

JOeSandbox Cloud BASIC



ID: 686004

Sample Name:
dl18aYTB05.docx

Cookbook:
defaultwindowsofficecookbook.jbs

Time: 03:56:06

Date: 18/08/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report dl18aYTB05.docx	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	4
Initial Sample	4
PCAP (Network Traffic)	5
Dropped Files	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Exploits	6
System Summary	6
Persistence and Installation Behavior	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	9
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	9
World Map of Contacted IPs	12
Public IPs	12
General Information	12
Warnings	13
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASNs	14
JA3 Fingerprints	14
Dropped Files	14
Created / dropped Files	14
C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.accdb	14
C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.ini	14
C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.laccdb	14
C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\CE458921-C0C4-4579-9BB4-3A4F11873036	15
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Content.MSO\1BDECE2D.txt	15
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Content.MSO\4C4C1387.txt	15
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMUU\bad[1].html	16
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMUU\bad[1].txt (copy)	16
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\CS6IXJW6\bad[1].html	17
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\CS6IXJW6\bad[1].txt (copy)	17
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\dl18aYTB05.LNK	18
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	18
C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm	18
C:\Users\user\AppData\Roaming\Microsoft\UPProof\CUSTOM.DIC	19
C:\Users\user\Desktop\~\$18aYTB05.docx	19
Static File Info	19
General	19
File Icon	19
Network Behavior	20
Network Port Distribution	20
TCP Packets	20
UDP Packets	22
DNS Queries	22
DNS Answers	22
HTTP Request Dependency Graph	22

HTTPS Proxied Packets	22
Statistics	41
Behavior	41
System Behavior	41
Analysis Process: WINWORD.EXEPID: 5828, Parent PID: 796	41
General	41
File Activities	41
Registry Activities	41
Analysis Process: MSOSYNC.EXEPID: 5700, Parent PID: 5828	41
General	41
File Activities	42
Registry Activities	42
Disassembly	42

Windows Analysis Report

dl18aYTB05.docx

Overview

General Information

Sample Name:

dl18aYTB05.docx

Analysis ID:

686004

MD5:

b91615355a11f5..

SHA1:

7950b1730e05a2..

SHA256:

3fdd30eb0961c9..

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Follina CVE-2022-30190

Score: 96

Range: 0 - 100

Whitelisted: false

Confidence: 100%

Signatures

Antivirus / Scanner detection for sub...

Multi AV Scanner detection for subm...

Yara detected Microsoft Office Expl...

Malicious sample detected (through...

Multi AV Scanner detection for dom...

Antivirus detection for dropped file

Contains an external reference to an...

Detected suspicious Microsoft Offic...

Queries the volume information (nam...

Yara signature match

Potential document exploit detected...

Tries to load missing DLLs

Classification

Process Tree

System is w10x64

WINWORD.EXE (PID: 5828 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)

MSOSYNC.EXE (PID: 5700 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)

cleanup

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample				
Source	Rule	Description	Author	Strings
document.xml.rels	SUSP_Doc_WordXMLRels_May22	Detects a suspicious pattern in docx document.xml.rels file as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard, Wojciech Cieslak	0x39:\$a1: <Relationships 0x77c:\$a2: TargetMode="External" 0x774:\$x1: .html!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is referencing an external target in dropper OOXML documents	ditekSHen	0x703:\$olerel: relationships/oleObject 0x71c:\$target1: Target="http 0x77c:\$mode: TargetMode="External"

PCAP (Network Traffic)				
Source	Rule	Description	Author	Strings
sslproxypcap.pcap	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	0x3d19a:\$a: PCWDiagnostic 0x44b3e:\$a: PCWDiagnostic 0x48342:\$a: PCWDiagnostic 0x3d18e:\$sa3: ms-msdt 0x44b32:\$sa3: ms-msdt 0x48336:\$sa3: ms-msdt 0x3d20d:\$sb3: IT_BrowseForFile= 0x44bb1:\$sb3: IT_BrowseForFile= 0x483b5:\$sb3: IT_BrowseForFile=
sslproxypcap.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\NetCache\Content.MSO\4C4C1387.txt	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	0x1efa:\$a: PCWDiagnostic 0x1eee:\$sa3: ms-msdt 0x1f6d:\$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Content.MSO\4C4C1387.txt	EXPL_Follina_CVE_2022_30190_Msdt_MSPProtocolURL_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	0x1edd:\$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Content.MSO\4C4C1387.txt	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\bad[1].html	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	0x1efa:\$a: PCWDiagnostic 0x1eee:\$sa3: ms-msdt 0x1f6d:\$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\bad[1].html	EXPL_Follina_CVE_2022_30190_Msdt_MSPProtocolURL_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	0x1edd:\$re1: location.href = "ms-msdt:
Click to see the 7 entries				

Sigma Signatures	
	No Sigma rule has matched

Snort Signatures	
	No Snort rule has matched

Joe Sandbox Signatures	
------------------------	--

AV Detection	
Antivirus / Scanner detection for submitted sample	
Multi AV Scanner detection for submitted file	
Multi AV Scanner detection for domain / URL	



Exploits



Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected suspicious Microsoft Office reference URL

System Summary



Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

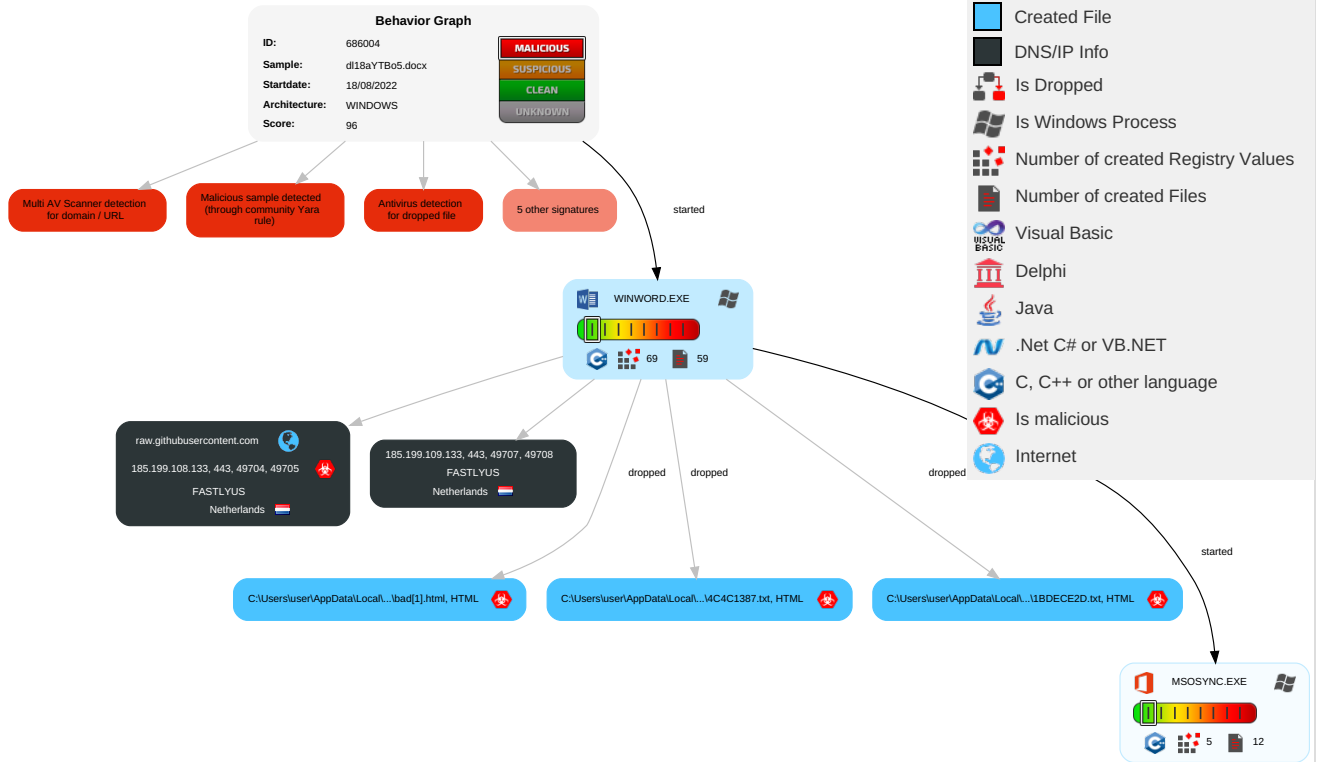


Contains an external reference to another file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	13 Exploitation for Client Execution	1 DLL Side-Loading	1 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Process Injection	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 DLL Side-Loading	Security Account Manager	12 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	14 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

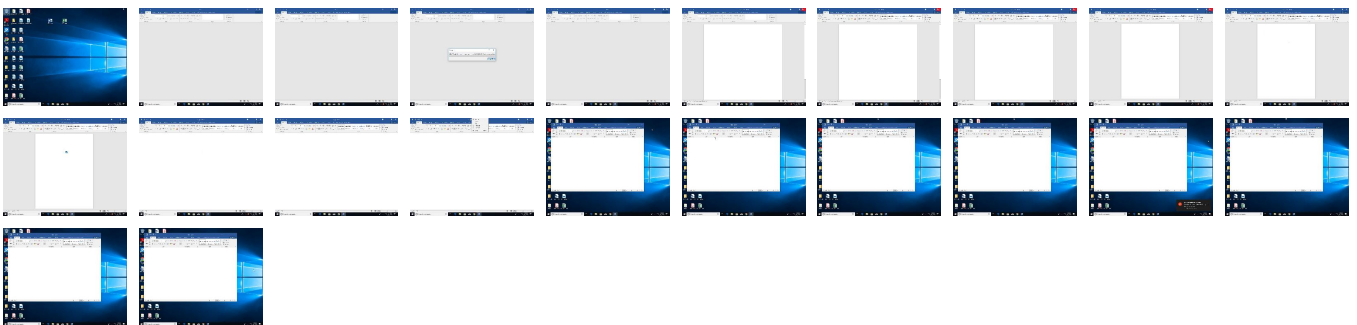
Behavior Graph

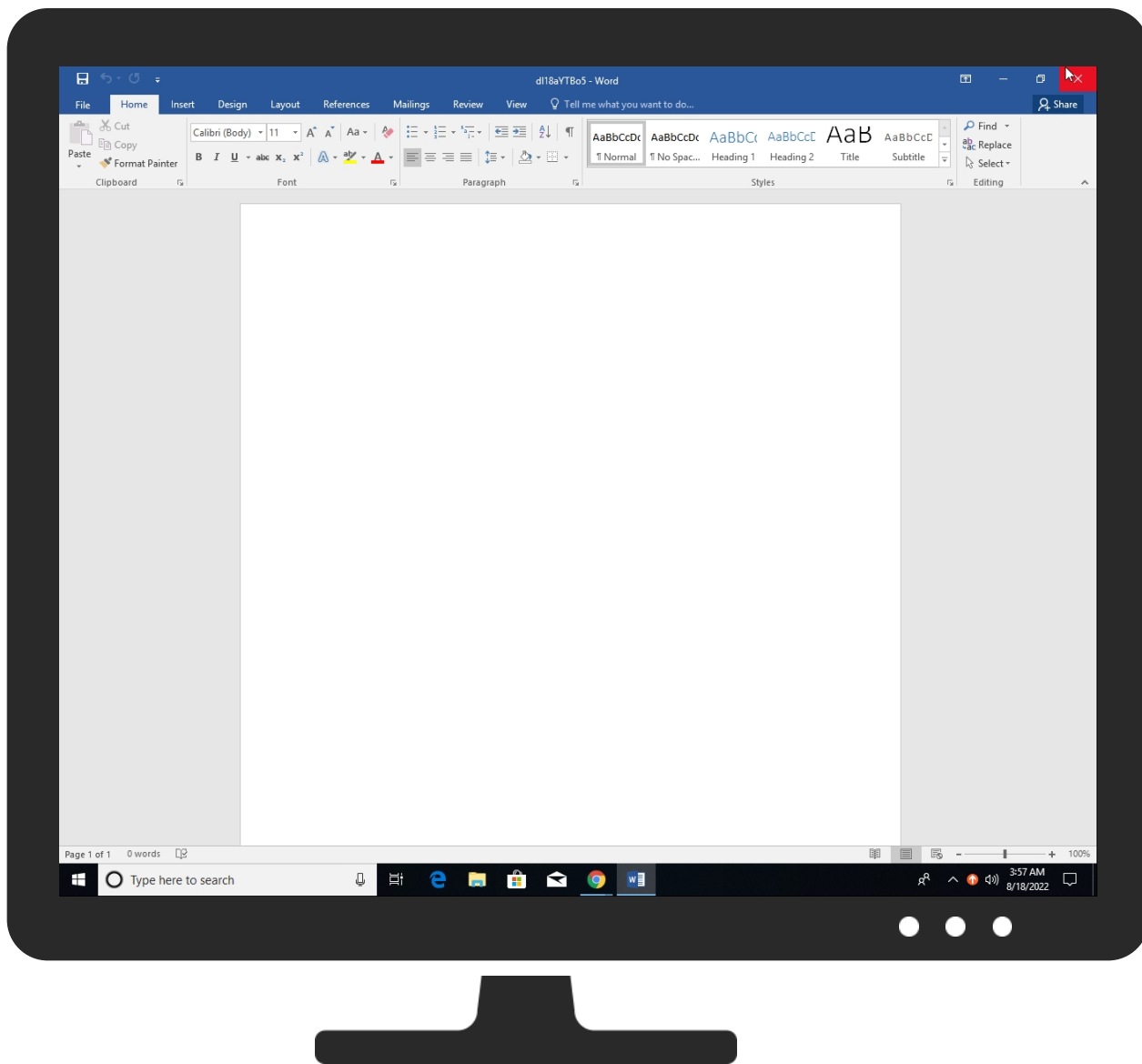


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
dl18aYTB05.docx	51%	Virustotal		Browse
dl18aYTB05.docx	20%	Metadefender		Browse
dl18aYTB05.docx	28%	ReversingLabs	Document-Word.Exploit.Heuristic	
dl18aYTB05.docx	100%	Avira	W97M/Dldr.Agent.G1	

Dropped Files

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

Unpacked PE Files

 No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
raw.githubusercontent.com	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://my.microsoftpersonalcontent.com	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://raw.githubusercontent.com/drgreenthumb93/CVE-2022-30190-follina/main/bad.html	6%	Virustotal		Browse
http://https://raw.githubusercontent.com/drgreenthumb93/CVE-2022-30190-follina/main/bad.html	0%	Avira URL Cloud	safe	
http://https://asgmsproxyapi.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
raw.githubusercontent.com	185.199.108.133	true	true	1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://raw.githubusercontent.com/drgreenthumb93/CVE-2022-30190-follina/main/bad.html	true	6%, Virustotal, Browse - Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

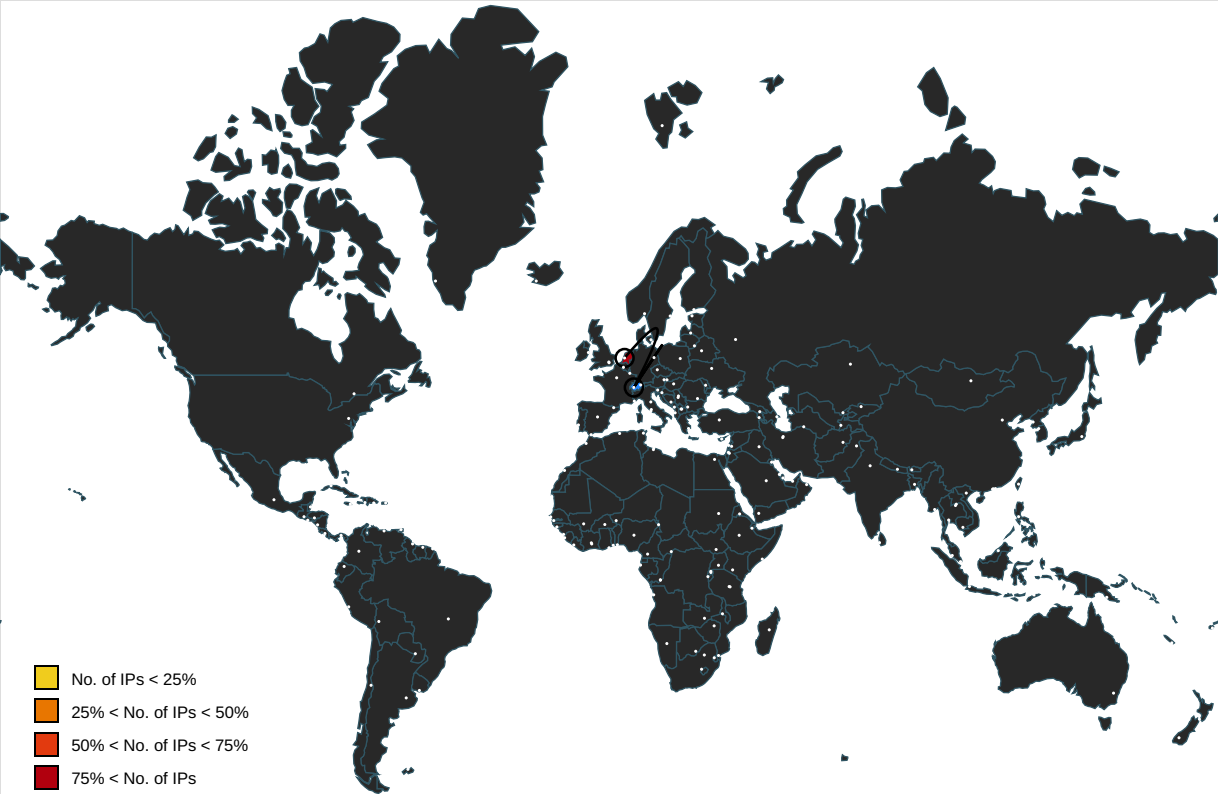
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticsdf.office.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://login.microsoftonline.com/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://shell.suite.office.com:1443	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://autodiscover-s.outlook.com/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://roaming.edog.	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://cdn.entity.	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://powerlift.acompli.net	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://cortana.ai	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://entitlement.diagnosticsdf.office.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://api.aadrm.com/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://api.microsoftstream.com/api/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://cr.office.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://graph.ppe.windows.net	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://my.microsoftpersonalcontent.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://messaging.engagement.office.com/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticsdf.office.com/v2/feedback	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://web.microsoftstream.com/video/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.addins.store.officeppe.com/addinstemplate	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://dataservice.o365filtering.com/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://ncus.contentsync	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscover.service.svc/root/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://weather.service.msn.com/data.aspx	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://apis.live.net/v5.0/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://messaging.lifecycle.office.com/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://management.azure.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://outlook.office365.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://wus2.contentsync	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://api.office.net	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://incidents.diagnostics.sdf.office.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://asgmsproxyapi.azurewebsites.net/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://entitlement.diagnostics.office.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://outlook.office.com/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://outlook.office365.com/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://webshell.suite.office.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://substrate.office.com/search/api/v1/SearchHistory	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://management.azure.com/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http:// https://messaging.lifecycle.office.com/getcustommessage16	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http:// https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http:// https://login.windows.net/common/oauth2/authorize	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http:// https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	URL Reputation: safe	unknown
http://https://graph.windows.net/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://devnull.onenote.com	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://messaging.action.office.com/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://ncus.pagecontentsync.	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false	URL Reputation: safe	unknown
http:// https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high
http://https://messaging.office.com/	CE458921-C0C4-4579-9BB4-3A4F11873036.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.199.109.133	unknown	Netherlands		54113	FASTLYUS	false
185.199.108.133	raw.githubusercontent.com	Netherlands		54113	FASTLYUS	true

General Information

Joe Sandbox Version:

35.0.0 Citrine

Analysis ID:	686004
Start date and time:	2022-08-18 03:56:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dl18aYTB05.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.expl.evad.winDOCX@3/15@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .docx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, mrxdav.sys, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.76.141, 52.109.12.24, 52.109.88.40, 52.109.88.39
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, prod-w.nexus.live.com.akadns.net, store-images.s.microsoft.com, config.officeapps.live.com, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

 No simulations

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files	
C:\Users\user\AppData\Local\Microsoft\Office\16.0\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):	0.4757000931758257
Encrypted:	false
SSDEEP:	384:KGfXGwX2JCwNR/f/HNvs8SF3fZ0jGB8wTvW6wtZ1lj+hVZO4Fg:hXGsmCdHvZyWe6/Ql
MD5:	CD17EFEF7B2FFAF9A9AA5B66A3ECFBFB
SHA1:	9C39FDE7C9A92D372A3EDA777E0E12C4042F37B6
SHA-256:	E943911CD0EE1A288605391DDDD0D342AE90CB285DB5F6340310370255BAEDFDD
SHA-512:	033D8FAF9119EB39224563151161619172B416D1D076646FA2B7CF98DC05ECE6B42907FF9F42159B7D385A23403CA6AF5F5F39FF583ECC6426E578C2DE2C5489
Malicious:	false
Reputation:	low
Preview:	Standard ACE DB.....n.b'..U.gr@?.~.....1.y..0...c...F...NqU.7...1.(....`.:{6....Z.C8..3..y[e. *..#....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:	3:5NixJIEIGUR:WrEcUR
MD5:	1F830B53CA33A1207A86CE43177016FA
SHA1:	BDF230E1F33AFBA5C9D5A039986C6505E8B09665
SHA-256:	EAF9CDC741596275E106DDDCF8ABA61240368A8C7B0B58B08F74450D162337EF
SHA-512:	502248E893FCFB179A50863D7AC1866B5A466C9D5781499EBC1D02DF4F6D3E07B9E99E0812E747D76734274BD605DAD6535178D6CE06F08F1A02AB60335DE06
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	C.e.n.t.r.a.l.T.a.b.l.e...a.c.c.d.b.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.laccdb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	1.4172860556164644

[illegible][illegible]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMU\bad[1].txt (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

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

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

C:\Users\user\Desktop\~\$18aYTB05.docx

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.358092282332054
Encrypted:	false
SSDEEP:	3:RI/ZddSBdl/tlpWQUnlqSpUWdQ6ltlltr:RtZfSr7WBooPvB
MD5:	375CCA4DBD946D609D4615D1F34044E2
SHA1:	D5FE02B6D69BE028B1DE29CABE684B7BB1AA83EC
SHA-256:	D8491E148D3AB089497B0709FE2B1C4DB166CDFAE6E3D1D07006B75D04CE087
SHA-512:	FB6BC1DBA2F9DE09395A1BA7AAB33C067F3C1ABE49677152C3008C18E0B81D8798D22E85471CA1AF85BDF1010D88442E59EA50FFE3D9C020A59B3AAE0003D249
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....s..F.....s..1.....T.....6C..8.6.s.....

Static File Info

General

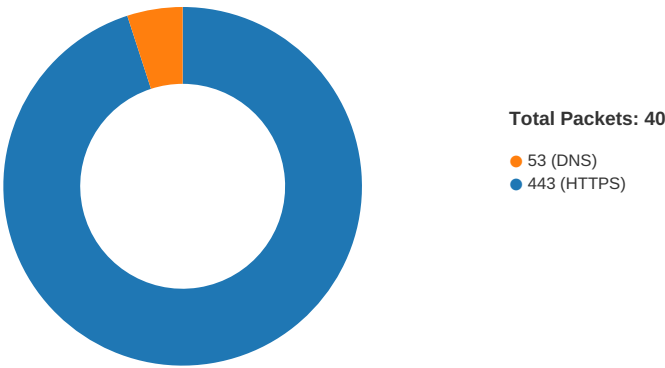
File type:	Microsoft OOXML
Entropy (8bit):	7.869840361272895
TrID:	- Word Microsoft Office Open XML Format document (49504/1) 49.01% - Word Microsoft Office Open XML Format document (43504/1) 43.07% - ZIP compressed archive (8000/1) 7.92%
File name:	dl18aYTB05.docx
File size:	10190
MD5:	b91615355a11f5bb8b7c381a8bc4485a
SHA1:	7950b1730e05a2dcdd19f1a98a697798a9edbf77
SHA256:	3fdd30eb0961c98259d58327745ec253588b1553d9822d613d45d076c4b07ec1
SHA512:	c8fbe110484db356ff4f67bcad94930b26fab9040a560a5a0d466d5766b2430b64585132048f787f0c7766b12e33ab765d415bd08a5fb7482a12d1da9160a00a
SSDEEP:	192:E5VR2DuRkZx41Jlb8VPkf+CFk4v1Y2VveFLC9Fi/CRQIZleDM:EHkZx0ID9+2Vv6aRdleDM
TLSH:	73229D3BEAA50DB4C6E69275E0AC1A25C35C06B7F33DF94A349423D812C85DD5BE530C
File Content Preview:	PK.....C.T...L.....[Content_Types].xml...n.0.E...m.NR....X...~...'.l.....Cl....sg..'.m..kp^...Q4d...H..1.X...., (.....x6..L.;>.b.c.!...}.A d,h.....i.....K....;.....1.R.M'O..U....^WF.....Ub....6W.@.....(aM...r..3e....?J(#.....7..S...p

File Icon

	
Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 03:57:05.526428938 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.526494026 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.526593924 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.526906967 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.526932955 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.573925018 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.574052095 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.577141047 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.577157974 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.577445030 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.579032898 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.603962898 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.604150057 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.604202032 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.604235888 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.604248047 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.604283094 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.604307890 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.604378939 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.604424953 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.604434967 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.604449987 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.604504108 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.604840040 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.604918957 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.604983091 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.604996920 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.605057001 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.605220079 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.605230093 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.605627060 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.605735064 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.606307030 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.606355906 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.606370926 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.606384993 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.606451035 CEST	443	49704	185.199.108.133	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 03:57:05.606506109 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.606517076 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.607175112 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.607285976 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.607351065 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.607368946 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.607424974 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.607436895 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.608016968 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.608083010 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.608097076 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.608172894 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.608227015 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.608237982 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.608653069 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.608716965 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.608731985 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.608810902 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.608866930 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.608879089 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.608949900 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.609002113 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.609014988 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.609500885 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.609566927 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.609579086 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.619195938 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.619288921 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.619314909 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.619474888 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.619538069 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.619549990 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.619615078 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.619692087 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.619694948 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.619714975 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.619767904 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.619786978 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.619930029 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.619982958 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.619997025 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.620279074 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.620335102 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.620351076 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.620439053 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.620496035 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.620510101 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.620980978 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.621049881 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.621067047 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.621174097 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.621242046 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.621253967 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.621484995 CEST	443	49704	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.621555090 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.630376101 CEST	49704	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.674331903 CEST	49705	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.674370050 CEST	443	49705	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.674452066 CEST	49705	443	192.168.2.4	185.199.108.133

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 03:57:05.674659967 CEST	49705	443	192.168.2.4	185.199.108.133
Aug 18, 2022 03:57:05.674670935 CEST	443	49705	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.709250927 CEST	443	49705	185.199.108.133	192.168.2.4
Aug 18, 2022 03:57:05.725590944 CEST	49705	443	192.168.2.4	185.199.108.133

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 03:57:05.506854057 CEST	52239	53	192.168.2.4	8.8.8.8
Aug 18, 2022 03:57:05.525362015 CEST	53	52239	8.8.8.8	192.168.2.4
Aug 18, 2022 03:57:09.049834013 CEST	61007	53	192.168.2.4	8.8.8.8
Aug 18, 2022 03:57:09.066267014 CEST	53	61007	8.8.8.8	192.168.2.4

DNS Queries							
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 18, 2022 03:57:05.506854057 CEST	192.168.2.4	8.8.8.8	0x5d75	Standard query (0)	raw.github usercontent.com	A (IP address)	IN (0x0001)
Aug 18, 2022 03:57:09.049834013 CEST	192.168.2.4	8.8.8.8	0xd5d0	Standard query (0)	raw.github usercontent.com	A (IP address)	IN (0x0001)

DNS Answers									
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 18, 2022 03:57:05.525362015 CEST	8.8.8.8	192.168.2.4	0x5d75	No error (0)	raw.github usercontent.com		185.199.108.133	A (IP address)	IN (0x0001)
Aug 18, 2022 03:57:05.525362015 CEST	8.8.8.8	192.168.2.4	0x5d75	No error (0)	raw.github usercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Aug 18, 2022 03:57:05.525362015 CEST	8.8.8.8	192.168.2.4	0x5d75	No error (0)	raw.github usercontent.com		185.199.110.133	A (IP address)	IN (0x0001)
Aug 18, 2022 03:57:05.525362015 CEST	8.8.8.8	192.168.2.4	0x5d75	No error (0)	raw.github usercontent.com		185.199.111.133	A (IP address)	IN (0x0001)
Aug 18, 2022 03:57:09.066267014 CEST	8.8.8.8	192.168.2.4	0xd5d0	No error (0)	raw.github usercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Aug 18, 2022 03:57:09.066267014 CEST	8.8.8.8	192.168.2.4	0xd5d0	No error (0)	raw.github usercontent.com		185.199.111.133	A (IP address)	IN (0x0001)
Aug 18, 2022 03:57:09.066267014 CEST	8.8.8.8	192.168.2.4	0xd5d0	No error (0)	raw.github usercontent.com		185.199.108.133	A (IP address)	IN (0x0001)
Aug 18, 2022 03:57:09.066267014 CEST	8.8.8.8	192.168.2.4	0xd5d0	No error (0)	raw.github usercontent.com		185.199.110.133	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph	
raw.githubusercontent.com	

HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49704	185.199.108.133	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:05 UTC	0	OUT	OPTIONS /drgreenthumb93/CVE-2022-30190-follina/main/ 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: raw.githubusercontent.com

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:05 UTC	0	IN	HTTP/1.1 403 Forbidden Connection: close Cache-Control: no-cache Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-Frame-Options: deny X-XSS-Protection: 0 Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline' Accept-Ranges: bytes Date: Thu, 18 Aug 2022 01:57:05 GMT Via: 1.1 varnish X-Served-By: cache-mxp6929-MXP X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1660787826.582963,VS0,VE9 Access-Control-Allow-Origin: * X-Fastly-Request-ID: 3ff7e4b791bcf59d1adae5143531aa79a139b0de Expires: Thu, 18 Aug 2022 02:02:05 GMT Vary: Authorization,Accept-Encoding transfer-encoding: chunked
2022-08-18 01:57:05 UTC	0	IN	Data Raw: 34 32 61 0d 0a Data Ascii: 42a
2022-08-18 01:57:05 UTC	0	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 0d 0a 0d 0a 48 65 6c 6c 6f 20 66 75 74 75 72 65 20 47 69 74 48 75 62 62 65 72 21 20 49 20 62 65 74 20 79 6f 75 27 72 65 20 68 65 72 65 20 74 6f 20 72 65 6d 6f 76 65 20 74 68 6f 73 65 20 6e 61 73 74 79 20 69 6e 6c 69 6e 65 20 73 74 79 6c 65 73 2c 0d 0a 44 52 59 20 75 70 20 74 68 65 73 65 20 74 65 6d 70 6c 61 74 65 73 20 61 6e 64 20 6d 61 6b 65 20 27 65 6d 20 6e 69 63 65 20 61 6e 64 20 72 65 2d 75 73 61 62 6c 65 2c 20 72 69 67 68 74 3f 0d 0a 0d 0a 50 6c 65 61 73 65 2c 20 64 6f 6e 27 74 2e 20 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 73 74 79 6c 65 67 75 69 64 65 2f 74 65 6d 70 6c 61 74 65 73 2f 32 2e 30 0d 0a 0d 0a 2d 2d 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 3c 68 65 61 64 3e 0d Data Ascii: <!DOCTYPE html>...Hello future GitHubber! I bet you're here to remove those nasty inline styles,DRY up these templates and make 'em nice and re-usable, right?Please, don't. <a 220="" 43="" 963="" 975"="" data-label="Page-Footer" href="https://github.com/styleguide/templates/2.0--><html> < head></td></tr> <tr> <td>2022-08-18 01:57:05 UTC</td><td>2</td><td>IN</td><td>Data Raw: 0d 0a
Data Ascii:</td></tr> <tr> <td>2022-08-18 01:57:05 UTC</td><td>2</td><td>IN</td><td>Data Raw: 31 35 36 38 0d 0a
Data Ascii: 1568</td></tr> <tr> <td>2022-08-18 01:57:05 UTC</td><td>2</td><td>IN</td><td>Data Raw: 6f 67 6f 20 7b 20 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 33 35 70 78 3b 20 7d 0d 0a 20 20 20 20 20 2e 6c 6f 67 6f 2d 69 6d 67 2d 32 78 20 7b 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 20 7d 0d 0a 20 20 20 20 20 20 40 6d 65 64 69 61 0d 0a 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 20 32 29 2c 0d 0a 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 20 20 20 6d 69 6e 2d 2 d 6d 6f 7a 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 20 32 29 2c 0d 0a 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 20 20 20 2d 6f 2d 6d
Data Ascii: ogo { display: inline-block; margin-top: 35px; } .logo-img-2x { display: none; } @media only screen and (-webkit-min-device-pixel-ratio: 2), only screen and (min--moz-device-pixel-ratio: 2), only screen and (-o-</td></tr> <tr> <td>2022-08-18 01:57:05 UTC</td><td>3</td><td>IN</td><td>Data Raw: 4f 46 52 76 45 35 46 75 4f 50 53 34 57 4c 53 74 37 2b 38 61 6a 76 58 63 4a 70 63 79 4e 76 68 7a 74 53 77 55 6b 54 47 67 5a 7a 39 75 44 53 78 52 6e 50 5a 77 73 6e 54 6b 71 79 37 6a 70 73 50 74 2f 41 78 79 76 6e 41 65 4a 4d 41 78 50 6e 4d 69 71 50 4a 59 49 79 7a 66 34 2f 4b 71 72 50 65 64 61 4b 35 62 49 73 51 77 66 54 6f 32 74 37 32 68 55 65 70 50 57 76 6e 36 6d 4f 38 56 6f 58 72 67 62 44 52 61 4a 58 6c 65 36 72 37 35 46 7a 5a 6d 37 53 32 54 6e 79 54 4e 55 5 8 76 35 65 69 44 41 41 36 6a 30 57 6d 4b 79 57 76 35 31 6c 69 52 41 41 43 6a 50 30 4f 5a 4e 56 75 77 61 34 4c 2b 75 51 41 63 77 2f 53 69 4e 47 48 35 37 6d 49 78 78 50 4b 6d 55 33 44 67 70 4c 32 73 58 33 72 75 74 63 33 2f 76 68 39 67 75 31 44 33 74 4e 45 41 74 76 4f 53 4b 56 41 6d 78 66 61 67 52 6d 62 6e
Data Ascii: OFRvE5FuOPS4WLSi7+8ajvXcJpcyNvhztSwUkTGgZz9uDsxRnRPNzwsnTkqy7jpsPt/AxyvnaeJMAxPnMiqPJYlyzf4/KqrPedaK5bIsQwfTo2t72hUepPWvn6mO8VoXrgbDRaJXle6r75FzZm7S2TnyTNUXv5eiDAA6j0WmKyWv51liRAACJP0OZNVuwa4L+uQAcwSiNGH57mlxxPKmU3DgpL2sX3rutc3/vh9gu1D3tNEAtvOSKvAmxfagRmbn</td></tr> <tr> <td>2022-08-18 01:57:05 UTC</td><td>4</td><td>IN</td><td>Data Raw: 72 36 57 31 6b 54 53 63 51 70 46 6a 50 78 4b 4f 77 44 67 41 49 55 7a 79 7a 51 4f 51 52 59 4d 79 64 6b 7a 49 37 59 5a 62 69 64 44 6b 63 54 6b 55 4b 51 57 61 7a 4f 65 69 74 58 46 39 68 42 77 35 53 5a 63 69 5a 4f 69 39 54 36 47 6e 6b 4d 70 30 75 4b 79 6d 51 6b 44 48 48 41 78 7a 4d 4c 77 63 53 4d 2b 65 5a 4a 71 57 68 73 6b 68 4f 4d 69 76 44 44 73 63 49 43 35 6f 68 79 57 2b 78 31 6c 54 6d 35 36 2b 76 32 44 6b 47 47 6c 7a 39 46 53 45 6e 79 6e 52 64 67 50 4b 55 6 c 65 7a 54 43 53 54 65 34 7a 47 6e 5a 66 73 56 74 6d 57 54 33 34 6b 6c 6a 41 6d 4a 67 41 62 42 53 45 75 59 79 51 49 6a 4c 6e 67 6e 6b 4c 42 55 67 6b 4a 46 59 36 50 64 62 67 63 4b 61 45 78 54 66 7a 3a 38 46 6e 78 61 61 6e 78 38 66 47 70 36 68 6c 59 31 66 76 63 55 37 70 38 53 53 45 59 32 38 38 4e 41 6e 50
Data Ascii: r6W1kTScQpFjPxKOWdgAlUyzzyQQQRYMydkzl7YZbidDkcTkUKQWazOeitXFhBw5SZciZOi9T6GnkMp0uKymQkDHHAXzMLwcSM+eZJqWhskhOMivDDscIC5ohyW+x1ITm56+v2dKGGLz9FSEnynRdgPKUleZTCSTe4zGnZfsVtmWT34kljAmJgAbSEuYyQlJLngnKLBUgkJFY6PdbgcKaExTfz48Fnxaxn8fGp6hY1fvcU7p8SSEY288NAnP</td></tr> <tr> <td>2022-08-18 01:57:05 UTC</td><td>6</td><td>IN</td><td>Data Raw: 4d 32 65 2b 37 31 46 64 32 4b 66 48 4a 42 34 32 73 76 46 77 7a 70 4b 67 41 7a 45 4e 56 6e 59 52 37 2f 64 62 68 7a 49 79 66 4e 64 61 7a 43 4b 42 30 52 70 37 38 35 4a 41 34 71 39 73 57 4c 39 2b 73 70 4b 69 35 65 68 66 76 52 62 30 63 46 76 72 4b 30 4a 34 75 2b 64 33 70 6d 56 47 52 6c 77 31 73 47 38 70 74 37 61 6b 75 70 67 30 4b 6b 45 5a 73 5a 2f 66 39 45 64 65 61 38 42 68 43 51 79 33 37 69 41 70 43 69 43 52 2f 33 4b 4d 56 31 49 5a 79 64 32 56 2b 73 6c 79 59 6e 34 45 61 30 48 56 35 4d 69 4e 77 61 7a 52 6c 67 53 55 6d 58 42 41 79 34 72 66 56 71 42 34 4c 2b 76 53 49 36 53 38 71 34 43 32 2f 77 61 68 42 4b 2f 4a 79 48 39 2b 2f 4a 62 77 6a 6d 68 55 68 63 34 68 4d 39 4b 54 6b 65 45 64 5a 6f 35 6a 36 70 6a 34 77 77 6b 33 34 71 4b 4a 42 70 48 52 61 55 5a 67 7a 2f 34
Data Ascii: M2e+71Fd2KfHJB42svFwzpKgAzENVnYR7/dbhzlyfNdazCKB0Rp785JA4q9sWL9+spKi5ehfvRb0cFvrK0J4u+d3pmVGRlw1sG8pt7akupg0KkEZsZ/f9Edea8BhCQy37iApCiCR/3KMV1Izdy2V+slyYn4Ea0HV5MinwazRlgSUMXBAY4rfVqB4L+vSI6S8q4C2/wahBK/JyH9+/JbwjmHUh4hM9KTkeEdZo5j6pj4wwwk34qKJBpHRaUZgz/4</td></tr> <tr> <td>2022-08-18 01:57:05 UTC</td><td>7</td><td>IN</td><td>Data Raw: 0d 0a
Data Ascii:</td></tr> <tr> <td>2022-08-18 01:57:05 UTC</td><td>7</td><td>IN</td><td>Data Raw: 31 30 30 65 0d 0a
Data Ascii: 100e</td></tr> </table> </div> <div data-bbox="> Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:05 UTC	7	IN	Data Raw: 50 36 30 55 2b 49 53 4f 45 67 41 65 41 31 49 38 68 71 75 73 68 76 54 4f 48 45 69 31 59 53 54 67 51 37 37 50 5a 49 34 71 4d 74 58 4f 31 4d 33 2f 36 31 4b 6c 69 4f 30 58 31 69 37 43 55 53 4c 56 6a 4b 32 73 76 61 34 38 51 6f 6a 72 45 6a 57 57 78 49 79 67 37 51 54 67 49 53 51 7a 74 52 6f 76 56 34 6e 43 49 4a 79 54 4a 6a 54 45 4a 4c 4a 39 49 69 62 4e 54 35 32 71 72 6a 4a 50 69 34 49 74 71 6f 66 51 6e 44 4f 73 7a 78 73 38 62 79 43 77 49 63 52 78 35 4a 62 61 53 49 67 6d 47 34 6d 46 50 59 69 53 30 42 6b 56 57 50 48 6e 72 42 4f 75 46 5a 42 36 45 70 4c 37 66 41 44 4b 57 63 78 49 68 76 61 6f 76 49 6f 61 41 78 38 48 44 41 38 4d 49 4a 42 61 52 62 42 57 66 4c 72 61 54 6e 54 52 65 31 48 53 63 66 78 6c 51 65 46 44 68 41 49 37 72 51 49 35 7a 38 77 41 4f 70 43 39 4f 48 48 Data Ascii: P6OU+ISOEGAeA1I8hqshvTOHE1YSTgQ77PZI4qMxO1M3/61KliOOX1i7CUSLVjK2sva48QojrEjWWxlyg7QTgISQztRovV4nClJyTJTJTEJLJ9libNT52qrjJPi4ltqofQnDOszsx8byCwlcRx5JbaSlgmG4mFPYiS0BkVWPHnrBOuFZB6EpL7fADKWcxIhvaovloaAx8HDA8MIJBaRbBWfLraTnTre1HScfxlQeFDhAI7rQI5z8wAOpC9OHH
2022-08-18 01:57:05 UTC	8	IN	Data Raw: 6b 57 49 44 71 52 71 50 42 42 69 45 64 48 4b 71 71 41 79 5a 50 6a 36 50 67 41 42 6b 66 64 61 52 74 79 63 53 48 38 78 67 41 43 4a 66 59 77 77 52 44 44 52 6f 5a 51 74 7a 6e 2f 2b 2b 66 7a 46 69 38 76 4b 68 4b 6c 4d 4a 49 31 4c 4e 4a 7a 49 4b 46 39 74 6c 55 45 46 55 76 66 4f 6d 71 4c 56 71 31 63 45 46 66 37 66 6a 42 30 51 45 30 39 53 6d 55 71 6b 70 41 42 49 43 6e 6f 4c 43 67 70 4f 35 51 55 56 4a 4d 53 4b 39 46 31 62 77 43 61 6b 74 58 35 47 6b 73 69 57 6f 36 74 30 33 55 41 67 57 6f 78 61 71 77 4b 5a 64 48 4b 58 67 4e 77 6e 6a 64 37 2b 53 38 38 77 49 79 49 71 6b 47 4a 78 58 31 78 73 38 43 69 47 78 6e 73 77 50 42 7a 76 76 6a 51 71 5a 57 55 62 4e 6d 79 6f 34 39 71 77 51 57 65 69 50 37 73 42 31 51 6e 48 45 6b 45 46 57 4b 70 72 6f 4f 6f 69 6e 6a 61 76 50 6a 49 69 Data Ascii: kWIDqRqPBBiEdHKqQayZPJ6PgABkfaRtycSH8xgACJfYwwRDDRozQtzn/++fzFi8vKhKIMJ11LNJzIKF9tIUeFUvOmqlVq1cEFf7fjB0QE09SmUqkpABICnoLCgpoO5QUVJMSK9F1bwCaktX5GksiWo6i03UAgWoxaqwKZdHXKgNwnjd7+S88wlylqkGJxX1xs8CiGxnsWPBzvjqQzWUbNmyo49qwQWeip7sB1QnHEKEFWKproOoinjavPjli
2022-08-18 01:57:05 UTC	10	IN	Data Raw: 34 45 6e 76 44 4e 6c 5a 59 2f 55 45 4a 35 6b 48 79 70 45 34 52 45 4a 4e 36 7a 4a 69 4d 4e 63 51 6d 57 45 68 70 71 59 31 37 4c 54 4b 53 32 68 4a 6b 58 57 36 6d 31 69 51 50 50 34 6b 51 59 58 64 64 35 7a 6f 4d 4d 64 50 46 6a 55 30 36 44 7a 63 34 47 54 7a 77 43 45 43 71 39 6e 63 65 32 2b 51 50 76 55 68 41 71 71 4c 57 78 47 75 6b 62 47 2f 62 47 30 4d 75 5a 67 42 42 71 72 57 48 71 68 45 35 5a 4f 30 41 6b 54 45 65 53 4d 4b 67 52 46 4d 68 48 6c 39 2f 66 61 59 77 5 6 2f 56 64 47 38 72 47 5a 32 41 61 69 2f 4f 71 43 6e 4e 7a 38 52 52 38 46 73 53 66 46 55 59 42 72 56 68 52 59 33 55 6f 45 74 58 73 58 73 62 46 57 2b 2b 78 42 6d 4a 30 47 70 4d 43 50 50 75 31 67 49 6a 4e 56 74 72 56 61 30 4e 63 4a 2b 46 52 45 58 50 7a 77 6a 32 42 4c 67 62 33 51 43 44 70 66 43 34 52 68 33 Data Ascii: 4EnvDNIZY/UEJ5kHypE4REJN6zJiMNCmWEhpqY17LTKS2hJkXW6m1iQPP4kQYXdd5zoMMdPFjU06Dzc4GtzwCECq9nce2+QPvUhAqqlWxGukbG/bG0MuZgBBqrWHqhE5ZO0AKTEeSMKgRFMhH9/fayYwV/VdG8rGZ2Aai/OqCnNz8RR8FsSFUYBrVhRY3UoEtXsXsbFW++xBmJ0GpMCPpu1gljNVtrVa0NcJ+FREXPzwj2BLgb3QCDpfC4Rh3
2022-08-18 01:57:05 UTC	11	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	11	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	11	IN	Data Raw: 2b 7a 45 6e 77 41 6b 6a 4d 69 62 71 4e 66 64 53 6d 68 52 62 79 53 4f 4b 46 76 52 65 65 51 69 62 38 72 6c 74 6c 4a 34 37 73 77 35 33 4d 36 63 51 6c 41 42 44 55 45 48 4f 41 51 52 76 6e 63 45 67 59 4e 5a 46 78 49 70 4e 63 42 54 76 69 56 4c 46 46 57 45 6e 66 69 54 71 46 43 65 63 69 41 30 69 35 64 41 2f 56 70 71 62 45 46 4d 64 73 41 36 6c 4f 70 6d 68 48 68 61 62 2b 66 74 52 6a 4c 58 6d 61 6b 45 59 49 4b 2b 43 57 5a 4b 43 41 68 61 68 6c 35 6d 32 59 53 69 52 46 62 49 68 34 48 49 68 46 42 65 67 73 63 53 51 49 36 74 6a 47 79 63 55 4a 4a 31 72 2b 32 6a 55 4d 2b 62 45 55 42 75 48 45 4c 53 51 2b 56 36 37 78 58 61 4a 70 54 4f 35 49 72 67 51 53 57 47 65 48 53 4f 61 73 52 7a 68 58 69 45 38 6a 31 61 51 49 42 5a 4b 49 6e 56 4c 4d 52 6a 56 57 68 68 71 56 51 63 59 43 4c 4d Data Ascii: +zEnwAkjMibqNfdSmhRbySOKFvReeQib8ritJ47sw53M6cQIABDUeHOAQrVncEgYNZFxlPnCBTviV LFFWEnfITqFCeciaAOi5dA/VpqbEFMdsA6lOpmhHhab+ftRjLXmakEYIK+CWZKCAhahI5m2YsIRfBlh4HIhFBegscSQ I6tjGycUJJ1r+2jUM+bEUBuHELSQ+V67xXaJpTO5IrgQSWGeHSOasRzhXiE8j1aQIBZKInVLMRjVWhhgVQcYCLM
2022-08-18 01:57:05 UTC	12	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	12	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	12	IN	Data Raw: 77 6c 4e 35 46 48 45 45 75 65 4f 43 52 49 53 44 5a 41 43 61 52 57 42 59 75 4e 4d 79 6c 62 69 6c 34 6b 46 5a 64 45 4e 6f 42 4b 50 42 66 45 44 63 53 6a 4a 30 51 6b 54 69 38 48 36 63 59 69 4e 48 39 42 5a 47 4e 52 49 52 63 56 6f 6d 74 74 37 79 38 76 4c 65 32 61 61 4f 58 65 5a 30 53 68 6f 31 68 73 33 77 47 51 6a 74 72 6b 62 33 59 79 73 57 54 58 76 46 64 6e 32 43 69 63 64 6d 45 4a 4e 6a 51 70 69 33 69 6e 6f 44 38 54 33 31 6b 4a 77 74 6c 43 49 69 38 32 53 4d 50 30 35 4a 68 64 46 67 66 52 73 74 58 4a 7a 41 35 46 58 54 66 6f 53 76 51 57 66 54 68 44 57 32 34 58 4b 68 37 73 49 6b 45 47 31 6b 71 73 72 41 64 46 77 79 74 65 58 6e 35 65 63 45 45 4f 77 79 65 45 4a 46 6b 49 6a 4b 6c 51 49 7a 30 56 33 49 47 48 55 53 6b 71 62 62 38 44 70 71 2f 61 50 32 69 39 32 75 56 6e 4c Data Ascii: wIN5FHEEueOCRI5DZACaRWBYuNMyIbi4kFZdENoBKPBFEdcSjJ0kqTi8H6cYiNH9BZGNRIRcVomtt 7y8vLe2aaOXeZ0Sho1hs3wGQjtrkb3YysWTXvFdn2CicdmEJNjQpi3inoD8T31kJwtlCii82SMP05JhdFgfRstXJzA 5FXTfoSvQWfThDW24XKh7slkEG1kqsrAdFwyteXn5ecEEOWyeEJfJkIjKlQz0V3IGHUskqbb8Ddpq/aP2i92uVnL
2022-08-18 01:57:05 UTC	14	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	14	IN	Data Raw: 61 62 34 0d 0a Data Ascii: ab4
2022-08-18 01:57:05 UTC	14	IN	Data Raw: 5a 33 49 65 6b 6d 52 64 61 45 4c 72 53 77 42 68 43 2b 49 52 45 58 31 4c 7a 2f 4b 51 76 4c 67 6b 72 4d 48 65 6b 34 4d 6a 64 65 4a 48 67 7a 58 44 52 34 34 34 48 4b 48 59 43 75 75 6d 75 65 58 61 30 41 45 6b 72 4f 4c 2b 50 31 44 6f 43 77 6c 4b 67 54 69 36 70 4b 6c 32 45 63 51 4d 54 4c 68 6c 35 66 58 72 61 43 35 4f 66 68 32 61 6a 56 4f 4f 52 44 52 6a 39 66 4f 44 56 58 4c 64 6c 74 70 65 55 6b 4a 70 6f 53 34 79 6c 64 54 6f 38 33 4e 33 2f 6d 49 49 77 33 72 6b 50 4a 71 38 51 51 33 32 6e 52 54 51 58 54 78 67 70 36 52 45 70 38 63 79 7a 6c 32 30 6f 36 49 48 67 31 45 62 67 47 51 74 74 75 76 39 77 7a 53 53 57 33 52 77 72 43 44 34 73 33 65 4e 54 42 34 63 4d 39 62 62 37 7a 39 39 68 2b 46 33 6e 37 37 6a 62 66 32 48 42 78 75 41 5a 63 42 47 63 61 69 45 42 54 48 38 34 67 71 Data Ascii: Z3lekmRdaELrSwBhC+IREX1Lz/KQvLgkrMHek4MjdeJHgzXDR444HKHYCuumueXa0AEkrOL+P1DoCw lKgTi6pKl2EcQMTLhI5fXraC5Ofh2ajVOORDRj9fODVXLdltpEukJpoS4yldTo83N3/mlIw3rkPJq8QQ32nRTQXTxg p6REp8cyl20o6IHg1EBgGQtuv9wzSSW3RwrCD4s3eNTB4cM9bb7z99h+F3n77jbf2HBXuAZcBGcaieBTH84gq

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:05 UTC	15	IN	Data Raw: 30 43 62 63 55 65 72 6a 6b 77 68 4a 51 57 58 70 31 61 65 45 6c 4d 68 42 44 4f 39 54 37 64 37 61 35 66 41 4f 51 32 47 55 50 48 39 37 32 2f 6e 61 4e 43 70 43 38 66 7a 69 72 5a 53 44 4c 48 32 43 7a 34 74 4c 69 55 31 50 78 6b 52 69 4a 45 67 33 55 78 52 69 49 55 5a 41 6f 33 71 42 6f 6f 39 44 49 46 75 53 6f 33 74 68 55 4c 76 37 50 4d 4a 49 6d 75 43 31 42 78 4d 32 4e 70 4d 47 41 67 6a 32 71 77 75 46 2f 2f 77 57 41 6f 42 71 42 45 63 46 43 36 6e 4d 36 73 62 50 54 70 42 7a 4a 48 67 48 6b 4e 66 78 65 57 41 5a 6d 54 41 61 76 49 34 70 45 74 58 74 64 6a 48 30 51 65 66 43 78 54 63 72 6b 67 37 63 50 44 76 57 34 58 46 37 30 67 73 79 53 35 72 6e 43 6f 56 78 64 78 76 64 58 7a 77 4c 4b 65 4b 31 61 4a 59 78 6b 6d 32 38 67 32 34 63 45 71 49 64 43 7a 30 4c 4c 73 79 31 39 31 Data Ascii: 0CbCUErjkwhJQWXp1aeEIMhBDO9T7d7a5fAOQ2GUPH972/naNCpC8fzirZSDLH2Cz4tLiU1PxkRiJEg3UxRilUZAo3qB0o9DIFuSo3thULv7PMJImuC1BxM2NpMGAgj2qwuF//wWAoBqBEcFC6nM6sbPTpBzJHgHkNfxeWAZmTAavi4pEtXtdjH0QefCxTcrkg7cPDvW4XF70gsyS5rnCoVxdxvdXzwLKeK1aJYxkm28g242cEqldCz0LLsy191
2022-08-18 01:57:05 UTC	16	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	16	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	16	IN	Data Raw: 6a 45 42 59 68 51 6b 34 6c 54 45 5a 6c 44 68 35 31 43 58 64 72 54 54 79 57 38 46 37 58 6c 4d 42 71 77 53 55 53 51 61 52 67 4c 52 55 6d 48 57 38 41 73 41 38 70 4f 54 4d 42 5a 38 50 6e 46 4f 54 69 73 4d 78 31 37 66 59 45 78 6b 37 59 62 76 45 6a 7a 6f 73 6a 4f 4b 6d 79 62 6c 45 4e 57 35 51 37 72 78 7a 61 47 2f 37 42 74 75 32 66 76 6d 6f 66 74 63 68 39 37 37 46 47 67 65 4b 46 41 42 6c 50 75 33 43 55 6f 30 6b 72 65 48 59 53 56 65 2b 46 63 7a 65 31 37 77 57 50 4c 74 55 72 72 37 39 6c 65 41 49 67 7a 6b 48 4c 39 62 52 6e 6a 67 73 51 59 55 6b 69 61 47 59 64 50 36 63 74 49 78 59 65 50 7a 77 7a 35 31 63 75 65 49 61 42 67 6a 34 66 30 61 67 59 35 6d 78 67 42 4d 59 6b 42 49 58 37 69 6d 32 59 69 54 54 6a 54 71 70 63 75 6b 31 4b 4e 4e 46 75 53 7a 38 79 2b 69 6e 35 4b 6e Data Ascii: jEBYhQk4ITEZIDh51CXdrTTYW8F7XIMBqwSUSQaRgLrUmHW8AsA8pOTMBZ8PnFOTisMx17fYExk7Yyb vEjzsjOKMyblENW5Q7rxzaG/7Btu2fvmofth977FGgeKFAbIPu3CUo0kreHYSVe+Fcze17wWPLtUrr79leAlgzkHL9bRnjgsQYU9kiaGYdP6ctixYePzwz51cuelaBgj4f0agY5mxgBMKYBIX7im2YITtJTqpcuk1KNFuSz8y+in5Kn
2022-08-18 01:57:05 UTC	18	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	18	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	18	IN	Data Raw: 62 61 52 69 47 4d 71 4b 77 5a 77 64 61 66 4d 4f 38 76 58 55 56 72 73 34 51 75 76 52 58 66 77 78 52 46 2f 49 77 45 55 6d 4f 47 5a 41 30 47 41 69 74 6a 64 4e 53 4f 79 69 51 6d 71 50 4c 39 74 4a 71 48 51 68 53 72 50 2f 37 33 33 2f 2b 6a 45 4c 49 30 63 33 4d 67 52 4a 2b 4e 31 43 63 62 41 41 4b 2b 2f 2f 38 39 61 39 47 46 36 73 79 36 4b 43 33 47 44 55 54 52 31 47 67 44 79 6b 48 68 76 5a 38 65 52 75 42 49 37 5a 4d 34 4c 71 36 78 69 46 70 65 39 73 33 35 4b 4b 7a 35 45 51 47 4c 49 43 63 58 63 72 76 75 76 56 74 32 38 6a 56 56 33 75 38 49 36 47 34 65 4c 72 51 64 65 62 63 6a 50 54 34 32 51 6e 50 55 45 37 46 57 5a 42 68 5a 4b 4e 39 77 67 35 76 34 79 77 45 44 41 50 48 41 52 2f 2f 37 44 39 65 2b 4d 58 76 66 6e 4e 67 32 48 58 34 2f 65 32 48 73 39 30 53 6e 56 6b 64 41 79 Data Ascii: baRiGMqKwZwdaFM08vXUVrs4QuvRXfwwRF/lwEUmOGZA0GAitjdNSOyiQmqPL9tJqHQhSrP/733/+j ELI0c3MgRJ+N1CcBAAK+//89a9GF6sy6KC3GDUTR1GgDykHhvZ8eRuBi7ZM4Lq6xiFpe9s35KKz5EQGLICcXcrruvV t28jVV3u8l6G4eLrQdebciPT42QnPUE7FWZBhZKN9wg5v4ywEDAPH1R//7D9e+MXvfnNg2HX4/e2Hs90SnVkdAy
2022-08-18 01:57:05 UTC	19	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	19	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	19	IN	Data Raw: 6f 37 61 65 33 72 69 54 7a 4f 4b 68 4c 75 53 4d 36 67 35 65 68 4b 32 72 34 6a 49 6a 39 6f 4c 6b 75 52 4e 66 71 52 2f 7a 44 35 74 7a 5a 71 6c 6c 4e 2f 75 32 6b 56 49 6f 42 36 6c 57 33 50 67 50 77 36 43 68 79 36 50 58 73 43 64 7a 42 76 6e 70 74 2f 5a 42 43 41 6d 69 49 69 37 43 47 33 76 41 77 69 51 6f 43 72 69 6f 52 54 78 38 72 2b 79 6e 74 56 76 66 76 50 68 50 36 48 56 76 67 55 7a 38 68 2f 2b 2b 55 4e 6d 73 68 52 55 65 63 47 44 57 61 7a 62 74 2b 48 54 4f 52 41 79 57 75 54 52 6b 59 33 38 4d 77 64 43 4a 5a 4f 51 34 6d 30 58 76 55 46 52 4a 52 6c 6c 56 64 35 4d 49 74 46 63 79 52 6 5 4e 45 7a 35 4a 64 64 62 2b 35 54 74 38 37 50 68 6a 77 4b 4a 48 58 75 49 74 78 49 67 45 4a 48 61 56 30 56 65 6f 52 75 6d 42 73 68 73 33 44 6a 63 49 48 6e 54 4d 43 55 52 2b 2b 66 6f 4c Data Ascii: o7ae3riTzOKhLuSM6g5ehK2r4jij9oLkuRNfqr/zD5tzZqllN/u2kVioB6lW3PgPw6Chy6PXsCdzBvnpt/ZBCAmi li7CG3vAwiQoCrioRtX8r+yntVvfvPhP6HvvgUz8h/+UNmshRUecGDWazbt+HTORAYWuTRky38MwdCJZO4m0XvUF RJRIIVd5MltFcyrReNEz5Jddb+5Ti87PhjwKJHXultxlGEJHaV0VeoRumBshs3DjclHmTMCUR++foL
2022-08-18 01:57:05 UTC	20	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	20	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	20	IN	Data Raw: 75 30 77 72 42 6e 77 58 39 50 73 58 5a 2b 78 64 47 49 79 55 57 50 66 35 61 6a 43 57 6e 71 71 74 2f 31 36 2b 33 6e 72 7a 52 66 4f 50 47 31 71 30 33 49 4c 6e 46 70 43 43 4c 4c 74 77 6b 4a 42 76 70 49 34 30 56 41 59 47 42 57 6b 64 42 4c 6a 72 7a 72 39 4c 36 4e 4e 36 62 34 68 72 79 75 34 63 61 43 56 31 48 6b 4a 42 34 32 49 6b 46 4a 43 44 4d 59 4f 32 42 76 53 4c 5a 2b 79 75 6d 49 4f 55 49 6b 36 45 69 43 4c 4e 43 6c 46 59 6d 4b 34 68 55 54 79 58 46 4e 52 63 45 58 4c 42 62 33 47 78 64 36 5a 37 6f 44 45 62 6e 6b 4a 46 6f 50 4a 61 30 58 34 4c 49 6a 34 64 32 56 62 56 57 35 52 74 43 32 63 4c 7a 75 50 57 2f 36 61 48 63 55 79 67 62 4e 6d 48 7a 53 64 41 33 56 67 78 6b 34 7a 73 41 6f 6b 52 56 7a 2f 51 4c 6f 45 6c 71 73 70 45 42 51 53 34 42 42 59 46 77 4c 50 68 4b 52 42 Data Ascii: uOwrBnwX9PsXZ+xdGlyUWPF5ajCWnqqt/16+3nrzRfOPG1q03lLnFpCCLLtwkJBvlp1t0VAYGBWkdBL jrzt9L6NN6b4hryu4caCV1HkJB42kfJCDMYO2BvSLZ+yumiOUIk6EiCLNCIFymK4hUTyXFNRcEXLBb3Gxd6Z7oDEb nkJFoPJa0X4Lj4d2VbVW5RyC2cLzuPW/6aHcUYgbNmHzSdA3Vgxk4zsAokRVz/QLoElqspEBQS4BBYFwLPhKRB
2022-08-18 01:57:05 UTC	22	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	22	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	22	IN	Data Raw: 48 2f 39 44 70 39 39 61 73 45 2f 32 58 37 33 2b 2b 31 6b 72 6b 72 42 41 31 45 76 65 4a 7a 6b 50 49 51 48 4d 51 2b 45 4c 5a 36 52 41 4b 53 47 56 4f 51 65 49 62 6c 73 73 39 70 6f 61 42 46 63 56 4a 78 75 33 48 66 76 36 6a 33 49 51 2f 7a 42 69 32 73 49 54 68 35 30 41 6b 68 4e 44 51 48 35 59 47 64 2f 44 56 6b 73 50 59 6e 63 4e 6b 7a 76 68 65 79 4f 73 50 75 48 6e 31 65 4a 77 37 65 44 69 44 55 71 52 57 7a 52 48 64 73 50 48 44 43 79 59 41 72 79 33 67 38 2f 4d 42 7 7 35 65 41 77 4c 41 4b 57 2f 42 76 37 38 42 75 4d 68 63 68 43 54 51 43 42 59 6a 73 79 47 33 4a 42 38 6c 6c 79 39 78 51 52 4b 38 64 47 44 68 42 56 69 55 7a 39 36 2f 2b 45 52 43 48 54 6b 31 72 5a 62 75 6f 62 73 73 39 4a 5a 71 5a 50 41 51 45 69 32 66 56 42 47 51 45 71 75 36 6f 6e 39 31 53 4f 44 4a 55 52 45 Data Ascii: H/9Dp99asE/2X73++1krkrBA1EveJzkPIQHMQ+ELZ6RAKSGVOqelbss9poaBFcVJxu3Hfv6j3IQ/zBi2siTh50A khNDQH5YGd/DVksPYncNkzvheyOsPuHn1eJw7eDiDUqRWzRHdsPHDCyYArY3g8/MBw5eAwLAKW/Bv78B uMhchCTQCBYsjG3JB8lly9xQRK8dGDhBViuZ96/+ERCHTK1rZbuobss9JzQZPAQEi2fVBGQEqu6on91SODJURE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:05 UTC	23	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	23	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	23	IN	Data Raw: 7a 79 61 32 72 75 6b 42 62 4c 71 76 52 78 66 73 55 6e 32 38 32 63 4f 31 6e 51 45 52 79 35 6f 4e 49 4b 77 6e 37 55 4b 41 57 57 78 6f 61 47 67 71 64 30 59 67 73 42 30 4f 71 45 46 70 34 41 68 36 62 51 59 50 6d 47 74 61 72 38 41 42 76 6d 51 4b 79 44 6b 43 30 38 78 30 56 41 78 42 38 61 62 34 50 4a 41 75 44 4b 2f 32 4e 69 49 6a 33 4a 58 79 6f 5a 63 47 6d 63 6d 46 41 38 49 4b 74 75 31 74 78 48 2f 79 59 6c 4a 63 31 35 78 57 53 42 77 6b 4c 48 4c 48 5a 70 38 2b 31 32 50 75 47 4f 75 70 39 71 6c 53 63 4f 7a 42 41 4f 73 4a 34 63 50 30 34 58 47 54 46 4b 4a 65 61 4a 4e 4e 7a 36 2f 52 56 47 6d 7a 79 4a 34 47 4d 78 49 51 50 34 54 4d 2f 58 45 55 61 79 77 59 67 5a 52 55 56 77 36 33 4e 67 33 41 57 51 4c 43 45 49 44 57 35 72 4b 4c 61 30 6b 58 43 6c 4b 53 6d 6c 56 41 78 68 77 Data Ascii: zya2rukBbLqvRxfUn282cO1nQERY5oNIKwn7UKAWWxoaGgqd0YgsB0OqEFp4Ah6bQYPmGtar8ABvm QKyDkC08x0VAXb8ab4PJAUdK/2Nijj3JXyoZcGmcmFA8IKtu1txH/yYIJc15xWSBwkLHLHZp8+12PuGOup9qIScOzBAOsJ4cP04XGTFKJeaJNNz6/RVGmzyJ4GMxIQP4TM/XEUaywYgZRUVw63Ng3AWQLCEIDW5rKLaoKXCiKSmlVAxhw
2022-08-18 01:57:05 UTC	24	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	24	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	24	IN	Data Raw: 48 4e 41 2b 47 79 76 30 4a 48 42 2b 31 79 67 4b 58 44 75 37 4b 6d 2f 43 76 6d 41 35 46 65 2f 2b 74 56 2f 2f 65 66 2b 6e 64 79 2f 48 57 35 41 74 61 56 43 52 37 4a 2f 4a 37 6b 57 48 67 53 54 62 57 73 75 67 31 64 69 6e 58 53 34 6a 78 4e 52 33 41 67 64 57 38 67 44 4f 4c 36 65 6e 4a 71 61 76 46 44 72 74 79 69 4b 5a 48 50 30 48 75 38 5a 6e 63 56 68 36 62 57 50 73 30 68 69 31 38 39 37 46 52 5a 35 61 6b 51 47 76 79 6e 59 76 6e 33 58 72 6c 30 46 67 2f 68 59 68 41 77 73 6c 43 37 4d 4c 30 36 76 4d 77 56 45 56 45 2b 45 48 38 6b 76 76 62 39 41 42 69 72 67 31 42 48 42 51 72 5a 74 4f 37 49 66 42 6d 78 34 2f 73 48 49 50 39 7a 46 48 55 6f 46 53 41 79 51 33 68 41 4d 7a 64 4d 33 46 78 32 55 32 58 34 41 37 43 55 37 35 63 4b 6d 73 6a 36 38 45 2f 6c 68 37 50 72 6b 31 4d 79 54 Data Ascii: HNA+Gyv0JHB+1ygKXD7Km/CvmA5Fe+tv//ef+ndy/HW5AtaVCR7J/J7kWHgStBWsug1dinXS4jxN R3AgdW8gDOL6enJqavFDrtyiKZHP0Hu8ZncVh6bWPs0hi1897FRZ5akQGvynYvn3Xrl0Fg/hYhAwsIC7ML06vMwVEV E+EH8kvvb9ABirg1BHBQRZtO7IfBmx4/sHIP9zFHUoFSaYQ3hAMzdM3Fx2U2X47CU75cKmsj68E/lh7Prk1MyT
2022-08-18 01:57:05 UTC	26	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	26	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	26	IN	Data Raw: 67 43 43 72 7a 50 49 4c 61 2b 72 6a 4e 71 37 39 50 6e 5a 72 41 6d 35 63 68 6f 6f 61 43 73 71 77 36 55 55 64 7a 2b 76 4a 7a 38 2f 49 4f 35 2b 54 6b 6c 4a 4b 6b 55 68 57 64 43 44 64 59 4b 50 50 53 52 59 53 53 38 78 79 64 69 52 46 37 52 2b 38 41 43 42 54 6b 4e 43 6d 49 56 6c 67 68 47 46 54 73 76 58 37 64 37 67 36 50 7a 6d 4b 39 74 58 75 46 67 5a 61 39 32 77 48 48 44 6d 33 72 37 72 57 50 70 70 48 49 31 7a 4e 31 50 6d 73 45 64 58 43 70 67 4f 46 49 6a 53 57 76 51 56 48 45 4e 4f 6b 71 67 61 41 7a 52 61 30 75 63 62 6b 43 31 76 71 39 51 33 37 45 4b 4a 47 67 6a 4b 35 2b 31 46 6b 4d 4c 68 43 56 72 4a 6a 52 66 41 6b 6f 70 54 68 77 68 35 31 59 39 68 6a 64 34 63 6e 76 6b 4d 49 31 4f 76 4d 52 46 6c 4f 51 75 6c 35 72 4a 4d 67 4f 67 63 59 42 77 34 34 53 49 2b 4c 67 4a 32 Data Ascii: gCCrZPILa+rjNq79PnZrAm5chooaCsqw6Uudz+vJz8/IO5+TkIJkKUhWdCDdYKPPSRYS8xydiRF7R +8ACBTkNcmlVlghGFTsvX7d7g6PzmK9tXuFgZa92wHHDm3r7rWPPpH1zN1PmsEdXCpgOFIjSWvQVHEN OkqgaAzRa0ucbkC1vq9Q37EKJGgjK5+1FkMLhCVrJjRfAkopThwh51Y9hjd4cnvkMI10vMRFIOQul5rJMgDgcYBw44 SI+LgJ2
2022-08-18 01:57:05 UTC	27	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	27	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	27	IN	Data Raw: 59 72 49 4e 6d 66 78 51 51 67 6d 53 68 56 4a 56 6c 54 44 75 50 57 71 67 55 43 35 58 73 65 64 50 42 43 36 33 69 68 59 6a 4a 68 4f 57 45 66 68 74 66 67 72 53 62 35 5a 6b 73 72 67 44 78 32 46 6b 75 52 76 76 41 59 65 6b 49 36 4a 4a 6b 31 42 34 4e 4e 46 76 51 34 32 36 6b 49 45 46 69 76 6f 50 7a 38 35 4d 7a 62 31 75 64 38 33 38 63 6e 48 44 6a 39 71 57 6a 33 32 6d 4a 6b 4f 33 39 68 70 53 2f 32 70 69 34 35 45 59 39 6f 50 6f 30 77 2b 71 5a 4e 73 6c 47 71 51 54 34 58 49 73 68 4a 53 46 77 6c 72 33 4a 6f 41 77 75 75 37 72 36 37 6e 65 63 68 36 32 64 4f 51 57 30 43 32 45 61 39 6b 4a 6a 71 59 35 61 6e 63 4c 65 67 6f 39 6b 6d 4f 4e 6f 78 65 73 53 35 46 35 77 52 54 6b 45 56 42 6c 76 32 4a 62 72 45 51 39 46 34 59 48 36 74 72 38 58 64 4f 66 50 4a 54 6b 39 4e 31 61 6a 5a 77 Data Ascii: YrlNmfxQQgmShVJVITDuPWqgUC5XsedPBC63ihYJhOWEftfgrSb5ZksrgDx2FkuRvwAYekl6JJk1 B4NNFvQ426klEFivoPz85Mzb1ud838cnHDj9qWj32mJkO39hpS/2pi45EY9oPoW+qZNsIGqQT4XlshJSFwlr3JoAw uu7r67nech62dOQW0C2Ea9kJjqY5ancLego9kmOnoxesS5F5wRTkEVB1v2JbrEQ9F4YH6trXDOFJTK9N1ajZw
2022-08-18 01:57:05 UTC	28	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	28	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	28	IN	Data Raw: 52 51 44 77 4e 47 2f 2f 2b 49 2b 49 6d 62 63 6f 4c 35 77 73 6e 34 31 71 30 34 6d 4d 42 4c 31 75 76 56 39 39 4a 78 36 7a 51 57 7a 4b 6e 49 51 42 43 44 33 46 45 79 73 79 69 6d 2f 41 34 6a 2b 4c 6f 56 43 63 2b 4e 6b 34 6a 2f 55 43 34 32 76 33 69 4a 56 31 4a 68 41 52 5a 49 36 54 59 6c 34 74 4b 59 30 47 42 7a 67 58 76 63 6e 62 6b 35 54 5a 47 44 7a 5a 4d 2b 42 73 72 32 39 32 70 70 33 4c 4a 73 78 79 47 79 41 74 35 5a 45 71 46 4c 4d 5a 65 63 70 33 52 4c 2b 72 43 53 66 33 36 45 7a 54 42 56 64 38 52 4d 39 65 34 59 4a 32 76 6f 45 6f 61 6b 68 6b 56 6f 55 59 6e 56 55 70 34 35 53 70 54 51 45 68 4a 33 6c 34 2f 4e 37 30 6c 5a 61 76 51 35 69 78 6b 68 66 6a 4f 66 4a 4c 47 7a 69 42 6d 48 51 6f 4c 48 53 35 72 64 32 57 37 50 59 42 41 4e 35 37 36 4a 43 73 6a 49 66 4a 43 38 5a Data Ascii: RQDwNG//+I+Imbcol5wsn41q04mMBL1uvV99Jx6zQWzKnlQBCD3FEysym/A4j+LoVcc+Nk4j/UC42 v3iJV1JhARZl6TYl4tkY0GBzgXvcnbk5TZGDzZM+Bsr292pp3LDSxyGyAt52EqFLMZecp3RL+rCSf36EzTBVD8RM9e 4YJ2voEoakhkVoUYnVUp45SpTQEHJ3l4/N70lZavQ5ixkhfOfJLGiBmHQoLHS5rd2W7PYBAN576JcsjlfJC8Z
2022-08-18 01:57:05 UTC	30	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	30	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:05 UTC	30	IN	Data Raw: 4d 78 64 64 67 55 31 46 33 61 58 56 62 53 79 42 73 52 34 43 59 38 50 61 56 79 53 54 33 66 33 6b 54 31 61 70 70 67 31 4b 34 4a 65 56 6e 6e 67 50 32 6e 6b 4d 63 73 4a 45 37 69 71 32 45 30 48 72 55 79 48 71 6b 52 38 48 67 68 7a 52 78 6e 4b 44 58 6c 39 52 68 48 72 33 74 63 41 79 4d 74 30 65 62 51 6e 65 6d 57 52 54 34 2f 46 77 7a 64 54 2b 33 6a 52 6f 58 70 4d 43 69 4b 47 53 4c 57 65 47 35 77 52 71 63 36 56 4f 5a 75 76 48 67 59 72 63 47 30 75 67 69 50 74 36 51 4d 69 55 64 6b 34 51 30 42 34 77 65 79 73 6c 56 2b 53 6c 33 55 67 34 71 35 63 31 52 50 74 48 6c 6b 45 68 42 5a 7a 44 38 56 2f 5a 67 6e 4d 45 47 75 6e 78 30 54 70 6e 59 33 49 52 58 6a 43 6a 32 69 59 54 72 41 7a 76 65 6a 77 64 39 61 62 74 2f 70 34 65 48 55 67 66 70 61 49 5a 43 7a 77 35 56 31 50 34 64 61 7a Data Ascii: MxddgU1F3aXVbSyBsR4CY8PaVyST3f3kT1appg1K4JeVnngP2nkMcsJE7iq2E0HrUyHqkR8HghzRxn KDXl9RhHr3tcAyMit0ebQnemWRT4/FwzdT+3jRoXpMCiKGSLWeG5wRqc6VOZuvHgYrcG0ugiPt6QMIUdk4Q0B4weysl V+Sl3Ug4q5c1RPtHlEhBZZD8V/ZgnMEGunx0TpnY3lRXjCj2iYtAzvejwd9abt/p4eHUgfpalZCzw5V1P4daz
2022-08-18 01:57:05 UTC	31	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	31	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	31	IN	Data Raw: 4e 31 56 30 34 2f 37 6e 46 47 77 77 52 55 31 63 62 4c 62 71 2b 32 4e 54 62 32 48 47 38 33 53 36 6d 55 4e 4e 6d 73 66 67 53 46 63 72 55 6e 31 32 2b 76 6d 54 39 6a 42 56 35 33 4c 46 6e 72 50 4a 44 4b 44 57 4d 30 49 37 46 72 41 4d 52 69 38 67 6c 52 39 50 6a 78 30 31 48 4d 62 4f 75 48 59 6b 79 45 6c 46 64 73 73 2f 56 33 54 36 4b 36 48 66 30 75 4d 76 6d 38 64 74 36 57 33 70 56 76 7a 64 45 35 73 71 44 4d 34 68 32 2f 42 4e 61 56 52 59 50 73 45 6d 37 74 46 5a 68 64 52 64 43 57 32 31 57 5a 4f 7a 75 74 4f 46 38 4b 67 4c 35 50 76 63 7a 39 38 46 34 4c 33 6f 74 67 46 41 7a 68 45 73 49 52 75 76 4d 6c 30 66 50 73 42 51 6b 48 45 74 4a 70 4b 63 70 36 67 70 5a 76 4e 58 59 34 68 34 4c 58 47 78 30 4a 43 53 46 37 70 31 57 32 4a 69 77 31 31 38 5a 5a 69 59 4b 46 37 65 77 57 31 Data Ascii: N1V04/7nFGwwRU1cbLbq+2NTb2HG83S6mUNNmsfgSfcrUn12+vmT9jBV53LFnrPJDKDWM0l7FrAMRi 8glR9Pjx01HMbOuHYkyElFdss/V3T6K6Hf0uMvm8dt6W3pVvzdE5sqDM4h2/BNaVRYPsEm7fZhdRdCW21WZOzutOF 8KgL5Pvc298F4L3otgFAzhEslRuvMI0fPsBQkHEtJpKcp6gpZvNXy4h4LXGx0JCSF7p1W2Jiw118Z2iYKf7ewW1
2022-08-18 01:57:05 UTC	32	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	32	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	32	IN	Data Raw: 56 47 7a 53 2b 33 54 30 56 4b 6e 53 6c 5a 32 67 59 6a 72 76 52 58 62 58 4f 6f 79 37 35 33 50 73 32 69 78 51 49 50 64 39 2f 31 45 61 4d 66 69 69 46 65 4e 52 4b 49 6d 48 6f 2f 4a 4b 66 36 44 57 48 35 6f 39 4f 74 47 6e 79 35 6d 54 72 49 38 6c 35 58 77 54 52 6a 36 49 50 79 68 4f 73 75 69 2f 71 7a 41 34 4c 70 78 5a 31 77 6f 68 2b 44 68 56 66 52 71 47 79 49 2b 4d 31 76 38 36 6f 4c 4d 46 66 6c 6f 4b 54 66 64 36 62 42 55 49 5a 4e 32 51 59 73 4c 45 62 4a 65 79 38 4c 56 69 69 6b 62 68 57 48 73 6b 71 5a 48 4d 68 75 71 41 62 39 68 70 45 45 34 6e 68 43 50 6b 4e 62 31 37 7a 43 56 5a 63 36 50 75 38 72 65 31 4b 4d 63 34 6c 4a 4d 6e 79 33 43 30 38 49 73 41 68 48 58 33 2f 76 71 74 55 35 36 38 69 4e 31 77 65 66 46 36 70 31 73 47 4b 72 72 64 79 5a 6e 68 4b 56 61 36 4d 2f 48 Data Ascii: VGzS+3TOVKnSlZ2gYjrvRXbXOoy753Ps2ixQlPd9/1EaMfiFeNRKImHo/JKf6DWH5o9OtGny5mTri8l5XwTRj6l PyhOsuI/qzA4LpxZ1woh+DhVfRqGyl+M1v86oLMFfIoKTFdf6bBUIZN2QYsLEbJey8LViikbhWHskqZHMhuqAb9hpEE 4nhCPkNb17zCVZc6Pu8re1KMc4lJMny3C08IsAhHX3/vqtU568iN1wefF6p1sGKrrdyZnhKVa6M/H
2022-08-18 01:57:05 UTC	34	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	34	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	34	IN	Data Raw: 75 68 39 70 32 76 4e 32 64 71 58 48 36 75 48 37 5a 32 2f 77 70 50 73 54 37 38 36 54 45 41 58 56 6d 73 62 49 48 52 47 78 77 6b 46 44 6e 4e 56 71 73 4d 45 70 73 73 46 67 64 73 66 52 2f 48 4f 50 43 57 45 32 4f 6e 66 30 38 34 55 38 45 46 61 34 61 4d 6c 54 44 31 64 74 30 6f 69 65 2b 55 68 6f 72 2b 78 39 50 54 6d 45 2f 57 55 54 56 49 6c 2f 76 6c 5a 2f 67 70 63 53 70 30 72 45 36 54 46 4f 49 47 43 75 72 47 67 4b 58 4c 68 75 48 6c 50 68 6a 50 48 59 68 49 2f 63 46 78 73 58 67 39 44 68 77 57 4b 41 63 50 4c 37 31 61 4b 70 68 48 34 57 6c 57 71 46 75 68 50 74 69 37 70 56 73 61 75 43 74 64 65 48 57 5a 38 4f 38 37 69 68 4f 6c 66 4b 46 41 64 6b 44 49 6e 62 4f 69 46 46 58 77 33 79 47 58 31 46 51 37 63 36 51 41 30 45 68 74 2b 36 53 31 63 76 53 6a 59 6a 73 69 62 72 38 70 42 Data Ascii: uh9p2vN2dqXH6uH7Z2/wpPsT786TEAXVmsblHRGxwkFDnNVqsMEpssFGdsfR/HOPCWE2Onf084U8EF 4a4aMITD1dt0oie+Uhor+X9PTmE/WUTVII/vIz/gpcSp0rE6TFOIGCurGgKXLhuHlPhPHYhl/cFxsXg9DhwWKAcpL7 1aKphH4WlWqFuhPti7pVsauCtdeHWZ8O87ihOlIfKfAdkDlnbOIFFXw3yGX1F7Qc6QA0Eht+6S1cvSjYjsibr8pB
2022-08-18 01:57:05 UTC	35	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	35	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	35	IN	Data Raw: 38 4b 4f 33 4e 44 49 64 4f 59 6b 33 4e 68 6d 4f 50 4a 73 37 4d 71 49 63 54 6c 49 78 48 5a 68 6a 4a 2b 43 70 37 49 69 39 75 5a 6d 47 51 69 4e 78 32 33 68 4d 56 62 71 45 78 4a 49 51 79 36 6d 4e 38 61 61 31 47 65 63 77 63 4d 4e 48 68 6d 55 51 50 58 52 4c 2f 43 59 4c 61 4f 77 69 38 4b 73 69 4f 58 73 2f 43 41 4b 75 38 49 6c 36 30 42 65 41 5a 44 35 72 44 43 63 34 74 4f 72 73 38 66 53 48 50 4c 79 33 78 69 48 4d 74 79 6a 47 65 57 42 44 63 38 54 34 75 71 6d 6e 77 6b 78 4d 4c 38 6f 34 74 36 7a 36 4e 75 53 52 2b 47 6e 43 72 4d 4d 68 4f 71 4b 71 71 70 50 6d 34 79 6b 57 6c 73 37 39 58 5 5 67 6e 74 36 51 6c 78 70 78 45 66 6a 7a 74 67 7a 7a 41 4a 42 32 37 2f 39 76 37 2b 78 2b 6d 6c 69 33 50 35 36 6a 69 50 49 71 4c 35 4b 6d 39 4d 2f 34 2f 54 31 36 53 77 77 78 41 67 6c 42 Data Ascii: 8KO3NDIdOYk3NhmOPJ57MqlcTlIxHZhjJ+Cp7li9uZmGQinX23hMVbqExJlQy6mN8aa1GecwcMNHhm UQPXRl/CYLaOwi8KsiOXs/CAKu8lI60BeAZD5rDcc4tOrs8fSHPLy3xiHmtYjGeWBDc8T4uqmnwKxML8o4t6z6NuSR +GnCrMMhOqKqppM4yKwls79XUgnt6QlXpEfjztgzAJB27/9v7+X+mli3P56jPlqlL5Km9M/4/T16SwwwAgIB
2022-08-18 01:57:05 UTC	36	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	36	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	36	IN	Data Raw: 34 45 30 4a 71 59 37 5a 52 59 35 58 6d 74 58 49 6b 6b 46 6c 65 6b 53 77 67 50 6e 46 30 41 5a 62 4f 74 6f 4d 5a 36 43 77 50 61 58 66 53 31 48 53 6d 6d 69 4d 52 4f 7a 30 2b 56 61 73 33 36 57 61 74 78 67 7a 37 58 33 55 57 67 4d 68 49 76 58 42 58 5a 46 70 70 4d 6c 5a 48 67 45 42 6a 45 51 2f 54 48 34 6e 4c 53 4a 62 66 71 71 57 6b 48 59 6c 5a 4b 4f 30 49 37 2b 76 54 37 4e 37 32 33 6b 48 70 49 67 39 46 70 71 4f 46 38 5a 64 64 72 50 70 67 6b 55 4c 46 61 73 35 45 7 9 45 6a 38 34 67 59 4e 53 65 4a 74 77 4d 79 68 51 35 54 39 72 43 5a 41 35 45 69 73 53 6a 2b 4b 64 52 79 43 33 43 34 51 58 6e 73 72 5a 7a 66 51 68 2b 57 71 7a 6f 61 4a 70 5a 44 72 59 75 4c 7a 70 35 31 58 2b 37 47 59 5a 75 38 2b 51 37 49 38 58 39 72 2b 52 53 50 43 37 55 39 34 41 55 66 75 44 64 36 31 6d 6a Data Ascii: 4E0JqY7ZRY5XmtXlkkFlekSwgPnF0AZbOtoMZ6CwPaXfS1HSmmiMROzo+Vas36Watxgz7X3UWgMhlv XBxZFppMlZHgEBjEQ/TH4nLSJbfqQWkHYlZKO0I7+vT7N723kHplg9FpqOF8ZddrPpgkULFas5EyEj84gYNSeJtwMy hQ5T9rCZA5EisSj+KdRyC3C4QXnsrZzfQh+WqzoaJpZDrYuLzp51X+7GYZu8+Q7l8X9r+RSPC7U94AUfuDd61mj

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:05 UTC	38	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	38	IN	Data Raw: 31 30 30 65 0d 0a Data Ascii: 100e
2022-08-18 01:57:05 UTC	38	IN	Data Raw: 66 6d 71 50 50 6b 66 63 4c 4c 32 4e 70 4f 31 53 47 59 52 2f 79 77 33 45 38 6e 30 6e 64 4a 59 62 69 49 54 4d 71 33 48 55 33 6c 77 44 72 33 78 34 4c 32 33 70 70 69 61 45 57 35 61 46 4a 55 32 2f 55 33 61 35 48 6a 77 56 6f 48 77 48 63 38 4e 38 52 61 4b 69 2b 6b 48 7a 35 52 4a 58 34 54 47 32 6c 68 6d 6b 35 6f 49 70 2b 74 41 7a 48 4c 77 51 4c 7a 31 7a 43 4d 5a 33 43 36 64 58 51 30 47 71 37 54 54 65 38 33 53 49 6c 46 6b 76 64 68 75 71 72 32 44 70 42 65 61 65 78 6c 39 38 44 4b 63 59 2b 62 4b 58 46 50 32 44 45 52 6d 2f 4d 31 41 4a 4e 34 55 69 45 71 63 46 4f 35 31 43 67 68 36 73 5a 79 63 2b 2b 48 4c 68 52 57 78 65 58 2f 6e 2b 45 4c 36 69 46 74 6c 45 78 36 37 55 72 62 77 73 4e 52 71 43 50 63 36 47 35 69 58 32 4f 5a 78 73 37 73 32 56 66 78 37 51 63 30 6d 66 4c 78 78 Data Ascii: fmqPPkfcLL2NpO1SGYR/yw3E8n0ndJYbiITMq3HU3lwDr3xL423ppiaEW5aFJU2/U3a5HjwVoHwHc8 N8RaKi+kHz5RJX4TG2lhmK5olp+tAzHLwQLz1zCMZ3C6dXQ0Gq7TTe83SIIlFkvdhuqr2DpBeaexl98DKcY+bKXFP2D ERm/M1AJN4UiEQcFO51Cgh6sZyc++HLhRWxeX/n+EL6iFiEx67UrbvnsNRqCPc6G5iX2OZxs7s2Vfx7Qc0mfLxx
2022-08-18 01:57:05 UTC	39	IN	Data Raw: 48 31 64 4a 5a 6e 7a 54 51 4c 4f 6f 30 53 6a 53 72 46 62 4d 4b 57 44 49 59 79 57 53 30 6c 46 52 78 75 6c 62 63 4b 79 45 57 65 58 55 6d 72 4c 76 76 4c 36 66 2f 42 31 64 67 32 6d 6e 64 6f 30 52 48 79 67 46 79 37 50 58 36 51 31 4d 67 62 4e 4b 46 52 75 4d 45 51 67 65 41 77 4e 6c 58 6a 57 4d 68 58 35 49 6b 70 56 52 56 6f 59 57 2f 6d 42 50 61 6d 32 68 42 4f 71 4c 68 78 61 4c 34 4e 72 6f 74 74 6a 4c 7a 39 34 51 70 78 43 6a 52 57 70 5a 7a 48 63 76 78 2b 4f 7a 6a 33 55 77 35 35 52 44 5a 4f 6b 68 63 48 43 77 4a 58 58 67 57 72 70 7a 4c 33 61 57 54 4c 59 45 38 6c 4e 32 31 71 49 4b 76 3 8 32 51 4a 62 38 32 53 44 47 54 42 41 63 4c 79 49 77 57 45 76 62 39 4f 41 4c 6c 66 42 78 4a 50 36 66 42 78 75 56 71 59 32 4e 6b 50 6d 4b 62 66 55 52 62 78 63 44 51 53 4b 78 73 6f 67 79 Data Ascii: H1dJZnzTQLOo0SjSrFbMKWDIYyWS0lFRxulbcKyEWeXUmrLvL6f/B1dg2mndo0RHgYf7PX6Q1Mgb NKFRuMEQgeAwNlXjWMhX5lkpVRVoYw/mBPam2hBOqLhxaL4NrottjLz94QpxCjRWpZzhcvx+Ozj3Uw55RDZ0khcHCw JXxgWwRpZL3aWTLYE8lN21qIKv82QJb82SDGTBAcLylwWEvb9OALfBxBJP6fBxuVqY2NkPmKbUfURbxcDQSKxsogy
2022-08-18 01:57:05 UTC	40	IN	Data Raw: 4e 6c 6c 41 63 45 65 4f 64 6b 76 45 43 79 66 32 43 66 47 78 73 76 34 2b 73 75 51 6e 6f 77 52 6a 6d 54 79 4d 55 67 74 62 50 69 46 55 53 63 62 6f 70 49 79 64 6f 30 48 66 4c 62 63 68 63 57 42 59 54 7a 76 62 58 79 32 72 4d 52 6b 2b 77 4f 57 41 46 49 58 75 46 4e 31 65 30 69 57 42 44 6f 52 4b 6a 6f 75 55 77 51 31 6c 75 6c 46 70 6e 49 38 61 75 6f 5a 74 43 4e 54 33 53 49 7a 69 39 74 46 6c 4c 6f 75 65 62 73 44 37 72 37 55 32 6e 6b 78 68 48 46 61 43 65 6d 69 56 41 66 5a 36 36 63 4d 69 4b 52 57 47 61 54 47 6c 62 49 6e 64 62 5a 79 35 4b 55 49 7a 36 54 38 78 4f 74 4e 70 6c 77 36 69 5 2 2b 37 4e 47 45 79 4c 62 64 2b 77 4a 49 64 44 6c 65 35 59 77 4b 44 45 6a 4f 64 6a 4c 51 48 51 64 43 6a 55 38 77 41 68 68 63 31 47 78 47 56 6d 49 4e 38 7a 54 53 67 5a 50 30 45 35 7a 67 Data Ascii: NlIAcEeOdkvECyf2CfGxsv4+suQnowRjmTyMUgtbPiFUScboplydo0HflbchcWBYTzvbXy2rMRk+wO WAFIXuFN1e0iWBD0oORKjouUwQ11ulFpnl8auoZtCNT3Sizi9tFILouebSd7r7U2nkhxHFaCemiVAFz66cMiKRWGaTG lbnDbZy5KUIz6T8xOtNplw6iR+7NGEYlDb+wJldle5YwKDEjOdjLQHqdcJ8uAhhc1GxGvMln8zTSgZP0E5zg
2022-08-18 01:57:05 UTC	42	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	42	IN	Data Raw: 31 30 30 65 0d 0a Data Ascii: 100e
2022-08-18 01:57:05 UTC	42	IN	Data Raw: 54 52 41 77 6a 61 32 54 6d 32 78 57 51 44 31 53 63 68 75 43 48 46 6c 37 4f 7a 61 37 4d 55 4f 49 68 6c 64 78 64 49 52 41 7a 35 57 68 77 62 76 31 51 36 61 77 5a 43 45 67 49 6c 66 53 44 2b 55 52 56 71 6e 4f 78 77 61 59 6c 45 4c 36 53 55 43 7a 53 6e 54 62 4b 39 58 72 70 79 46 4a 4f 56 70 39 77 5a 4c 4c 70 39 30 66 59 4b 36 70 34 30 4e 57 49 62 67 44 79 53 49 79 63 34 54 45 57 79 34 66 74 56 68 78 4f 30 56 73 6c 66 56 34 68 44 4c 73 78 41 35 6f 6c 46 70 67 68 5 4 62 56 69 6c 54 4d 32 56 4e 6e 4d 33 4f 7a 73 33 47 50 5a 4b 59 2f 4a 51 54 42 50 55 74 6d 64 30 2b 30 51 42 74 4c 53 35 2b 43 4c 30 64 34 30 46 6d 77 49 41 71 41 68 69 6d 33 45 2b 72 57 33 49 73 46 37 53 57 46 31 41 52 41 5a 69 50 44 39 59 7a 61 63 4c 51 58 45 5a 38 6f 68 38 65 4b 45 6b 7a 6f 52 72 57 Data Ascii: TRAwaJ2m2xWQD1SchuCHFI7Oza7MUOIhldxdIRAZ5Whwbv1Q6awZCEglfISD+URVqnOxwaYIEL6SU CzSnTbK9XrpyFJOVp9wZLLp90fYK6p40NWlbgDySlyc4TEWY4ftVhxO0VslfV4hLdsxA50lFpghtbVilTM2VNnm3Oz s3GPZKY/JQTBPUtmd0+OQBtLS5+CL0d40FmwIAqAhim3E+rW3isF7SWF1ARAZiPD9YzacLQXEZ8oh8eKEkz0RrW
2022-08-18 01:57:05 UTC	43	IN	Data Raw: 4c 38 47 6f 41 52 36 47 6e 7a 62 79 47 44 4a 78 79 4c 61 7a 79 31 71 45 47 78 6a 79 36 56 71 64 43 55 54 34 71 6c 42 54 6c 35 58 67 39 4d 72 6e 43 7a 6d 30 55 2f 76 59 39 63 42 63 62 4a 34 36 68 68 36 5a 6e 64 4f 50 4f 33 44 54 35 38 78 6e 41 46 55 38 4a 6a 7a 47 48 78 56 33 6b 31 41 51 4b 42 7a 64 48 45 64 45 55 63 55 61 45 32 59 36 50 36 4b 76 72 48 6b 4a 45 66 6f 48 73 6e 4f 67 64 79 34 68 6a 36 69 7a 62 51 76 39 50 48 63 43 51 56 49 62 33 43 71 6f 6e 58 51 71 6d 35 41 65 6c 79 66 4c 38 65 67 49 6d 39 43 64 6f 6c 35 44 46 43 45 33 6f 56 41 4a 75 54 31 53 74 37 65 55 55 5a 53 69 71 51 45 55 55 6e 38 30 32 65 38 36 4e 55 53 62 45 4d 53 45 41 77 6e 51 4a 5a 6b 78 4d 74 50 42 75 58 70 53 6c 4b 59 31 6e 54 77 77 47 4c 57 36 2b 63 47 63 72 67 53 46 62 6e Data Ascii: L8GoAR6GnzbyGDJxyLazy1qEGxjy6VqdCUT4qlBTl5Xg9MrnCzm0U/Y9cBcbJ46hh6ZndOPO3DT58 xnAFU8JjzGHxV3k1AQKBzdHEdEUcUaE2y6P6KvrHkJEfoHsnOgdy4hj6izbQv9PHcCQVlb3CqonXQqm5AelyfL8egl m9Cdol5DFCE30VAJuT1St7eUUZSiqQUEUUn802e86NUSbEMSE4AwnQJZkxMtPBuXsIKY1nTwwGLW6+cGcrgSfBfn
2022-08-18 01:57:05 UTC	44	IN	Data Raw: 67 70 4c 58 47 48 72 69 57 63 32 6e 61 31 76 73 58 4c 31 36 38 72 73 6d 70 46 45 56 6e 46 79 34 64 5a 79 55 4c 62 45 68 62 5a 38 71 75 41 4e 39 6b 75 33 65 4a 6b 4f 6e 31 72 2f 2f 71 62 65 69 36 51 61 66 36 76 2f 49 6b 2b 67 71 46 4f 79 4e 55 73 4f 30 52 49 48 49 62 56 61 41 42 69 57 6e 36 30 6a 69 61 72 62 53 51 71 37 34 7a 4e 74 55 65 6a 6f 49 39 79 74 71 69 44 61 64 58 54 38 70 56 41 42 35 34 69 44 6d 38 71 76 50 71 34 58 53 6c 54 37 77 51 76 51 4e 45 46 45 63 47 41 77 31 72 42 59 74 5a 48 44 50 58 52 41 50 52 42 68 44 52 72 74 4d 4f 6a 6b 4c 2f 57 4a 73 38 78 4d 73 38 78 58 74 58 76 50 43 51 31 7a 2b 73 45 65 48 59 44 39 47 50 37 69 6b 67 63 75 33 51 71 46 6a 31 32 50 6f 68 43 30 58 41 71 63 6c 72 57 59 42 47 78 65 34 66 66 73 54 61 6f 68 32 54 6e 76 Data Ascii: gpLXGHriWc2na1vsXL168rsmPFEVnFy4dZyULbEhbZ8quAN9ku3eJkOn1r//qbei6Qaf6v/lk+gqFOyNusO0RIHl bVaABiWn60jarbSQQ74zNtUeJol9ytqiDadXT8pVAB54Idm8qvPq4XSIT7wQvQNEFEcGAW1rBYtZHDpXRAPRBhDRr tMOjkl/WJs8xMs8xXtXvPCQz1sEeHYD9GP7ikgcu3QqFj12PohC0XAqclrWYBGxe4f5Taoh2Tnv
2022-08-18 01:57:05 UTC	46	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	46	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:05 UTC	46	IN	Data Raw: 38 4f 50 75 6f 52 48 7a 77 4a 42 42 49 4c 52 50 30 70 68 63 57 39 63 55 31 4e 4f 4f 44 44 65 42 71 5a 38 71 77 6b 4f 71 39 41 33 33 68 58 6d 6f 35 65 42 54 4e 41 53 53 62 6e 58 49 33 54 49 48 70 59 62 42 39 5a 53 6e 77 73 63 47 41 44 31 59 6a 2f 74 55 7a 6a 34 56 4b 62 76 64 59 31 34 39 43 34 51 5a 64 42 78 76 35 64 58 78 62 6c 78 56 4f 48 6f 41 67 63 31 66 71 2b 2b 30 64 4f 2b 62 43 4f 4f 71 59 49 31 69 47 58 6f 33 63 4f 6a 52 34 47 6f 4b 34 35 79 32 32 67 38 33 39 7a 50 7a 56 4d 58 76 6a 41 64 33 2f 39 36 62 38 50 52 4c 62 6f 61 78 53 6f 50 75 73 64 36 39 44 41 51 35 57 43 42 78 34 49 79 49 43 37 54 63 66 78 52 52 75 56 48 70 32 2f 66 76 53 35 72 74 71 76 44 76 67 5a 74 4e 66 53 6f 65 36 78 48 37 77 4a 42 30 64 61 57 45 35 4e 68 51 4e 53 51 51 5a 65 66 Data Ascii: 8OPuoRHzwJBbILRP0phcW9cU1NOODDeBqZ8qwkOq9A33hXmo5eBTNASSbnXI3TIHpYbB9ZSnwscGAD1Yj/tUzj4VKbvdY149C4QZdBxv5dXxbIxVOHoAgc1fq++0dO+bCOOqY11iGXo3cOjR4GoK45y22g839zPzVMXvjAd3/96b8PRLboaxSoPusd69DAQ5WCBx4lylC7TcfxRRuVHp2/fvS5rtqvDvgZtNfSoe6xH7wJB0daWE5NhQNSQQZef
2022-08-18 01:57:05 UTC	47	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	47	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:05 UTC	47	IN	Data Raw: 31 41 30 4d 46 2f 36 6e 64 37 59 64 63 6a 44 75 63 2f 6d 51 59 33 51 78 6b 59 68 52 62 68 68 34 4d 44 49 34 43 78 61 52 69 30 65 4e 42 65 46 76 6e 2f 77 46 56 34 75 68 6a 4b 63 32 76 57 41 41 41 41 42 4a 52 55 35 45 72 6b 4a 67 67 67 3d 3d 22 3e 0d 0a 20 20 20 20 20 3c 2f 70 3e 0d 0a 0d 0a 20 20 20 20 20 3c 70 3e 3c 73 74 72 6f 6e 67 3e 54 68 65 20 72 65 71 75 65 73 74 20 6d 61 64 65 20 77 61 73 20 74 6f 20 66 6f 72 62 69 64 64 65 6e 20 63 6f 6e 7 4 65 6e 74 2e 3c 2f 73 74 72 6f 6e 67 3e 3c 2f 70 3e 0d 0a 20 20 20 20 20 3c 70 3e 53 6f 72 72 79 20 61 62 6f 75 74 2 0 74 68 61 74 2e 20 50 6c 65 61 73 65 20 74 72 79 20 72 65 66 72 65 73 68 69 6e 67 20 61 6e 64 20 63 6f 6e 74 61 63 74 20 75 73 20 69 66 20 74 68 65 20 70 72 6f 62 6c 65 6d 20 70 65 72 Data Ascii: 1A0MF/6nd7YdcjDuc/mQY3QxkYhRbh4MDI4CxaRi0eNBeFvn/wFV4uhjKc2vWAAAAABJRUErkJggg=="> The request made was to forbidden content. Sorry about that. Please try refe shing and contact us if the problem per
2022-08-18 01:57:05 UTC	49	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	49	IN	Data Raw: 61 62 34 0d 0a Data Ascii: ab4
2022-08-18 01:57:05 UTC	49	IN	Data Raw: 7a 61 47 39 77 49 45 4e 54 4e 69 41 6f 54 57 46 6a 61 57 35 30 62 33 4e 6f 4b 53 49 67 65 47 31 77 54 55 30 36 53 57 35 7a 64 47 46 75 59 32 56 4a 52 44 30 69 65 47 31 77 4c 6d 6c 70 5a 44 70 46 4d 54 5a 43 52 44 59 33 52 45 49 7a 52 6a 41 78 4d 55 55 79 51 55 51 7a 52 45 49 78 51 7a 52 45 4e 55 46 46 4e 55 4d 35 4e 69 49 67 65 47 31 77 54 55 30 36 52 47 39 6a 64 57 31 6c 62 6e 52 4a 52 44 30 69 65 47 31 77 4c 6d 52 70 5a 44 70 46 4d 54 5a 43 52 44 59 33 52 55 49 7a 52 6a 41 78 4d 55 55 79 51 55 51 7a 52 45 49 78 51 7a 52 45 4e 55 46 46 4e 55 4d 35 4e 69 49 2b 49 44 78 34 62 58 42 4e 54 54 70 45 5a 58 4a 70 64 6d 56 6b 52 6e 4a 76 62 53 42 7a 64 46 4a 6c 5a 6a 70 70 62 6e 4e 30 59 57 35 6a 5a 55 6c 45 50 53 4a 34 62 58 41 75 61 57 6c 6b 4f 6b 55 78 4e 6b Data Ascii: zaG9wIENTNiAoTWfJaW50b3NoKSilgeG1wTU06SW5zdGfuY2VJRd0ieG1wLmlpZDpFMTZCRDY3RElZRjAxMUUyQUQzRElXQzRENUFFNUM5NilgeG1wTU06RG9jdW1lbnRJRD0ieG1wLmRpZDpFMTZCRDY3RUIzRjAxMUUyQUQzRElXQzRENUFFNUM5Nil+IDx4bXBNTTpEZXJpdmVkrNjVbSBZdFJlZjppbnN0YW5jZU1EPSJ4bXAuaWlkOkUxNk
2022-08-18 01:57:05 UTC	50	IN	Data Raw: 75 6f 34 62 30 37 46 42 61 4f 68 73 75 30 41 34 55 6e 63 2b 54 31 54 55 31 4e 6a 33 4b 73 53 53 45 35 79 4a 36 35 6a 71 46 32 44 44 64 38 51 71 57 59 6d 41 5a 72 49 4d 32 56 6c 5a 54 64 6e 5a 6d 62 36 41 62 70 64 56 39 56 36 65 63 39 7a 6e 66 35 51 37 48 6a 59 75 6d 64 52 45 30 4a 4f 70 33 4d 6a 69 74 4f 34 53 46 61 2b 63 5a 7a 38 55 6d 71 65 33 54 43 62 53 4c 76 64 66 6b 52 2f 6b 57 44 64 4e 51 6c 35 49 6e 75 54 63 79 73 4f 63 70 46 54 33 35 5a 72 62 42 7 8 78 34 70 33 4a 41 48 6c 5a 56 56 57 31 4d 2f 36 33 34 56 52 74 2b 46 76 4c 42 67 4b 2f 76 35 4c 56 39 57 53 2b 31 30 78 4d 54 45 77 74 52 77 37 58 76 71 4f 4c 2b 65 32 51 38 56 33 41 59 49 4f 49 41 58 51 32 36 2f 68 65 57 56 6e 5a 43 56 66 63 79 4b 48 67 32 43 42 67 54 70 6d 50 6d 6a 59 4d 38 6c 32 34 Data Ascii: uo4b07FBaOhsu0A4Unc+T1U1Nj3KsSSE5yJ65jqF2DD8QqWYmAZrIM2VIZTdnZmb6AbpdV9V6ec9znf5Q7HjYumdre0JOp3MjitO4Sfa+cZz8Umqe3TCbSLvdfkR/kWVDdNQI5InuTcysOcpFT35ZrbBxx4p3JAHIZVvW1D/634VRt+FvLBgK/v5LV9WS+10xMTEwtRw7XvqQL+e2Q8V3AYIOIAXQ26/heWvNzCVfcykHg2CBgTpmPmjYM8l24
2022-08-18 01:57:05 UTC	51	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	51	IN	Data Raw: 61 62 34 0d 0a Data Ascii: ab4
2022-08-18 01:57:05 UTC	51	IN	Data Raw: 7a 64 47 46 75 59 32 56 4a 52 44 30 69 65 47 31 77 4c 6d 6c 70 5a 44 70 45 51 55 4d 31 51 6b 55 78 52 55 49 30 4d 55 4d 78 4d 55 55 79 51 55 51 7a 52 45 49 78 51 7a 52 45 4e 55 46 46 4e 55 4d 35 4e 69 49 67 65 47 31 77 54 55 30 36 52 47 39 6a 64 57 31 6c 62 6e 52 4a 52 44 30 69 65 47 31 77 4c 6d 52 70 5a 44 70 45 51 55 4d 31 51 6b 55 78 52 6b 49 30 4d 55 4d 78 4d 55 55 79 51 55 51 7a 52 45 49 78 51 7a 52 45 4e 55 46 46 4e 55 4d 35 4e 69 49 2b 49 44 78 34 62 58 42 4e 54 54 70 45 5a 58 4a 70 64 6d 56 6b 52 6e 4a 76 62 53 42 7a 64 46 4a 6c 5a 6a 70 70 62 6e 4e 30 59 57 35 6a 5a 55 6c 45 50 53 4a 34 62 58 41 75 61 57 6c 6b 4f 6b 55 78 4e 6b 4a 45 4e 6a 64 47 51 6a 4e 47 4d 44 45 78 52 54 4a 42 52 44 4e 45 51 6a 46 44 4e 45 51 31 51 55 55 31 51 7a 6b 32 49 69 Data Ascii: zdGFuY2VJRd0ieG1wLmlpZDpEQUM1QkUxRUI0MUMxMUUyQUQzRElXQzRENUFFNUM5NilgeG1wTU06RG9jdW1lbnRJRD0ieG1wLmRpZDpEQUM1QkUxRkI0MUMxMUUyQUQzRElXQzRENUFFNUM5Nil+IDx4bXBNTTpEZXJpdmVkrNjVbSBZdFJlZjppbnN0YW5jZU1EPSJ4bXAuaWlkOkUxNkJENjdGQjNGMDExRTJBRDNEQjFDNEQ1QUU1Qzk2li
2022-08-18 01:57:05 UTC	53	IN	Data Raw: 50 46 78 5a 79 71 52 70 58 41 52 47 2f 59 4f 72 31 4f 62 46 4a 30 67 55 73 6b 58 42 62 61 6d 63 52 31 4f 4b 6d 4d 55 76 44 78 48 52 41 75 38 2f 4c 6d 59 33 6a 46 4c 4d 55 70 46 71 7a 39 48 78 47 36 35 73 6d 59 4a 64 79 4b 79 45 43 4f 78 44 69 45 41 65 2f 70 31 67 6a 46 32 6f 6f 6e 69 76 5a 41 73 78 56 67 6c 32 64 61 61 34 45 51 57 43 57 36 4a 35 35 71 46 41 46 46 5a 69 4a 57 59 4c 78 4e 51 79 32 71 4f 53 55 7a 47 52 73 79 58 43 55 44 49 65 6c 69 77 41 48 45 4f 34 57 53 6c 57 51 42 52 46 6f 5a 61 6b 58 63 4b 6d 43 58 6d 79 58 41 4b 73 30 56 65 39 76 6c 38 71 34 32 57 6f 49 59 70 4a 55 34 68 56 33 68 4b 63 4e 73 38 6d 39 67 6c 37 70 2f 78 51 37 33 65 46 35 6b 42 34 6a 35 6d 4e 72 57 6d 54 4a 52 4e 77 41 7a 71 69 56 31 43 78 6a 56 54 5a 43 49 6b 45 71 2b 5a Data Ascii: PFxZyqPzXARG/YOr1ObFJ0gUskXBamcR1OKmMUvDxHRAu8/LmY3JfLMUPFqz9HxG65smYJdyKyECOxDiEAe/p1gjF2oonivZAsxVgl2daa4EQWCW6J55qFAFFZiJWYLxNQy2qOSUzGrsyXCUDIeliwAHEO4WSIWQBRFoZakXcKmCXmyXAKs0Ve9vl8q42WoIYpJU4hV3hKcNs8m9gl7p/xQ73eF5kB4j5mNrWmTJRNwAaqiV1CjxjVTZCikEq+Z
2022-08-18 01:57:05 UTC	54	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:05 UTC	54	IN	Data Raw: 31 37 66 0d 0a Data Ascii: 17f

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:05 UTC	54	IN	Data Raw: 51 45 6b 4c 2b 63 44 4d 53 6f 4c 76 5a 6f 32 66 51 42 37 41 4a 73 73 4e 41 75 46 75 76 6f 72 6c 44 56 56 6b 6b 67 32 49 38 37 2b 6a 6f 32 4b 32 51 41 56 70 68 44 72 66 79 56 69 4b 35 56 71 74 4f 33 34 4f 6b 61 78 58 43 70 2b 37 64 72 64 44 42 43 41 64 75 62 6d 36 65 69 64 58 2b 32 57 77 71 54 35 6b 6f 6d 77 68 34 59 51 4c 6b 2b 48 34 61 45 39 33 68 38 58 67 32 67 76 48 65 6b 51 5a 4f 47 53 67 4c 5a 54 4c 79 44 54 4c 4a 34 4c 78 39 2f 4b 5a 57 4b 42 53 61 6 9 6e 54 34 49 79 33 46 71 51 42 66 6e 55 5a 52 34 32 50 4b 51 46 6b 73 42 72 39 51 4b 56 58 43 50 75 73 44 33 4f 69 41 2f 52 6b 51 35 6b 50 38 71 56 2f 4a 6c 31 57 79 77 41 70 2f 36 2b 64 63 6d 50 4d 32 7a 4c 31 55 72 55 61 68 65 34 4a 71 66 6e 57 57 4b 58 49 75 6c 33 75 55 62 66 50 38 6e 6a 41 46 4c 57 Data Ascii: QEkL+cDMSoLvZo2fQB7AJssNAuFuvorlDVVkg2l87+jo2K2QAVphDrfyViK5VqtO34OkaxXCp+7dr dDBCAdubm6eidX+2WwqT5komwh4YQLk+H4aE93h8Xg2gvHekQZOGSgLTZLYDTLJ4Lx9/KZWKBSainT4ly3FqQBfnUZ R42PKQFksBr9QKVXCPusD3OiA/RkQ5kP8qV/Jl1WywAp/6+dcPM2zL1UrUahe4JqfnWWKXlul3uUbfP8njAFLW
2022-08-18 01:57:05 UTC	54	IN	Data Raw: 0d 0a 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49705	185.199.108.133	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:05 UTC	54	OUT	HEAD /drgreenthumb93/CVE-2022-30190-follina/main/bad.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: raw.githubusercontent.com
2022-08-18 01:57:05 UTC	55	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 14 Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline'; sandbox Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-Frame-Options: deny X-XSS-Protection: 1; mode=block Content-Type: text/plain; charset=utf-8 X-GitHub-Request-Id: 7924:06B9:5187D0:55A96E:62FD9C71 Accept-Ranges: bytes Date: Thu, 18 Aug 2022 01:57:05 GMT Via: 1.1 varnish X-Served-By: cache-mxp6939-MXP X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1660787826.732014,VS0,VE121 Vary: Authorization,Accept-Encoding,Origin Access-Control-Allow-Origin: * X-Fastly-Request-ID: b9594ed1c6d167616f9ea3a4eaa3aa878f0b48f7 Expires: Thu, 18 Aug 2022 02:02:05 GMT Source-Age: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49714	185.199.109.133	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:10 UTC	96	OUT	HEAD /drgreenthumb93/CVE-2022-30190-follina/main/bad.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: raw.githubusercontent.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:10 UTC	97	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 14 Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline'; sandbox Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-Frame-Options: deny X-XSS-Protection: 1; mode=block Content-Type: text/plain; charset=utf-8 X-GitHub-Request-Id: 7924:06B9:5187D0:55A96E:62FD9C71 Accept-Ranges: bytes Date: Thu, 18 Aug 2022 01:57:10 GMT Via: 1.1 varnish X-Served-By: cache-mxp6941-MXP X-Cache: HIT X-Cache-Hits: 1 X-Timer: S1660787831.680249,VS0,VE0 Vary: Authorization,Accept-Encoding,Origin Access-Control-Allow-Origin: * X-Fastly-Request-ID: 9cc769d5c6e06fa7a2b3dd1d9f39dd18e6512588 Expires: Thu, 18 Aug 2022 02:02:10 GMT Source-Age: 5

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49715	185.199.109.133	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

[illegible]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49706	185.199.108.133	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:08 UTC	55	OUT	OPTIONS /drgreenthumb93/CVE-2022-30190-follina/ 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: raw.githubusercontent.com
2022-08-18 01:57:08 UTC	56	IN	HTTP/1.1 403 Forbidden Connection: close Cache-Control: no-cache Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-Frame-Options: deny X-XSS-Protection: 0 Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline' Accept-Ranges: bytes Date: Thu, 18 Aug 2022 01:57:08 GMT Via: 1.1 varnish X-Served-By: cache-mxp6942-MXP X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1660787829.961872,VS0,VE9 Access-Control-Allow-Origin: * X-Fastly-Request-ID: 1e438572101bdeafcc9fe390762dd85dc0c41b96 Expires: Thu, 18 Aug 2022 02:02:08 GMT Vary: Authorization,Accept-Encoding transfer-encoding: chunked
2022-08-18 01:57:08 UTC	56	IN	Data Raw: 34 32 61 0d 0a Data Ascii: 42a
2022-08-18 01:57:08 UTC	56	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 0d 0a 0d 0a 48 65 6c 6c 6f 20 66 75 74 75 72 65 20 47 69 74 48 75 62 62 65 72 21 20 49 20 62 65 74 20 79 6f 75 27 72 65 20 68 65 72 65 20 74 6f 20 72 65 6d 6f 76 65 20 74 68 6f 73 65 20 6e 61 73 74 79 20 69 6e 6c 69 6e 65 20 73 74 79 6c 65 73 2c 0d 0a 44 52 59 20 75 70 20 74 68 65 73 65 20 74 65 6d 70 6c 61 74 65 73 20 61 6e 64 20 6d 61 6b 65 20 27 65 6d 20 6e 69 63 65 20 61 6e 64 20 72 65 2d 75 73 61 62 6c 65 2c 20 72 69 67 68 74 3f 0d 0a 0d 0a 50 6c 65 61 73 65 2c 20 64 6f 6e 27 74 2e 20 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 73 74 79 6c 65 67 75 69 64 65 2f 74 65 6d 70 6c 61 74 65 73 2f 32 2e 30 0d 0a 0d 0a 2d 2d 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 3c 68 65 61 64 3e 0d Data Ascii: <IDOCTYPE html>...Hello future GitHubber! I bet you're here to remove those nasty inline styles,Dry up these templates and make 'em nice and re-usable, right?Please, don't. <html> < head>">https://github.com/styleguide/templates/2.0--><html> < head>
2022-08-18 01:57:08 UTC	57	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:08 UTC	57	IN	Data Raw: 31 35 36 38 0d 0a Data Ascii: 1568
2022-08-18 01:57:08 UTC	57	IN	Data Raw: 6f 67 6f 20 7b 20 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 33 35 70 78 3b 20 7d 0d 0a 20 20 20 20 20 2e 6c 6f 67 6f 2d 69 6d 67 2d 32 78 20 7b 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 20 7d 0d 0a 20 20 20 20 20 20 40 6d 65 64 69 61 0d 0a 20 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 20 32 29 2c 0d 0a 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 20 20 20 6d 69 6e 2d 2 d 6d 6f 7a 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 20 32 29 2c 0d 0a 20 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 20 20 20 20 2d 6f 2d 6d Data Ascii: ogo { display: inline-block; margin-top: 35px; } .logo-img-2x { display: none; } @media only screen and (-webkit-min-device-pixel-ratio: 2), only screen and (min-moz-device-pixel-ratio: 2), only screen and (-o-m
2022-08-18 01:57:08 UTC	59	IN	Data Raw: 4f 46 52 76 45 35 46 75 4f 50 53 34 57 4c 53 74 37 2b 38 61 6a 76 58 63 4a 70 63 79 4e 76 68 7a 74 53 77 55 6b 54 47 67 5a 7a 39 75 44 53 78 52 6e 50 5a 77 73 6e 54 6b 71 79 37 6a 70 73 50 74 2f 41 78 79 76 6e 41 65 4a 4d 41 78 50 6e 4d 69 71 50 4a 59 49 79 7a 66 34 2f 4b 71 72 50 65 64 61 4b 35 62 49 73 51 77 66 54 6f 32 74 37 32 68 55 65 70 50 57 76 6e 36 6d 4f 38 56 6f 58 72 67 62 44 52 61 4a 58 6c 65 36 72 37 35 46 7a 5a 6d 37 53 32 54 6e 79 54 4e 55 5 8 76 35 65 69 44 41 41 36 6a 30 57 6d 4b 79 57 76 35 31 6c 69 52 41 41 43 6a 50 30 4f 5a 4e 56 75 77 61 34 4c 2b 75 51 41 63 77 2f 53 69 4e 47 48 35 37 6d 49 78 78 50 4b 6d 55 33 44 67 70 4c 32 73 58 33 72 75 74 63 33 2f 76 68 39 67 75 31 44 33 74 4e 45 41 74 76 4f 53 4b 56 41 6d 78 66 61 67 52 6d 62 6e Data Ascii: OFRvE5FuOPS4WLSi7+8ajvXcJpcyNvhztSwUkTGgZz9uDSxRnPWZwsnTkqy7jpsPt/AxyvnAeJMAxPnMiqPJYlyzf4/KqrPedaK5blsQwfT02t72hUepPWvn6mO8VoXrgbDRaJXle6r75FzZm7S2TnyTNUXv5eiDAA6j0WmKyWv51liRAACJP0OZNVuwa4L+uQAacw/SiNGH57mlxxPKmU3DgpL2sX3rutc3/vh9gu1D3tNEAtvOSKVAmxfagRmbn

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:09 UTC	72	OUT	HEAD /drgreenthumb93/CVE-2022-30190-follina/main/bad.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: raw.githubusercontent.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:09 UTC	72	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 14 Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline'; sandbox Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-Frame-Options: deny X-XSS-Protection: 1; mode=block Content-Type: text/plain; charset=utf-8 X-GitHub-Request-Id: 7924:06B9:5187D0:55A96E:62FD9C71 Accept-Ranges: bytes Date: Thu, 18 Aug 2022 01:57:09 GMT Via: 1.1 varnish X-Served-By: cache-mxp6955-MXP X-Cache: HIT X-Cache-Hits: 1 X-Timer: S1660787830.535497,VS0,VE0 Vary: Authorization,Accept-Encoding,Origin Access-Control-Allow-Origin: * X-Fastly-Request-ID: 4aa7bf1bd86ec554d4344a3b644d235210eff816 Expires: Thu, 18 Aug 2022 02:02:09 GMT Source-Age: 4

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49709	185.199.109.133	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:09 UTC	73	OUT	HEAD /drgreenthumb93/CVE-2022-30190-follina/main/bad.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: raw.githubusercontent.com Connection: Keep-Alive
2022-08-18 01:57:09 UTC	73	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 14 Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline'; sandbox Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-Frame-Options: deny X-XSS-Protection: 1; mode=block Content-Type: text/plain; charset=utf-8 X-GitHub-Request-Id: 7924:06B9:5187D0:55A96E:62FD9C71 Accept-Ranges: bytes Date: Thu, 18 Aug 2022 01:57:09 GMT Via: 1.1 varnish X-Served-By: cache-mxp6925-MXP X-Cache: HIT X-Cache-Hits: 1 X-Timer: S1660787830.792096,VS0,VE1 Vary: Authorization,Accept-Encoding,Origin Access-Control-Allow-Origin: * X-Fastly-Request-ID: 8f764b5df9319996b8b6c3a33902dda0dd52d219 Expires: Thu, 18 Aug 2022 02:02:09 GMT Source-Age: 4

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49710	185.199.108.133	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:09 UTC	74	OUT	OPTIONS /drgreenthumb93/CVE-2022-30190-follina/main/ 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: raw.githubusercontent.com

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:09 UTC	74	IN	HTTP/1.1 403 Forbidden Connection: close Cache-Control: no-cache Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-Frame-Options: deny X-XSS-Protection: 0 Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline' Accept-Ranges: bytes Date: Thu, 18 Aug 2022 01:57:09 GMT Via: 1.1 varnish X-Served-By: cache-mxp6950-MXP X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1660787830.911926,VS0,VE9 Access-Control-Allow-Origin: * X-Fastly-Request-ID: 90f3b6f9be95938ba8c5b82af688f9434fb26d83 Expires: Thu, 18 Aug 2022 02:02:09 GMT Vary: Authorization,Accept-Encoding transfer-encoding: chunked
2022-08-18 01:57:09 UTC	75	IN	Data Raw: 34 32 61 0d 0a Data Ascii: 42a
2022-08-18 01:57:09 UTC	75	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 0d 0a 0d 0a 48 65 6c 6c 6f 20 66 75 74 75 72 65 20 47 69 74 48 75 62 62 65 72 21 20 49 20 62 65 74 20 79 6f 75 27 72 65 20 68 65 72 65 20 74 6f 20 72 65 6d 6f 76 65 20 74 68 6f 73 65 20 6e 61 73 74 79 20 69 6e 6c 69 6e 65 20 73 74 79 6c 65 73 2c 0d 0a 44 52 59 20 75 70 20 74 68 65 73 65 20 74 65 6d 70 6c 61 74 65 73 20 61 6e 64 20 6d 61 6b 65 20 27 65 6d 20 6e 69 63 65 20 61 6e 64 20 72 65 2d 75 73 61 62 6c 65 2c 20 72 69 67 68 74 3f 0d 0a 0d 0a 50 6c 65 61 73 65 2c 20 64 6f 6e 27 74 2e 20 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 73 74 79 6c 65 67 75 69 64 65 2f 74 65 6d 70 6c 61 74 65 73 2f 32 2e 30 0d 0a 0d 0a 2d 2d 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 3c 68 65 61 64 3e 0d Data Ascii: <!DOCTYPE html>...Hello future GitHubber! I bet you're here to remove those nasty inline styles,DRY up these templates and make 'em nice and re-usable, right?Please, don't. ">https://github.com/styleguide/templates/2.0--> <html> < head>
2022-08-18 01:57:09 UTC	76	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:09 UTC	76	IN	Data Raw: 61 62 34 0d 0a Data Ascii: ab4
2022-08-18 01:57:09 UTC	76	IN	Data Raw: 6f 67 6f 20 7b 20 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 33 35 70 78 3b 20 7d 0d 0a 20 20 20 20 20 2e 6c 6f 67 6f 2d 69 6d 67 2d 32 78 20 7b 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 20 7d 0d 0a 20 20 20 20 20 20 20 20 40 6d 65 64 69 61 0d 0a 20 20 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 20 32 29 2c 0d 0a 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 20 20 20 6d 69 6e 2d 2 d 6d 6f 7a 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 20 32 29 2c 0d 0a 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 20 20 20 20 2d 6f 2d 6d Data Ascii: ogo { display: inline-block; margin-top: 35px; } .logo-img-2x { display: none; } @media only screen and (-webkit-min-device-pixel-ratio: 2), only screen and (min--moz-device-pixel-ratio: 2), only screen and (-o-m
2022-08-18 01:57:09 UTC	77	IN	Data Raw: 4f 46 52 76 45 35 46 75 4f 50 53 34 57 4c 53 74 37 2b 38 61 6a 76 58 63 4a 70 63 79 4e 76 68 7a 74 53 77 55 6b 54 47 67 5a 7a 39 75 44 53 78 52 6e 50 5a 77 73 6e 54 6b 71 79 37 6a 70 73 50 74 2f 41 78 79 76 6e 41 65 4a 4d 41 78 50 6e 4d 69 71 50 4a 59 49 79 7a 66 34 2f 4b 71 72 50 65 64 61 4b 35 62 49 73 51 77 66 54 6f 32 74 37 32 68 55 65 70 50 57 76 6e 36 6d 4f 38 56 6f 58 72 67 62 44 52 61 4a 58 6c 65 36 72 37 35 46 7a 5a 6d 37 53 32 54 6e 79 54 4e 55 5 8 76 35 65 69 44 41 41 36 6a 30 57 6d 4b 79 57 76 35 31 6c 69 52 41 41 43 6a 50 30 4f 5a 4e 56 75 77 61 34 4c 2b 75 51 41 63 77 2f 53 69 4e 47 48 35 37 6d 49 78 78 50 4b 6d 55 33 44 67 70 4c 32 73 58 33 72 75 74 63 33 2f 76 68 39 67 75 31 44 33 74 4e 45 41 74 76 4f 53 4b 56 41 6d 78 66 61 67 52 6d 62 6e Data Ascii: OFRvE5FuOPS4WLSi7+8ajvXcJpcyNvhztSwUkTGgZz9uDsxRnRPNzwsnTkqy7jpsPt/AxyvnAeJMAxPnMiqPJYlyzf4/KqrPedaK5bIsQwfTo2t72hUepPWvn6mO8VoXrgbDRaJXle6r75FzZm7S2TnyTNUXv5eiDAA6j0WmKyWv51liRAACJP0OZNVuwa4L+uQAchwSiNGH57mlxxPKmU3DgpL2sX3rutc3/vh9gu1D3tNEAtvOSKVAmxagRmbn
2022-08-18 01:57:09 UTC	78	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:09 UTC	78	IN	Data Raw: 61 62 34 0d 0a Data Ascii: ab4
2022-08-18 01:57:09 UTC	78	IN	Data Raw: 4f 4a 77 75 5a 67 39 62 31 6a 66 33 67 51 52 37 72 36 57 31 6b 54 53 63 51 70 46 6a 50 78 4b 4f 77 44 67 41 49 55 7a 79 7a 51 4f 51 52 59 4d 79 64 6b 7a 49 37 59 5a 62 69 64 44 6b 63 54 6b 55 4b 51 57 61 7a 4f 65 69 74 58 46 39 68 42 77 35 53 5a 63 69 5a 4f 69 39 54 36 47 6e 6b 4d 70 30 75 4b 79 6d 51 6b 44 48 48 41 78 7a 4d 4c 77 63 53 4d 2b 65 5a 4a 71 57 68 73 6b 68 4f 4d 69 76 44 44 73 63 49 43 35 6f 68 79 57 2b 78 31 6c 54 6d 35 36 2b 76 32 44 6b 47 4 7 6c 7a 39 46 53 45 6e 79 6e 52 64 67 50 4b 55 6c 65 7a 54 43 53 54 65 34 7a 47 6e 5a 66 73 56 74 6d 57 54 33 34 6b 6c 6a 41 6d 4a 67 41 62 42 53 45 75 59 79 51 49 6a 4c 6e 67 6e 6b 4c 42 55 67 6b 4a 46 59 36 50 64 62 67 63 4b 61 45 78 54 66 7a 34 38 46 6e 78 61 61 6e 78 38 66 47 70 36 68 6c 59 31 66 76 Data Ascii: OJwuZg9b1f3gQR7r6W1kTScQpFjPxKOWDgAIUzyzQQQRYMYdkzl7YZbidDkcTkUKQWazOeitXF9hBwSSZciZOi9T6GnkMp0uKymQkDHHAxzMLwcSM+eZJqWhshkOmiVDDscIC5ohyW+xlITm56+v2DkGGIz9FSEynRdgPKUlezTCSTe4zGnZfsVtmWT34kljAmJgAbBSEuYyQljlNgnkLBUgkJFY6PdbgcaExTfz48Fnxaanx8fGp6hY1fv
2022-08-18 01:57:09 UTC	80	IN	Data Raw: 4c 51 41 67 44 51 31 6c 56 52 37 67 34 6f 63 43 4d 32 65 2b 37 31 46 64 32 4b 66 48 4a 42 34 32 73 76 46 77 7a 70 4b 67 41 7a 45 4e 56 6e 59 52 37 2f 64 62 68 7a 49 79 66 4e 64 61 7a 43 4b 42 30 52 70 37 38 35 4a 41 34 71 39 73 57 4c 39 2b 73 70 4b 69 35 65 68 66 76 52 62 30 63 46 76 72 4b 30 4a 34 75 2b 64 33 70 6d 56 47 52 6c 77 31 73 47 38 70 74 37 61 6b 75 70 67 30 4b 6b 45 5a 73 5a 2f 66 39 45 64 65 61 38 42 68 43 51 79 33 37 69 41 70 43 69 43 52 2f 33 4b 4d 56 31 49 5a 79 64 32 56 2b 73 6c 79 59 6e 34 45 61 30 48 56 35 4d 69 4e 77 61 7a 52 6c 67 53 55 6d 58 42 41 79 34 72 66 56 71 42 34 4c 2b 76 53 49 36 53 38 71 34 43 32 2f 77 61 68 42 4b 2f 4a 79 48 39 2b 2f 4a 62 77 6a 6d 68 55 68 63 34 68 4d 39 4b 54 6b 65 45 64 5a 6f 35 6a 36 70 6a 34 77 77 6b Data Ascii: LQAgDQ1IVR7g4ocCM2e+71Fd2KfHJB42svFwzpKgAzENVnYR7f/dbhzlyfNdazCKB0Rp785JA4q9sWL9+spKi5ehfvRb0cFvrK0J4u+d3pmVGRlw1sG8pt7akupg0KkEZsZ/f9Edea8BhCQy37iApCiCR/3KMV1IZyd2V+slyYn4Ea0HV5MiNwazRlgSUMXBAy4rfVqB4L+vSI6S8q4C2/wahBK/JyH9+JbwjmhUhc4hM9KtkeEdZo5j6pj4wwk

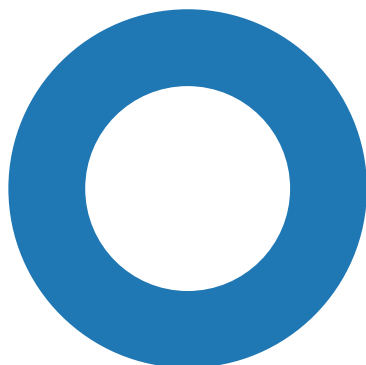
Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:09 UTC	81	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:09 UTC	81	IN	Data Raw: 61 62 34 0d 0a Data Ascii: ab4
2022-08-18 01:57:09 UTC	81	IN	Data Raw: 50 36 30 55 2b 49 53 4f 45 67 41 65 41 31 49 38 68 71 75 73 68 76 54 4f 48 45 69 31 59 53 54 67 51 37 37 50 5a 49 34 71 4d 74 58 4f 31 4d 33 2f 36 31 4b 6c 69 4f 30 58 31 69 37 43 55 53 4c 56 6a 4b 32 73 76 61 34 38 51 6f 6a 72 45 6a 57 57 78 49 79 67 37 51 54 67 49 53 51 7a 74 52 6f 76 56 34 6e 43 49 4a 79 54 4a 6a 54 45 4a 4c 4a 39 49 69 62 4e 54 35 32 71 72 6a 4a 50 69 34 49 74 71 6f 66 51 6e 44 4f 73 7a 78 73 38 62 79 43 77 49 63 52 78 35 4a 62 61 53 49 67 6d 47 34 6d 46 50 59 69 53 30 42 6b 56 57 50 48 6e 72 42 4f 75 46 5a 42 36 45 70 4c 37 66 41 44 4b 57 63 78 49 68 76 61 6f 76 49 6f 61 41 78 38 48 44 41 38 4d 49 4a 42 61 52 62 42 57 66 4c 72 61 54 6e 54 52 65 31 48 53 63 66 78 6c 51 65 46 44 68 41 49 37 72 51 49 35 7a 38 77 41 4f 70 43 39 4f 48 48 Data Ascii: P60U+ISOEgAeA1I8hqushvTOHEi1YSTgQ77PZI4qMtXO1M3/61KliO0X1i7CUSLVjK2sva48QojrEjWWxlyg7QTgISQztRovV4nClJyTjTEJLJ9libNT52qrjJPi4ltqofQnDOszxs8byCwlcRx5JbaSIgmG4mFPYiS0BkVWPHnrBOuFZB6EpL7fADKWcxlhvaovloaAx8HDA8MIJBaRbBWfLraTnTRe1HScfxlQeFDhAI7rQI5z8wAOpC9OHH
2022-08-18 01:57:09 UTC	83	IN	Data Raw: 6b 57 49 44 71 52 71 50 42 42 69 45 64 48 4b 71 71 41 79 5a 50 6a 36 50 67 41 42 6b 66 64 61 52 74 79 63 53 48 38 78 67 41 43 4a 66 59 77 77 52 44 44 52 6f 5a 51 74 7a 6e 2f 2b 2b 66 7a 46 69 38 76 4b 68 4b 6c 4d 4a 49 31 4c 4e 4a 7a 49 4b 46 39 74 6c 55 45 46 55 76 66 4f 6d 71 4c 56 71 31 63 45 46 66 37 66 6a 42 30 51 45 30 39 53 6d 55 71 6b 70 41 42 49 43 6e 6f 4c 43 67 70 4f 35 51 55 56 4a 4d 53 4b 39 46 31 62 77 43 61 6b 74 58 35 47 6b 73 69 57 6f 36 74 30 33 55 41 67 57 6f 78 61 71 77 4b 5a 64 48 4b 58 67 4e 77 6e 6a 64 37 2b 53 38 38 77 49 79 49 71 6b 47 4a 78 58 31 78 73 38 43 69 47 78 6e 73 77 50 42 7a 76 76 6a 51 71 5a 57 55 62 4e 6d 79 6f 34 39 71 77 51 57 65 69 50 37 73 42 31 51 6e 48 45 6b 45 46 57 4b 70 72 6f 4f 6f 69 6e 6a 61 76 50 6a 49 69 Data Ascii: kWIDqRqPBBIEdHKqQyZPJ6PgABkfdaRtycSH8xgACJfYwwRDDRoZQtzn/++fzFi8vKhKIMJI1LNJzIKF9tIUeFUvOmqlVq1cEFF7fjB0QE09SmUqkpABICnoLCgpO5QUVJMSK9F1bwCaktX5GksiWo6t03UAgWoxaqwKZdHKXgNwnjd7+S88wlylqkGJxX1xs8CiGxnsWPBzvvjQqZWUbNmyo49qwQWeiP7sB1QnHEkEFWKproOoinjavPjli
2022-08-18 01:57:09 UTC	84	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:09 UTC	84	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:57:09 UTC	84	IN	Data Raw: 54 54 4f 4a 38 59 56 6c 5a 4f 2b 2f 49 41 34 70 34 45 6e 76 44 4e 6c 5a 59 2f 55 45 4a 35 6b 48 79 70 45 34 52 45 4a 4e 36 7a 4a 69 4d 4e 63 51 6d 57 45 68 70 71 59 31 37 4c 54 4b 53 32 68 4a 6b 58 57 36 6d 31 69 51 50 50 34 6b 51 59 58 64 64 35 7a 6f 4d 4d 64 50 46 6a 55 30 36 44 7a 63 34 47 54 7a 77 43 45 43 71 39 6e 63 65 32 2b 51 50 76 55 68 41 71 71 4c 57 78 47 75 6b 62 47 2f 62 47 30 4d 75 5a 67 42 42 71 72 57 48 71 68 45 35 5a 4f 30 41 6b 54 45 65 5 3 4d 4b 67 52 46 4d 68 48 6c 39 2f 66 61 59 77 56 2f 56 64 47 38 72 47 5a 32 41 61 69 2f 4f 71 43 6e 4e 7a 38 52 52 38 46 73 53 66 46 55 59 42 72 56 68 52 59 33 55 6f 45 74 58 73 58 73 62 46 57 2b 2b 78 42 6d 4a 30 47 70 4d 43 50 50 75 31 67 49 6a 4e 56 74 72 56 61 30 4e 63 4a 2b 46 52 45 58 50 7a 77 6a Data Ascii: TTOJ8YVIZO+/IA4p4EnvDNIZY/UEJ5kHypE4REJN6zJiMNcQmWEhpgY17LTKS2hJkXW6m1iQPP4kQYXdd5zoMMdPFJjU06Dzc4GTzwCECq9nce2+QPvUhAqLWxGukbG/bG0MuZgBBqrWHqhE5Z00AKTEeSMKgR FMhHl9/faYwV/VdG8rGZZAai/OqCnNz8RR8FsSfFUYBrVhRY3UoEtXsXsbfW++xBmJ0GpMCPPu1gljNVtrVa0NcJ+F REXP2wj
2022-08-18 01:57:09 UTC	85	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:57:09 UTC	85	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49711	185.199.108.133	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:57:10 UTC	85	OUT	HEAD /drgreenthumb93/CVE-2022-30190-follina/main/bad.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: raw.githubusercontent.com

Statistics

Behavior



● WINWORD.EXE
● MSOSYNC.EXE



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 5828, Parent PID: 796

General

Target ID:	0
Start time:	03:56:59
Start date:	18/08/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x320000
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: 5700, Parent PID: 5828

General

Target ID:	1
Start time:	03:57:04
Start date:	18/08/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe
Imagebase:	0x960000
File size:	466688 bytes

MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol
----------	------------	-------	----------------	--------

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

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

Disassembly

 No disassembly