ID: 686026
Sample Name:
C1ZGt61uGv.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 04:28:08
Date: 18/08/2022
Version: 35.0.0 Citrine

Table of Contents

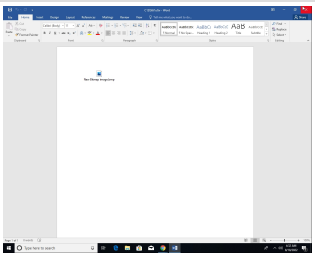
Windows Analysis Report

C1ZGt61uGv.docx

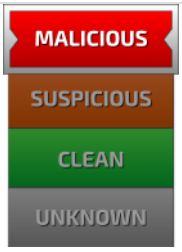
Overview

General Information

Sample Name:	C1ZGt61uGv.docx
Analysis ID:	686026
MD5:	98998af843c2c9…
SHA1:	b1a1dda90b3df0..
SHA256:	b0cfd511498cba…
Infos:	



Detection



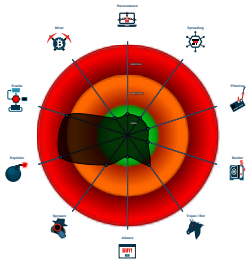
Follina CVE-2022-30190

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Microsoft Office Expl…
- Malicious sample detected (through…
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Contains an external reference to an…
- Detected suspicious Microsoft Offic…
- Queries the volume information (nam…
- Yara signature match
- Potential document exploit detected…
- Tries to load missing DLLs

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 5772 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 5500 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
document.xml.rels	SUSP_Doc_WordXMLRels_May22	Detects a suspicious pattern in docx document.xml.rels file as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard, Wojciech Cieslak	• 0x39:$a1: <Relationships • 0x3d2:$a2: TargetMode="External" • 0x3ca:$x1: .html!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x375:$olerel: relationships/oleObject • 0x38e:$target1: Target="http • 0x3d2:$mode: TargetMode="External

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
sslproxydump.pcap	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8DA80A60.htm	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x1444:$a: PCWDiagnostic • 0x1438:$sa3: ms-msdt • 0x1498:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8DA80A60.htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1427:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8DA80A60.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[1].htm	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x1444:$a: PCWDiagnostic • 0x1438:$sa3: ms-msdt • 0x1498:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[1].htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1427:$re1: location.href = "ms-msdt:
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Powershell commands sent B64 1 - Source IP: 35.186.245.55 - Destination IP: 192.168.2.22

Timestamp:	35.186.245.55192.168.2.22443491762025010 08/18/22-04:23:24.931708
SID:	2025010
Source Port:	443
Destination Port:	49176
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Powershell commands sent B64 1 - Source IP: 35.186.245.55 - Destination IP: 192.168.2.22

Timestamp:	35.186.245.55192.168.2.22443491812025010 08/18/22-04:23:28.806682
SID:	2025010
Source Port:	443
Destination Port:	49181
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Antivirus detection for dropped file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected suspicious Microsoft Office reference URL

Networking

Snort IDS alert for network traffic

System Summary

Malicious sample detected (through community Yara rule)

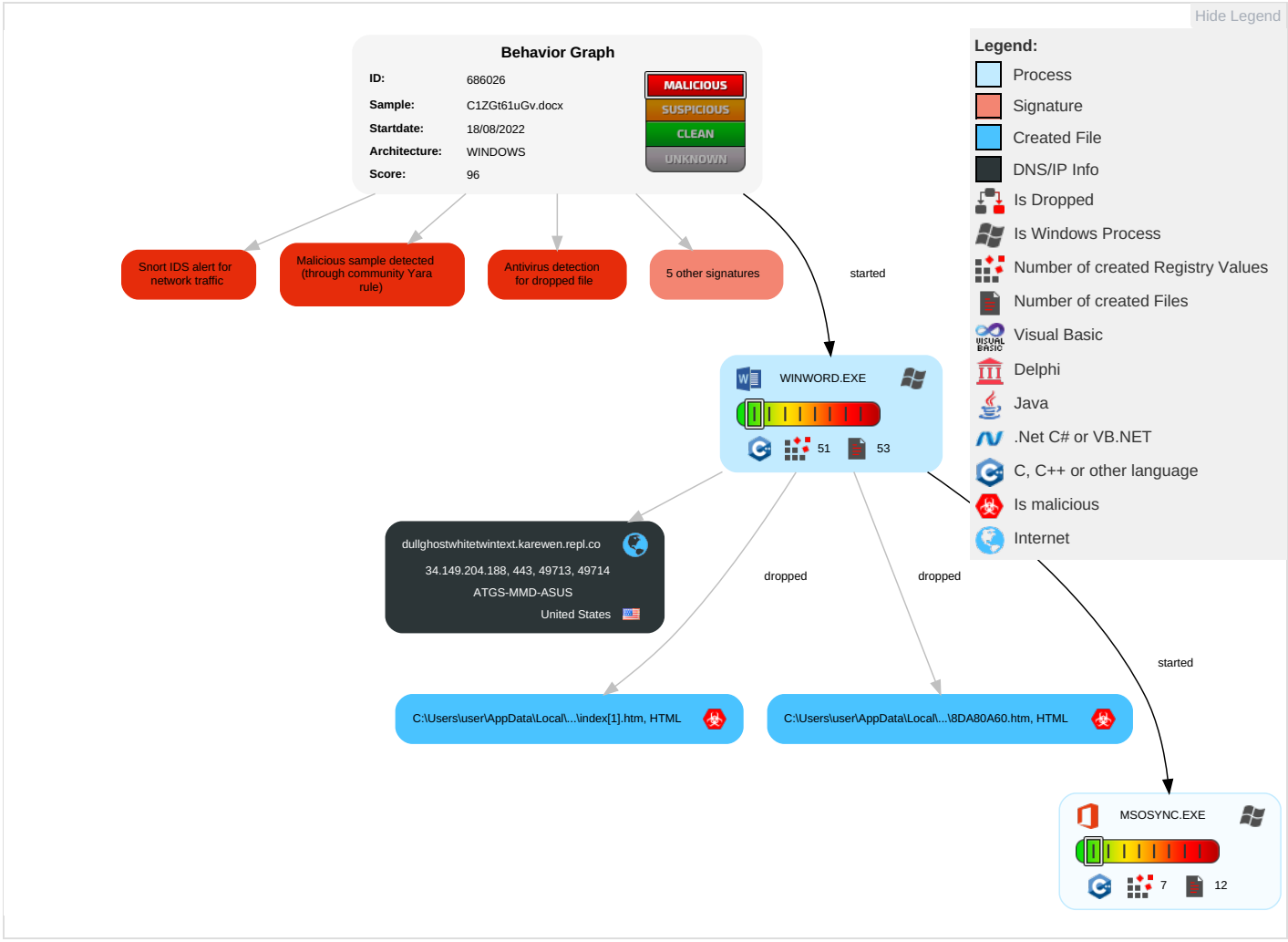
Persistence and Installation Behavior

Contains an external reference to another file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 3 Exploitation for Client Execution	1 DLL Side-Loading	1 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Process Injection	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 DLL Side-Loading	Security Account Manager	1 2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

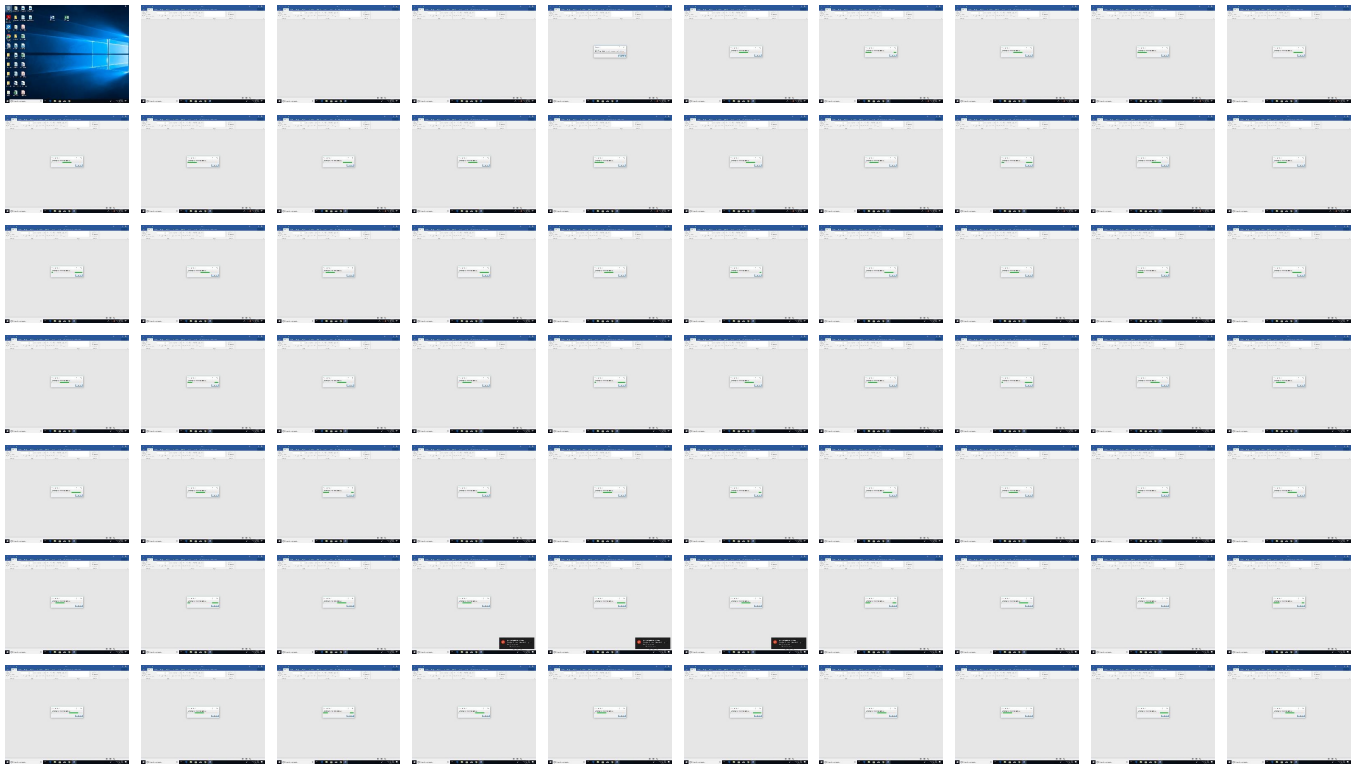
Behavior Graph

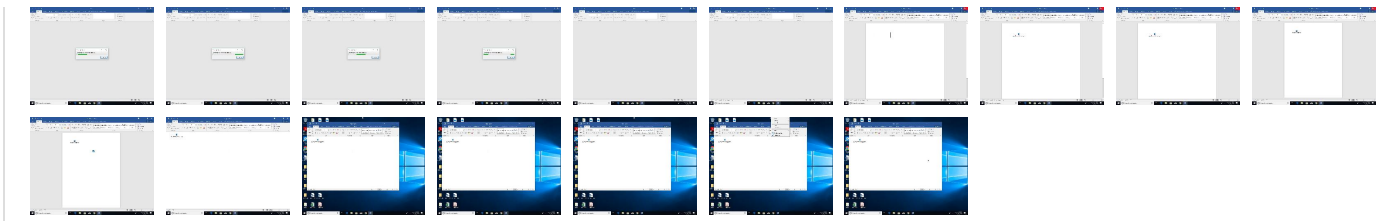


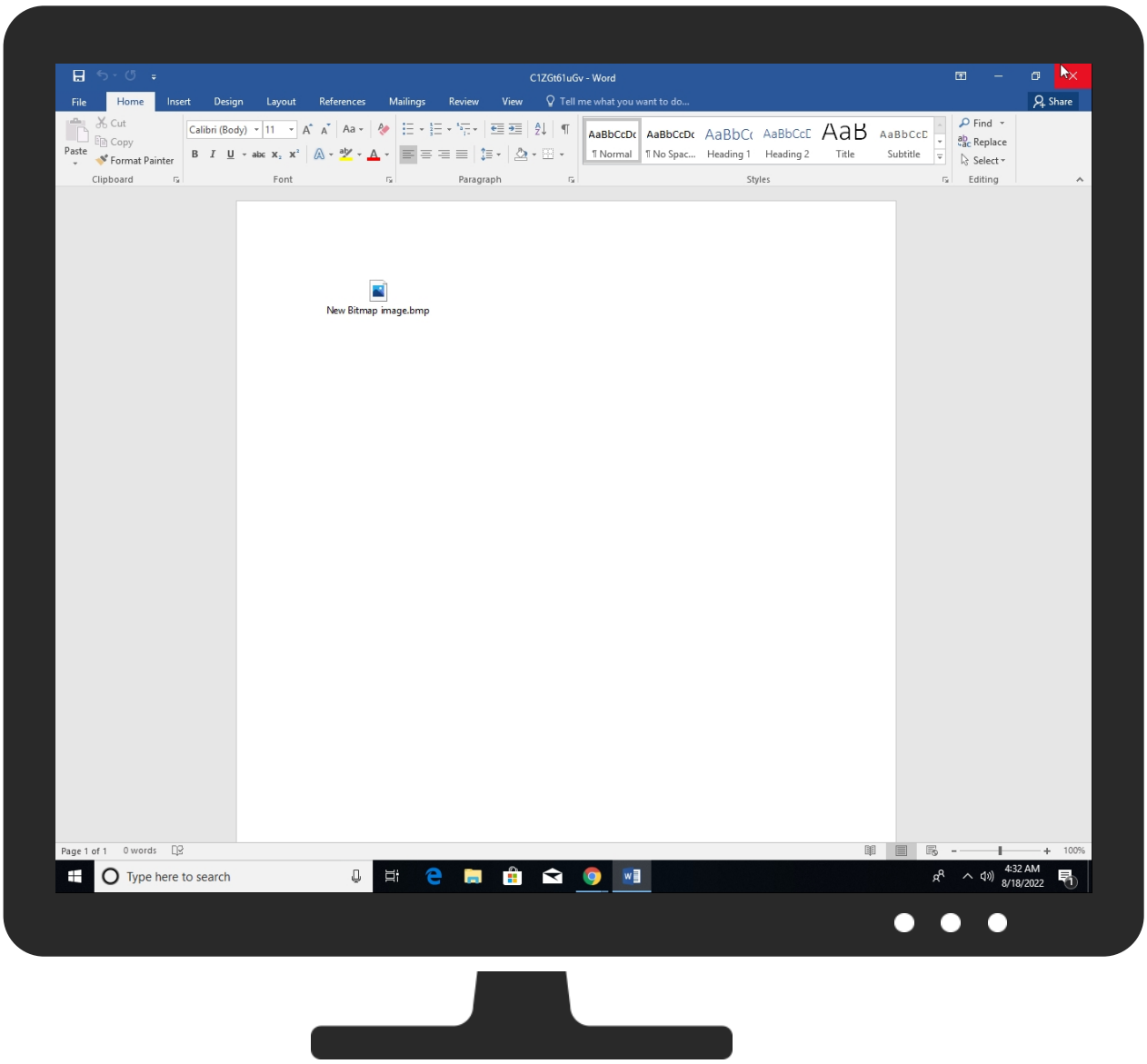
Screenshots

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
C1ZGt61uGv.docx	46%	Virustotal		Browse
C1ZGt61uGv.docx	26%	Metadefender		Browse
C1ZGt61uGv.docx	35%	ReversingLabs	Document-Word.Trojan.Minerva	
C1ZGt61uGv.docx	100%	Avira	W97M/Dldr.Agent.G1	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[1].htm	100%	Avira	JS/CVE-2022-30190.G	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8DA80A60.htm	100%	Avira	JS/CVE-2022-30190.G	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://my.microsoftpersonalcontent.com	0%	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dullghostwhitetwintext.karewen.repl.co	34.149.204.188	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://dullghostwhitetwintext.karewen.repl.co/index.html	false		high

URLs from Memory and Binaries

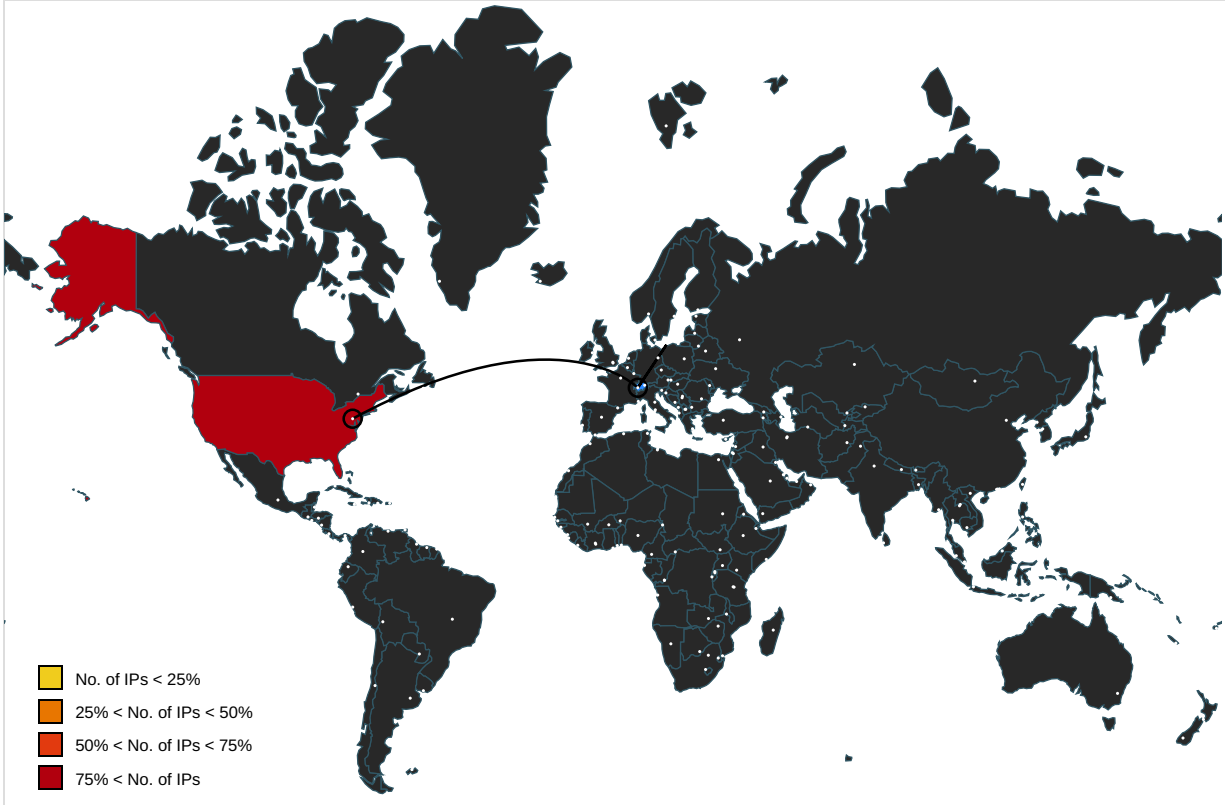
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://login.microsoftonline.com/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://autodiscover-s.outlook.com/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://roaming.edog.	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://cdn.entity.	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://powerlift.acompli.net	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://cortana.ai	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://api.aadrm.com/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://api.microsoftstream.com/api/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://cr.office.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://graph.ppe.windows.net	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://my.microsoftpersonalcontent.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://messaging.engagement.office.com/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.odwebp.svc.ms	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://web.microsoftstream.com/video/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://dataservice.o365filtering.com/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://ncus.contentsync.	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://weather.service.msn.com/data.aspx	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://apis.live.net/v5.0/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://messaging.lifecycle.office.com/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://management.azure.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://outlook.office365.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://wus2.contentsync.	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://api.office.net	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://entitlement.diagnostics.office.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://outlook.office.com/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://outlook.office365.com/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://webshell.suite.office.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://management.azure.com/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://devnull.onenote.com	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://messaging.action.office.com/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://ncus.pagecontentsync.	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high
http://https://messaging.office.com/	9AD07AEC-2B98-4723-BED2-037E998950B4.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.149.204.188	dullghostwhitetwintext.karewen.repl.co	United States		2686	ATGS-MMD-ASUS	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	686026
Start date and time:	2022-08-18 04:28:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	C1ZGt61uGv.docx
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:	25
Number of new started drivers analysed:	1
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:	mal96.expl.evad.winDOCX@3/12@2/1
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: .docx • Adjust boot time • Enable AMSI • 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, mrxdav.sys, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.76.141, 52.109.88.38, 52.109.76.36, 52.109.12.24, 52.109.76.33
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, prod-w.nexus.live.com.akadns.net, config.officeapps.live.com, prod.configsvc1.live.com.akadns.net, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, store-images.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 NtCreateFile calls found.
- 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\OfficeFileCache\CentralTable.accdb

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Microsoft Access Database
Category:	dropped
Size (bytes):	528384
Entropy (8bit):	0.47577658796690125
Encrypted:	false
SSDEEP:	384:z0HGfXArJCKE8SFNfZ0jGBChxQWfwtZ1II+hVZO4Fg:z3fXACdHZZM3Df/zI
MD5:	F1D2BA9091205066A55618062B66050A
SHA1:	41BECA7F78E2F2AEE28F1EF883608BBB0672D36E
SHA-256:	9EB44F67B6945C225F04371D022EA02E1C6761CD5F11630EB3CC5C5F083A62E2
SHA-512:	6A71B7FE43E54FEA2A93710BD3FB540109A0FD0F1C36310F8D6BA107E29D9F5EE3AB996210C4B3B13F978D523A2633B78533C61DF16E6A6DD8CDF215CD0C9E3
Malicious:	false
Reputation:	low
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...NqU.7...1.(....`.:{6....Z.C8..3..y[e.|*..|.....Q.n...f_...$.g..'D...e....F.x....-b.T...4.0..... ....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.ini

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	36
Entropy (8bit):	2.730660070105504
Encrypted:	false
SSDEEP:	3:5NixJlElGUR:WrEcUR
MD5:	1F830B53CA33A1207A86CE43177016FA
SHA1:	BDF230E1F33AFBA5C9D5A039986C6505E8B09665
SHA-256:	EAF9CDC741596275E106DDDCF8ABA61240368A8C7B0B58B08F74450D162337EF
SHA-512:	502248E893FCFB179A50863D7AC1866B5A466C9D5781499EBC1D02DF4F6D3E07B9E99E0812E747D76734274BD605DAD6535178D6CE06F08F1A02AB60335DE06
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	C.e.n.t.r.a.l.T.a.b.l.e...a.c.c.d.b.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.laccdb

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	1.4172860556164644
Encrypted:	false
SSDEEP:	3:mpl/vaV:mLu
MD5:	13B298EF83EFE8258432E1FFC9D94466
SHA1:	A093E48FD3BACC5E346ADFFC3B803ADB0CEF64C0
SHA-256:	B93F8A727C7BFD26FB41AE610DA83BA8B71C73E8058EF09F2F1B2F702BD71CED
SHA-512:	98C7D1A261AD0AC2F1AA6B03A36B7E37E6B2475A35EE42113F6ED4F52EE9BE6888D5DB29D7B69275A70A86C69C870901517B900A716E9BD38AE71ABDBE38A2BA
Malicious:	false
Reputation:	low
Preview:	927537. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\9AD07AEC-2B98-4723-BED2-037E998950B4

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	148061
Entropy (8bit):	5.358146407288765
Encrypted:	false
SSDEEP:	1536:IcQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:r1Q9DQe+zuXYr
MD5:	5C5C8FA149FACF1CBE4B3EBD3382A785
SHA1:	9BBD5D561FE0539C16C2E7EF0D5E6AAE1280DC4C
SHA-256:	F81CA7FA8430DBD1BFF3CBEDC0A28695D47CC80EEE4ACFBFFE96A3A08D24BBC4
SHA-512:	EDD3C0D7F0AE09DCC4DEF8B056346C1358F9FA53F81A6B52116E2D52AEC3434491AC6BBC3CF2037E9D2411D0DDA3C33730AEA5C44B4A51451550B668A062E49
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-08-18T02:29:04">.. Build: 16.0.15614.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.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\Microsoft\Windows\INetCache\Content.MSO\8DA80A60.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	5901
Entropy (8bit):	4.701941274629396
Encrypted:	false
SSDEEP:	96:O/iGBF2nPW5mDwID8qImX1I8vHWYMLJJ2lpyffnbTc7Om/EAEwCgEAKKiSe+0glg:OZ5mDwIDukGTlKEHbTcKCZEwCgEzKiSs
MD5:	2C855A56E062B197D4CC9D021DF71219
SHA1:	C3161D4AF43AD3DA1B08FF367C06D12FA7D483D5
SHA-256:	A6F55957542982348EB412B9B49797E1931183A6BF395016885E1294C5A08DBD
SHA-512:	11B94B5B6E3F4AEC38B15BF73A3B6836955980F5A47293266BB1FAA88005C94EBBF57465D02D8D4CF164E3F28236A7190592CA6E8C3E82A98CBF7708CF1DCDC0
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8DA80A60.htm, Author: Nasreddine Bencherchali, Christian Burkard • Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8DA80A60.htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8DA80A60.htm, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low

Preview:	<!doctype html>.<html lang="en">.<head>.<title>.Good thing we disabled macros.</title>.</head>.<body>.<p>.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor...Curabitur rutrum leo tortor, venenatis fermentum ex portti tor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit...Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique ante, dignis

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\DCC6D7C5.emf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	10172
Entropy (8bit):	3.928478624213631
Encrypted:	false
SSDEEP:	48:q373cifeyUaIWmBJOhTDOj1WN7M60iIiB7rSwVauLM/Myof9NLRgMy7k3e2kW86J:873xeXaIBckry+Ks8D+plS
MD5:	C349F98D0BBE0D72F9A6E34335918207
SHA1:	B2184C336F95E1ED5F338D1B27D06A4F8E1C535F
SHA-256:	8ACC7CBE7BEB283D3908F418FB5390623F1EB46018F426D4911F5515E786CAA5
SHA-512:	A6DE09C1E4B3947EF4B8BF46B14A3E77AFFB6004EDED3560814720B8304542F1722EFEF83502E0532C76B438015B84200302BE5CE5F8C1228A881F050BE8AE5B
Malicious:	false
Reputation:	low
Preview:	....I.....I.....'...9... EMF.....'.....8...5.....R...R...p.....S.e.g.o.e. .U.I..... .....dv.....%. .....r....$..`.....`/...`.....0...0.....?.....?.....I...4.....$..0...0...(...0...0..... .....$..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[1].htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5901
Entropy (8bit):	4.701941274629396
Encrypted:	false
SSDEEP:	96:O/iGBF2nPW5mDwID8qImX1I8vHWYMLJJ2lpyffnbTc7Om/EAEwCgEAKKiSe+0glg:OZ5mDwIDukGTlKEHbTcKCZEwCgEzKiSs
MD5:	2C855A56E062B197D4CC9D021DF71219
SHA1:	C3161D4AF43AD3DA1B08FF367C06D12FA7D483D5
SHA-256:	A6F55957542982348EB412B9B49797E1931183A6BF395016885E1294C5A08DBD
SHA-512:	11B94B5B6E3F4AEC38B15BF73A3B6836955980F5A47293266BB1FAA88005C94EBBF57465D02D8D4CF164E3F28236A7190592CA6E8C3E82A98CBF7708CF1DCDC 0
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[1].htm, Author: Nasreddine Bencherchali, Christian Burkard • Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[1].htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[1].htm, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
IE Cache URL:	http://https://dullghostwhitetwintext.karewen.repl.co/index.html
Preview:	<!doctype html>.<html lang="en">.<head>.<title>.Good thing we disabled macros.</title>.</head>.<body>.<p>.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor...Curabitur rutrum leo tortor, venenatis fermentum ex portti tor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit...Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique ante, dignis

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\C1ZGt61uGv.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Aug 16 12:41:31 2022, mtime=Thu Aug 18 01:31:47 2022, atime=Thu Aug 18 01:29:02 2022, length=26614, window=hide
Category:	dropped
Size (bytes):	1060
Entropy (8bit):	4.697968162284448
Encrypted:	false
SSDEEP:	12:8D3ZjUhcduCH2zE4ECH0+WpmtGxbKzjEjAJ/Dt3t/DmGK/NDu9u9L44t2Y+xIBj1:8D3sUKxxaoUAJbt3J8DMMk7aB6m
MD5:	59E0ACC4554DE387C6E188AC9F18E591

SHA1:	29DAEE6057B458A415690799D1B379B8AB66590D
SHA-256:	F412CE351B2C63DA034DCCD6B74F314B5B4BC72154AF85FDFD17247A2BED36D1
SHA-512:	08E150A76E5A0E4FA89B147ED68DDB3E839844991B32E781FE20465A990CFC7DD8E8EC4E26A429EDD09BC726CE6F9979DCD76265A26855CC335D434EE8E813 7
Malicious:	false
Preview:	L.....F.... ....C..u.../.....G.....g.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...U.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....U1m..user.<.....N...U.....#J.....,.j.o.n.e.s.....~.1.....U2m..Desktop.h.....N...U.....Y.....>.....8.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-2. 1.7.6.9.....l.2..g...U.. .C1ZGT6~1.DOC..P.....U0m.U.....P.....,_..C.1.Z.G.t.6.1.u.G.v...d.o.c.x.....U.....-.....T.....>.S.....C:\Users\user\Desktop\C1 ZGt61uGv.docx..&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.1.Z.G.t.6.1.u.G.v...d.o.c.x.....:..,.LB.)...As...`.....X.....927537.....!a..%.H.VZAj.....!a..%.H.VZAj..... .....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.....9...1

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.780851828270855
Encrypted:	false
SSDEEP:	3:bDuMJl+Uqe3TAlmxWtmx3TAlv:bCne3CE3W
MD5:	69F6516C10F77E405479AA56E74F44A0
SHA1:	36194337D22DE7E093B6659C3E3A1C98A2F243CE
SHA-256:	EFAE2CC5C7CBDFF13D4AC0A4FB3F0C0000C52A4E1C9AD499C834F0135A8ECCFB
SHA-512:	3443F8CF1E2804F86512DDDCEC8DF5F0F3683FA2D1E57FC4592E8A13FC7CCC9E402230D71F956DDB8D3873B6825979EB706599CB0F7B2FF32D1A993F31D945 B
Malicious:	false
Preview:	[folders]..Templates.LNK=0..C1ZGt61uGv.LNK=0..[misc]..C1ZGt61uGv.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.664661183360374
Encrypted:	false
SSDEEP:	3:Rl/Zdal6/XxUcrz1l5z14jZRest:RtZMl6/m41l5zmF4st
MD5:	1D0F7C6E4240901C9BABDE8067DDC94A
SHA1:	74559DEAC17CBF1DED4DD89B48E64331A2F701B4
SHA-256:	FF53715400739909187E1CDB686AFD0092F12B48E2A7DD2974CE5011411A483E
SHA-512:	B2922955A42F3C6298AC1C845361363D6758EAD7430FDDC6FFF936D508435340063D23981EE9A8F44A8740364412D7C337B3042C55C9135782539E4AC0758CD1
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....xF.....&.....dF.....`F.....&.....

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

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

C:\Users\user\Desktop\~$ZGt61uGv.docx

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

Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.664661183360374
Encrypted:	false
SSDEEP:	3:Rl/Zdal6/XxUcrz1l5z14jZRest:RtZMl6/m41l5zmF4st
MD5:	1D0F7C6E4240901C9BABDE8067DDC94A
SHA1:	74559DEAC17CBF1DED4DD89B48E64331A2F701B4
SHA-256:	FF53715400739909187E1CDB686AFD0092F12B48E2A7DD2974CE5011411A483E
SHA-512:	B2922955A42F3C6298AC1C845361363D6758EAD7430FDDC6FFF936D508435340063D23981EE9A8F44A8740364412D7C337B3042C55C9135782539E4AC0758CD1
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....xF.....&.....dF.....`F.....&.....

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.316883678675453
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	C1ZGt61uGv.docx
File size:	26614
MD5:	98998af843c2c938c079a102abe6c73d
SHA1:	b1a1dda90b3df0ba5f23430a6c55c48a9c3dbe9d
SHA256:	b0cfd511498cbaed084fa622cfeb1a07de7478205cbff58cb40cb89091813593
SHA512:	4b3fee7cddc41a3f742d2ca3bcc6db766e43d183b926153927ec5591d73cce2d0cf5b4ade9d0f010bf6b104f463d44e383e423984d0bf5684e58971dd0665ee7
SSDEEP:	384:aW5NndAzG46H8kwV1xEw2imBTQUhGnhHpAKIQqRrINxt/ZtNNiW2+30Ony/6MY:awlO1Ew2HGHiKpqRrSxllN2+3By/e
TLSH:	DCC2C057D12B5C75CC6A4EBCD82C8ABCEA9430D0F9151187244DE6C9B24BD73133EA1A
File Content Preview:	PK.....!..l..$u.....[Content_Types].xml ... (.....

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/686026/sample/C1ZGt61uGv.docx"

Indicators

Has Summary Info:	
Application Name:	
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

Title:	
Subject:	

Author:	Karewen .
Keywords:	
Template:	Normal.dotm
Last Saved By:	Karewen .
Revion Number:	2
Total Edit Time:	0
Create Time:	2022-06-03T10:03:00Z
Last Saved Time:	2022-06-03T10:03:00Z
Number of Pages:	1
Number of Words:	3
Number of Characters:	18
Creating Application:	Microsoft Office Word
Security:	0

Document Summary	
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:	16.0000

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 76

General

Stream Path:	\x1CompObj
File Type:	data
Stream Size:	76
Entropy:	3.093449526469053
Base64 Encoded:	False
Data ASCII:	. . . . . F . . . . O L E P a c k a g e . . . . . P a c k a g e . 9 q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 0c 00 03 00 00 00 00 00 c0 00 00 00 00 00 00 46 0c 00 00 00 4f 4c 45 20 50 61 63 6b 61 67 65 00 00 00 00 00 08 00 00 00 50 61 63 6b 61 67 65 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x1Ole10Native, File Type: data, Stream Size: 2240124

General

Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	2240124
Entropy:	0.005070123031127669
Base64 Encoded:	True
Data ASCII:	x . " . . . N e w B i t m a p i m a g e . b m p . D : \ \ S a y a a r \ \ P e r s o n a l \ \ C o d i n g \ \ M S D T Z e r o - D a y \ \ M S F o l l i n a \ \ N e w B i t m a p i m a g e . b m p . . . . . ^ . . . C : \ \ U s e r s \ \ k a r e w \ \ A p p D a t a \ \ L o c a l \ \ T e m p \ \ { 4 9 2 A 0 5 A 6 - 0 F C E - 4 3 E 2 - A F E 7 - D D 9 A E A 8 4 F C 1 B } \ \ N e w B i t m a p i m a g e . b m p . 6 , " . B M 6 , " . . . . . 6 . . . (. . . . . , " . . . . .
Data Raw:	78 2e 22 00 02 00 4e 65 77 20 42 69 74 6d 61 70 20 69 6d 61 67 65 2e 62 6d 70 00 44 3a 5c 53 61 79 61 61 72 5c 50 65 72 73 6f 6e 61 6c 5c 43 6f 64 69 6e 67 5c 4d 53 44 54 20 5a 65 72 6f 2d 44 61 79 5c 4d 53 46 6f 6c 6c 69 6e 61 5c 4e 65 77 20 42 69 74 6d 61 70 20 69 6d 61 67 65 2e 62 6d 70 00 00 00 00 03 00 5e 00 00 00 43 3a 5c 55 73 65 72 73 5c 6b 61 72 65 77 5c 41 70 70 44 61 74 61

Stream Path: \x3EPRINT, File Type: Windows Enhanced Metafile (EMF) image data version 0x10000, Stream Size: 10172

General

Stream Path:	\x3EPRINT
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Stream Size:	10172
Entropy:	3.928478624213631
Base64 Encoded:	False
Data ASCII:	. . . . l . . . . . l . . . . . ' . . . 9 . . . E M F . . . . ' . . . . . 8 . . . 5 . . . . . R . . . R . . . p . . . . . S . e . g . o . e . . U . l . . . . .
Data Raw:	01 00 00 00 6c 00 00 00 18 00 00 00 00 00 00 00 d7 00 00 00 49 00 00 00 00 00 00 00 00 00 00 00 27 0f 00 00 39 05 00 00 20 45 4d 46 00 00 01 00 bc 27 00 00 0d 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 07 00 00 38 04 00 00 35 01 00 00 ae 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 b7 04 00 b0 a7 02 00 0a 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 09 00 00 00

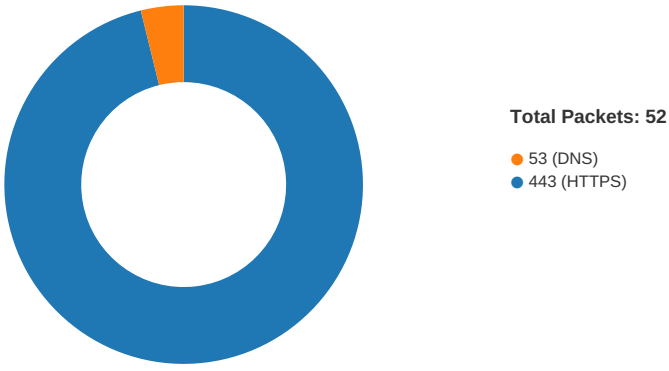
Stream Path: \x3ObjInfo, File Type: data, Stream Size: 6	
General	
Stream Path:	\x3ObjInfo
File Type:	data
Stream Size:	6
Entropy:	1.2516291673878228
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	00 00 03 00 0d 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
35.186.245.55192.168.2.22443491762025010 08/18/22-04:23:24.931708	TCP	2025010	ET TROJAN Powershell commands sent B64 1	443	49176	35.186.245.55	192.168.2.22
35.186.245.55192.168.2.22443491812025010 08/18/22-04:23:28.806682	TCP	2025010	ET TROJAN Powershell commands sent B64 1	443	49181	35.186.245.55	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 04:29:08.099875927 CEST	49713	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:08.099941015 CEST	443	49713	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:08.100186110 CEST	49713	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:08.109353065 CEST	49713	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:08.109415054 CEST	443	49713	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:08.270021915 CEST	443	49713	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:08.270116091 CEST	49713	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:08.274015903 CEST	49713	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:08.274029970 CEST	443	49713	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:08.274280071 CEST	443	49713	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:08.277177095 CEST	49713	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:08.323370934 CEST	443	49713	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:08.548890114 CEST	443	49713	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:08.549051046 CEST	443	49713	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:08.549146891 CEST	49713	443	192.168.2.4	34.149.204.188

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 04:29:08.576126099 CEST	49713	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:08.576155901 CEST	443	49713	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:08.719228029 CEST	49714	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:08.719273090 CEST	443	49714	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:08.719378948 CEST	49714	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:08.720356941 CEST	49714	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:08.720372915 CEST	443	49714	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:08.875041962 CEST	443	49714	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:08.878197908 CEST	49714	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:08.878227949 CEST	443	49714	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:08.880148888 CEST	49714	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:08.880165100 CEST	443	49714	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:09.117562056 CEST	443	49714	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:09.117639065 CEST	443	49714	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:09.117698908 CEST	49714	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:09.117733002 CEST	49714	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:09.117752075 CEST	443	49714	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:09.117762089 CEST	49714	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:09.117769003 CEST	443	49714	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:12.157325983 CEST	49715	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:12.157398939 CEST	443	49715	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:12.157541990 CEST	49715	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:12.157762051 CEST	49715	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:12.157784939 CEST	443	49715	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:12.319632053 CEST	443	49715	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:12.320421934 CEST	49715	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:12.320453882 CEST	443	49715	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:12.322175026 CEST	49715	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:12.322185993 CEST	443	49715	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:12.601583958 CEST	443	49715	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:12.601955891 CEST	49715	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:12.825898886 CEST	49716	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:12.825948000 CEST	443	49716	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:12.826054096 CEST	49716	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:12.826745033 CEST	49716	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:12.826772928 CEST	443	49716	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:13.097120047 CEST	443	49716	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:13.097235918 CEST	49716	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:13.109215021 CEST	49716	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:13.109241009 CEST	443	49716	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:13.109560966 CEST	443	49716	34.149.204.188	192.168.2.4
Aug 18, 2022 04:29:13.109628916 CEST	49716	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:13.110523939 CEST	49716	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:29:13.151379108 CEST	443	49716	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:43.476154089 CEST	443	49716	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:43.476254940 CEST	443	49716	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:43.476346016 CEST	49716	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:43.476383924 CEST	443	49716	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:43.476397038 CEST	49716	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:43.476448059 CEST	49716	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:43.477057934 CEST	443	49716	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:43.477197886 CEST	49716	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:43.478065014 CEST	49716	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:43.478091955 CEST	49716	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:43.546355963 CEST	49765	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:43.546401978 CEST	443	49765	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:43.546539068 CEST	49765	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:43.546850920 CEST	49765	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:43.546869040 CEST	443	49765	34.149.204.188	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 04:31:43.705864906 CEST	443	49765	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:43.706513882 CEST	49765	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:43.706535101 CEST	443	49765	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:43.708982944 CEST	49765	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:43.708997011 CEST	443	49765	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:43.982458115 CEST	443	49765	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:43.982800961 CEST	49765	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:44.019804001 CEST	49766	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:44.019845963 CEST	443	49766	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:44.020030975 CEST	49766	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:44.020313025 CEST	49766	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:44.020324945 CEST	443	49766	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:44.177850962 CEST	443	49766	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:44.178363085 CEST	49766	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:44.178391933 CEST	443	49766	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:44.179773092 CEST	49766	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:44.179780006 CEST	443	49766	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:44.603888035 CEST	443	49766	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:44.604222059 CEST	443	49766	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:44.604403973 CEST	49766	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:44.604461908 CEST	49766	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:44.604480028 CEST	443	49766	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:44.604510069 CEST	49766	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:44.604518890 CEST	443	49766	34.149.204.188	192.168.2.4
Aug 18, 2022 04:31:44.624933004 CEST	49767	443	192.168.2.4	34.149.204.188
Aug 18, 2022 04:31:44.624974966 CEST	443	49767	34.149.204.188	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 04:29:08.064887047 CEST	61007	53	192.168.2.4	8.8.8.8
Aug 18, 2022 04:29:08.082041979 CEST	53	61007	8.8.8.8	192.168.2.4
Aug 18, 2022 04:29:12.806756973 CEST	61124	53	192.168.2.4	8.8.8.8
Aug 18, 2022 04:29:12.824287891 CEST	53	61124	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 18, 2022 04:29:08.064887047 CEST	192.168.2.4	8.8.8.8	0x6330	Standard query (0)	dullghostwhitetwintext.karewen.repl.co	A (IP address)	IN (0x0001)
Aug 18, 2022 04:29:12.806756973 CEST	192.168.2.4	8.8.8.8	0x188b	Standard query (0)	dullghostwhitetwintext.karewen.repl.co	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 18, 2022 04:29:08.082041979 CEST	8.8.8.8	192.168.2.4	0x6330	No error (0)	dullghostwhitetwintext.karewen.repl.co		34.149.204.188	A (IP address)	IN (0x0001)
Aug 18, 2022 04:29:12.824287891 CEST	8.8.8.8	192.168.2.4	0x188b	No error (0)	dullghostwhitetwintext.karewen.repl.co		34.149.204.188	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- dullghostwhitetwintext.karewen.repl.co

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49713	34.149.204.188	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:29:08 UTC	0	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: dullghostwhitetwintext.karewen.repl.co
2022-08-18 02:29:08 UTC	0	IN	HTTP/1.1 404 Not Found Content-Length: 207 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:29:08 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7757733; includeSubDomains Connection: close
2022-08-18 02:29:08 UTC	0	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 65 20 73 65 72 76 65 72 2e 20 49 66 20 79 6f 75 20 65 6e 74 65 72 65 64 20 74 68 65 20 55 52 4c 20 6d 61 6e 75 61 6c 6c 79 20 70 6c 65 61 73 65 20 63 68 65 63 6b 20 79 6f 75 72 20 73 70 65 6c 6c 69 6e 67 20 61 6e 64 20 74 72 79 20 61 67 61 69 6e 2e 3c 2f 70 3e 0a Data Ascii: <!doctype html><html lang=en><title>404 Not Found</title> Not Found The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49714	34.149.204.188	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:29:08 UTC	0	OUT	HEAD /index.html HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-IDCRL_ACCEPTED: t Host: dullghostwhitetwintext.karewen.repl.co
2022-08-18 02:29:09 UTC	1	IN	HTTP/1.1 200 OK Content-Length: 5901 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:29:09 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7757733; includeSubDomains Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49715	34.149.204.188	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:29:12 UTC	1	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: dullghostwhitetwintext.karewen.repl.co
2022-08-18 02:29:12 UTC	1	IN	HTTP/1.1 404 Not Found Content-Length: 207 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:29:12 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7757729; includeSubDomains Connection: close
2022-08-18 02:29:12 UTC	2	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 65 20 73 65 72 76 65 72 2e 20 49 66 20 79 6f 75 20 65 6e 74 65 72 65 64 20 74 68 65 20 55 52 4c 20 6d 61 6e 75 61 6c 6c 79 20 70 6c 65 61 73 65 20 63 68 65 63 6b 20 79 6f 75 72 20 73 70 65 6c 6c 69 6e 67 20 61 6e 64 20 74 72 79 20 61 67 61 69 6e 2e 3c 2f 70 3e 0a Data Ascii: <!doctype html><html lang=en><title>404 Not Found</title> Not Found The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49716	34.149.204.188	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:29:13 UTC	2	OUT	GET /index.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: dullghostwhitetwintext.karewen.repl.co Connection: Keep-Alive
2022-08-18 02:31:43 UTC	2	IN	HTTP/1.1 502 Bad Gateway Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Strict-Transport-Security: max-age=7757728; includeSubDomains Date: Thu, 18 Aug 2022 02:31:43 GMT Content-Type: text/html; charset=utf-8 Connection: close Transfer-Encoding: chunked
2022-08-18 02:31:43 UTC	3	IN	Data Raw: 38 30 30 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 55 6e 61 62 6c 65 20 54 6f 20 57 61 6b 65 20 55 70 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 0a 20 20 20 20 20 20 20 20 20 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 49 42 4d 2b 50 6c 65 78 2b 53 61 6e 73 22 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 31 30 30 76 68 3b 0a 20 20 20 20 20 Data Ascii: 800<!DOCTYPE html><html lang="en"> <head> <title>Unable To Wake Up</title> <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=IBM+Plex+Sans"> <style> body { margin: 0; height: 100vh;
2022-08-18 02:31:43 UTC	3	IN	Data Raw: 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 40 6d 65 64 69 61 20 28 6d 61 78 2d 77 69 64 74 68 3a 20 35 30 30 70 78 29 20 7b 0a 20 20 20 20 20 20 20 20 2e 6d 65 73 73 61 67 65 20 7b 0a 20 20 20 20 20 20 20 20 20 20 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 20 63 6f 6c 75 6d 6e 3b 0a 20 20 20 20 20 20 20 20 20 20 61 6c 69 67 6e 2d 69 74 65 6d 73 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 65 76 61 6c 2d 62 6f 74 20 7b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 34 65 6d 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 73 6f 6c 65 20 7b 0a 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 30 65 31 36 32 38 3b 0a 20 20 20 20 20 20 20 20 63 6f 6c Data Ascii: } @media (max-width: 500px) { .message { flex-direction: column; align-items: center; } } .eval-bot { margin: 4em; } .console { background-color: #0e1628; col

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:31:43 UTC	6	IN	Data Raw: 35 2e 33 33 34 20 31 31 35 2e 34 30 39 20 32 34 31 2e 32 31 31 20 31 31 37 2e 38 34 39 4c 32 34 31 2e 31 39 31 20 31 31 38 2e 30 33 39 43 32 32 36 2e 34 33 36 20 31 31 36 2e 35 34 31 20 32 31 34 2e 38 37 34 20 39 34 2e 35 39 30 31 20 32 31 35 2e 30 37 38 20 36 37 2e 38 34 37 31 43 32 31 35 2e 32 38 31 20 34 31 2e 30 39 36 39 20 32 32 37 2e 31 38 33 20 31 39 2e 33 35 30 35 20 32 34 31 2e 39 35 38 20 31 38 2e 31 32 33 32 4c 32 34 31 2e 39 37 32 20 31 38 2e 33 31 33 32 56 31 38 2e 33 31 33 32 5a 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 69 6c 6c 3d 22 23 37 37 45 41 39 34 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 70 61 74 68 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 3d 22 Data Ascii: 5.334 115.409 241.211 117.849L241.191 118.039C226.436 116.541 214.874 94.5901 215.078 67.8471C215.281 41.0969 227.183 19.3505 241.958 18.1232L241.972 18.3132V18.3132Z" fill="#77EA94" /> <path d="
2022-08-18 02:31:43 UTC	6	IN	Data Raw: 20 31 32 2e 32 35 30 32 43 32 32 33 2e 32 38 34 20 31 36 2e 35 30 31 36 20 32 31 31 2e 36 34 37 20 33 39 2e 37 31 36 33 20 32 31 31 2e 34 33 20 36 37 2e 38 31 37 39 43 32 31 31 2e 34 33 20 36 38 2e 35 34 38 34 20 32 31 31 2e 34 33 20 36 39 2e 32 37 31 36 20 32 31 31 2e 34 33 37 20 37 30 2e 30 30 32 48 32 31 31 2e 33 30 37 4c 31 39 33 2e 37 32 37 20 37 30 2e 33 34 35 34 48 31 39 33 2e 36 35 39 43 31 39 33 2e 36 38 36 20 36 39 2e 34 35 34 32 20 31 39 33 2e 37 30 36 20 36 38 2e 35 35 35 37 20 31 39 33 2e 37 31 33 20 36 37 2e 36 35 37 32 43 31 39 33 2e 38 32 39 20 35 32 2e 31 33 34 35 20 31 39 30 2e 34 33 39 20 33 38 2e 30 34 33 35 20 31 38 34 2e 38 35 35 20 32 37 2e 37 38 30 32 4c 31 38 35 2e 30 37 32 20 32 37 2e 36 34 31 34 4c 31 39 33 2e 35 38 34 20 32 36 Data Ascii: 12.2502C223.284 16.5016 211.647 39.7163 211.43 67.8179C211.43 68.5484 211.43 69.2716 211.437 70.002H211.307L193.727 70.3454H193.659C193.686 69.4542 193.706 68.5557 193.713 67.6572C193.829 52.1345 190.439 38.0435 184.855 27.7802L185.072 27.6414L193.584 26

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49765	34.149.204.188	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:31:43 UTC	11	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: dullghostwhitetwintext.karewen.repl.co
2022-08-18 02:31:43 UTC	11	IN	HTTP/1.1 404 Not Found Content-Length: 207 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:31:43 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7757578; includeSubDomains Connection: close
2022-08-18 02:31:43 UTC	11	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 65 20 73 65 72 76 65 72 2e 20 49 66 20 79 6f 75 20 65 6e 74 65 72 65 64 20 74 68 65 20 55 52 4c 20 6d 61 6e 75 61 6c 6c 79 20 70 6c 65 61 73 65 20 63 68 65 63 6b 20 79 6f 75 72 20 73 70 65 6c 6c 69 6e 67 20 61 6e 64 20 74 72 79 20 61 67 61 69 6e 2e 3c 2f 70 3e 0a Data Ascii: <!doctype html><html lang=en><title>404 Not Found</title> Not Found The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49766	34.149.204.188	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:31:44 UTC	12	OUT	HEAD /index.html HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-IDCRL_ACCEPTED: t Host: dullghostwhitetwintext.karewen.repl.co

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:31:44 UTC	12	IN	HTTP/1.1 200 OK Content-Length: 5901 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:31:44 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7757577; includeSubDomains Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49767	34.149.204.188	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:31:44 UTC	12	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: dullghostwhitetwintext.karewen.repl.co
2022-08-18 02:31:45 UTC	13	IN	HTTP/1.1 404 Not Found Content-Length: 207 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:31:44 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7757577; includeSubDomains Connection: close
2022-08-18 02:31:45 UTC	13	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 65 20 73 65 72 76 65 72 2e 20 49 66 20 79 6f 75 20 65 6e 74 65 72 65 64 20 74 68 65 20 55 52 4c 20 6d 61 6e 75 61 6c 6c 79 20 70 6c 65 61 73 65 20 63 68 65 63 6b 20 79 6f 75 72 20 73 70 65 6c 6c 69 6e 67 20 61 6e 64 20 74 72 79 20 61 67 61 69 6e 2e 3c 2f 70 3e 0a Data Ascii: <!doctype html><html lang=en><title>404 Not Found</title> Not Found The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49768	34.149.204.188	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:31:45 UTC	13	OUT	GET /index.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: dullghostwhitetwintext.karewen.repl.co Connection: Keep-Alive
2022-08-18 02:31:45 UTC	13	IN	HTTP/1.1 200 OK Content-Length: 5901 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:31:45 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7757576; includeSubDomains Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:31:45 UTC	14	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 0a 47 6f 6f 64 20 74 68 69 6e 67 20 77 65 20 64 69 73 61 62 6c 65 64 20 6d 61 63 72 6f 73 0a 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 70 3e 0a 4c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20 61 6d 65 74 2c 20 63 6f 6e 73 65 63 74 65 74 75 72 20 61 64 69 70 69 73 63 69 6e 67 20 65 6c 69 74 2e 20 51 75 69 73 71 75 65 20 70 65 6c 6c 65 6e 74 65 73 71 75 65 20 65 67 65 73 74 61 73 20 6e 75 6c 6c 61 20 69 6e 20 64 69 67 6e 69 73 73 69 6d 2e 20 4e 61 6d 20 69 64 20 6d 61 75 72 69 73 20 6c 6f 72 65 6d 2e 20 4e 75 6e 63 20 73 75 73 63 69 70 69 74 20 69 64 20 6d 61 67 6e 61 Data Ascii: <!doctype html><html lang="en"><head><title>Good thing we disabled macros</title></head><body><p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna
2022-08-18 02:31:45 UTC	15	IN	Data Raw: 2c 20 73 65 6d 70 65 72 20 74 75 72 70 69 73 20 75 74 2c 20 67 72 61 76 69 64 61 20 6c 6f 72 65 6d 2e 20 50 72 6f 69 6e 20 61 72 63 75 20 6c 69 67 75 6c 61 2c 20 76 65 6e 65 6e 61 74 69 73 20 61 6c 69 71 75 61 6d 20 74 72 69 73 74 69 71 75 65 20 75 74 2c 20 70 72 65 74 69 75 6d 20 71 75 69 73 20 76 65 6c 69 74 2e 0a 0a 50 68 61 73 65 6c 6c 75 73 20 74 72 69 73 74 69 71 75 65 20 6f 72 63 69 20 65 6e 69 6d 2c 20 61 74 20 61 63 63 75 6d 73 61 6e 20 76 65 6c 69 74 20 69 6e 74 65 72 64 75 6d 20 65 74 2e 20 41 65 6e 65 61 6e 20 6e 65 63 20 74 72 69 73 74 69 71 75 65 20 61 6e 74 65 2c 20 64 69 67 6e 69 73 73 69 6d 20 63 6f 6e 76 61 6c 6c 69 73 20 6c 69 67 75 6c 61 2e 20 41 65 6e 65 61 6e 20 71 75 69 73 20 65 6c 65 69 66 65 6e 64 20 64 6f 6c 6f 72 2e 20 49 6e 20 71 75 69 Data Ascii: , semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique ante, dignissim convallis ligula. Aenean quis felis dolor. In qui
2022-08-18 02:31:45 UTC	17	IN	Data Raw: 73 2c 20 74 75 72 70 69 73 20 64 6f 6c 6f 72 20 65 6c 65 69 66 65 6e 64 20 6d 61 73 73 61 2c 20 69 6e 20 6d 61 78 69 6d 75 73 20 73 61 70 69 65 6e 20 64 75 69 20 65 74 20 74 6f 72 74 6f 72 2e 20 51 75 69 73 71 75 65 20 76 61 72 69 75 73 20 65 6e 69 6d 20 73 65 64 20 65 6e 69 6d 20 76 65 6e 65 6e 61 74 69 73 20 74 65 6d 70 6f 72 2e 20 50 72 61 65 73 65 6e 74 20 71 75 69 73 20 76 6f 6c 75 74 70 61 74 20 6c 6f 72 65 6d 2e 20 50 65 6c 6c 65 6e 74 65 73 71 75 65 20 61 63 20 76 65 6e 65 6e 61 74 69 73 20 6c 61 63 75 73 2c 20 76 69 74 61 65 20 63 6f 6d 6d 6f 64 6f 20 6f 64 69 6f 2e 20 53 65 64 20 69 6e 20 6d 65 74 75 73 20 61 74 20 6c 69 62 65 72 6f 20 76 69 76 65 72 72 61 20 6d 6f 6c 6c 69 73 20 73 65 64 20 76 69 74 61 65 20 6e 69 62 68 2e 20 53 65 64 20 61 74 Data Ascii: s, turpis dolor eleifend massa, in maximus sapien dui et tortor. Quisque varius enim sed enim venenatis tempor. Praesent quis volutpat lorem. Pellentesque ac venenatis lacus, vitae commodo odio. Sed in metus at libero viverra mollis sed vitae nibh. Sed at
2022-08-18 02:31:45 UTC	17	IN	Data Raw: 20 71 75 69 73 20 65 6c 65 69 66 65 6e 64 20 6e 65 63 2c 20 73 75 73 63 69 70 69 74 20 73 69 74 20 61 6d 65 74 20 6d 61 73 73 61 2e 20 56 69 76 61 6d 75 73 20 69 6e 20 6c 65 63 74 75 73 20 65 72 61 74 2e 20 4e 75 6c 6c 61 20 66 61 63 69 6c 69 73 69 2e 20 56 69 76 61 6d 75 73 20 73 65 64 20 6d 61 73 73 61 20 71 75 69 73 20 61 72 63 75 20 65 67 65 73 74 61 73 20 76 65 68 69 63 75 6c 61 2e 20 4e 75 6c 6c 61 20 6d 61 73 73 61 20 6c 6f 72 65 6d 2c 20 74 69 6e 63 69 64 75 6e 74 20 73 65 64 20 66 65 75 67 69 61 74 20 71 75 69 73 2c 20 66 61 75 63 69 62 75 73 20 61 20 72 69 73 75 73 2e 20 53 65 64 20 76 69 76 65 72 72 61 20 74 75 72 70 69 73 20 73 69 74 20 61 6d 65 74 20 6d 65 74 75 73 20 69 61 63 75 6c 69 73 20 66 69 6e 69 62 75 73 2e 0a 0a 4d 6f 72 62 69 20 63 Data Ascii: quis eleifend nec, suscipit sit amet massa. Vivamus in lectus erat. Nulla facilisi. Vivamus sed massa quis arcu egestas vehicula. Nulla massa lorem, tincidunt sed feugiat quis, faucibus a risus. Sed viverra turpis sit amet metus iaculis finibus.Morbi c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49769	34.149.204.188	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:31:45 UTC	20	OUT	HEAD /index.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: dullghostwhitetwintext.karewen.repl.co Connection: Keep-Alive
2022-08-18 02:31:46 UTC	20	IN	HTTP/1.1 200 OK Content-Length: 5901 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:31:46 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7757576; includeSubDomains Connection: close

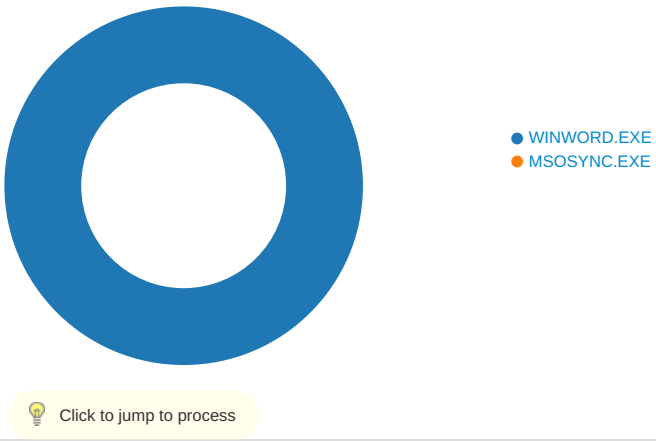
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49770	34.149.204.188	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:31:46 UTC	20	OUT	HEAD /index.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: dullghostwhitetwintext.karewen.repl.co Connection: Keep-Alive
2022-08-18 02:31:46 UTC	20	IN	HTTP/1.1 200 OK Content-Length: 5901 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:31:46 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7757575; includeSubDomains Connection: close

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **5772**, Parent PID: **796**

General

Target ID:	0
Start time:	04:29:02
Start date:	18/08/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0xd60000
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
Registry Activities

Analysis Process: MSOSYNC.EXE PID: **5500**, Parent PID: **5772**

General

Target ID:	1
Start time:	04:29:08
Start date:	18/08/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe
Imagebase:	0x940000
File size:	466688 bytes
MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

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