180f2bff
SSDEEP:	96:wDDhElLZDQvA+6Zjp6bfu+RxCL7kzmzpxjK93ytK3HCHXWxFpgNMsAL4qab+ptjR:w/ulLZEvA+6/6rrILd/Kf3HO8tsHwJA
TLSH:	1AA2EA46B2D5CD5AF22601B08947C3C4722DBE6D5E16C24B7B643F2EFCB12B14A36749
File Content Preview:	.....>.....'.....).....&.....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "l6C8uDXVRN.doc"

Indicators

Has Summary Info:	
Application Name:	Microsoft Office Word
Encrypted Document:	False
Contains Word Document Stream:	True
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

Summary

Code Page:	1252
Title:	
Subject:	
Author:	
Keywords:	
Comments:	
Template:	
Last Saved By:	
Revion Number:	1
Total Edit Time:	60
Create Time:	2022-10-02 10:52:00
Last Saved Time:	2022-10-02 10:53:00
Number of Pages:	1
Number of Words:	4

Number of Characters:	27
Creating Application:	
Security:	0

Document Summary	
Document Code Page:	1252
Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams	
Stream Path: \x1CompObj, File Type: data, Stream Size: 114	
General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.235956365095031
Base64 Encoded:	True
Data ASCII:	. . . . . F . . . M i c r o s o f t W o r d 9 7 - 2 0 0 3 D o c u m e n t . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . 9 q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 20 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 57 6f 72 64 20 39 37 2d 32 30 30 33 20 44 6f 63 75 6d 65 6e 74 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096	
General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.24406859507157763
Base64 Encoded:	False
Data ASCII:	. . . . . + , 0 . . . . . h . . . . . p . . . . . | . . . . . T i t l e . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e8 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096	
General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.5149245210202502
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . + ' 0 . . . | . . . . . 8 . . . . . D . . . . . P . . . . . \\ . . . . . d . . . . . l . . . . . t . . . . . a y m a n a l k h a t e e b . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 7c 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 a4 00 00 00 04 00 00 00 b0 00 00 00 05 00 00 00 c8 00 00 00 06 00 00 00 d4 00 00 00 07 00 00 00 e0 00 00 00 08 00 00 00 f4 00 00 00 09 00 00 00 0c 01 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6874	
General	
Stream Path:	1Table
File Type:	data
Stream Size:	6874
Entropy:	5.90667362609459
Base64 Encoded:	True

General	
Data ASCII:	. . . . . s . . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6
Data Raw:	0e 06 0f 00 12 00 01 00 73 01 0f 00 07 00 03 00 03 00 03 00 02 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: WordDocument, File Type: data, Stream Size: 4096	
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	4096
Entropy:	1.2676117739723565
Base64 Encoded:	False
Data ASCII:	. [. . . . . 0 . . . . . > . . . . . b j b j . . . . . p a ! \\ p a ! \\ . . . . . 6 . . . . . 6 . . . . . 0 . . . . .
Data Raw:	ec a5 c1 00 5b e0 09 04 00 00 f0 12 bf 00 00 00 00 00 00 30 00 00 00 00 00 08 00 00 3e 08 00 00 0e 00 62 6a 62 6a 12 0b 12 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e 0e 00 00 70 61 21 5c 70 61 21 5c 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 6124, Parent PID: 800

General	
Target ID:	0
Start time:	16:19:55
Start date:	03/10/2022
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:	0x10b0000
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

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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\l6C8uDXVRN.doc	0	24	success or wait	1	663E115D	unknown

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
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	663D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	success or wait	1	663D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	663D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\24C52	success or wait	1	663D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	663D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	663D5805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	success or wait	1	663D5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	success or wait	1	663D5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	663D5805	unknown
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	663D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Calibri	binary	02 0F 05 02 02 02 04 03 02 04	success or wait	1	663D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\24C52	24C52	binary	04 00 00 00 EC 17 00 00 2D 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 65 00 6E 00 67 00 69 00 6E 00 65 00 65 00 72 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 D6 08 9B B9 7E D7 D8 01 52 4C 02 00 52 4C 02 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	663D5805	unknown

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	File Path	unicode	C:\Users\user\AppData\Local\Temp\imgs.htm	success or wait	1	663D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2022-10-03T16:20	success or wait	1	663D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	663D5805	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\0000610911000000000000000F01FEC\Usage	ProductFiles	dword	1430454283	1430454284	success or wait	1	663D5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\0000610911000000000000000F01FEC\Usage	ProductFiles	dword	1430454284	1430454285	success or wait	1	663D5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	WordPerfect 5.x	success or wait	1	663D5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	success or wait	1	663D5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	663D5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	WordPerfect 5.x	WordPerfect 6.x - 7.0	success or wait	1	663D5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT632.CNV	success or wait	1	663D5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	doc	wpd doc	success or wait	1	663D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\24C52	24C52	binary	04 00 00 00 EC 17 00 00 2D 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 65 00 6E 00 67 00 69 00 6E 00 65 00 65 00 72 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00	04 00 00 00 EC 17 00 00 2D 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 65 00 6E 00 67 00 69 00 6E 00 65 00 65 00 72 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67	success or wait	1	663D5805	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 D6 08 9B B9 7E D7 D8 01 52 4C 02 00 52 4C 02 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 73 00 2E 00 68 00 74 00 00 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 52 4C 02 00 52 4C 02 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

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

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

Disassembly

No disassembly