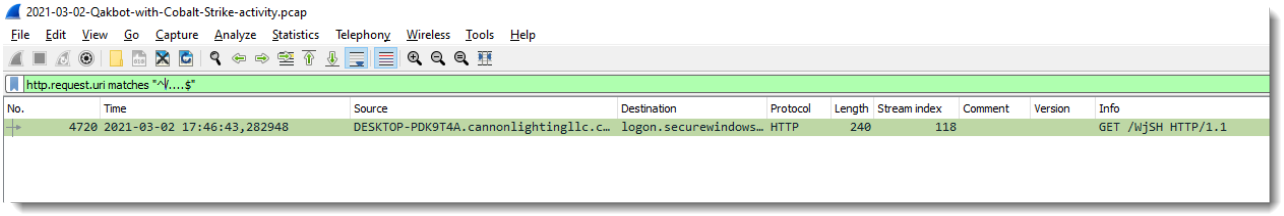
PCAPs and Beacons - SANS Internet Storm Center

By SANS Internet Storm Center

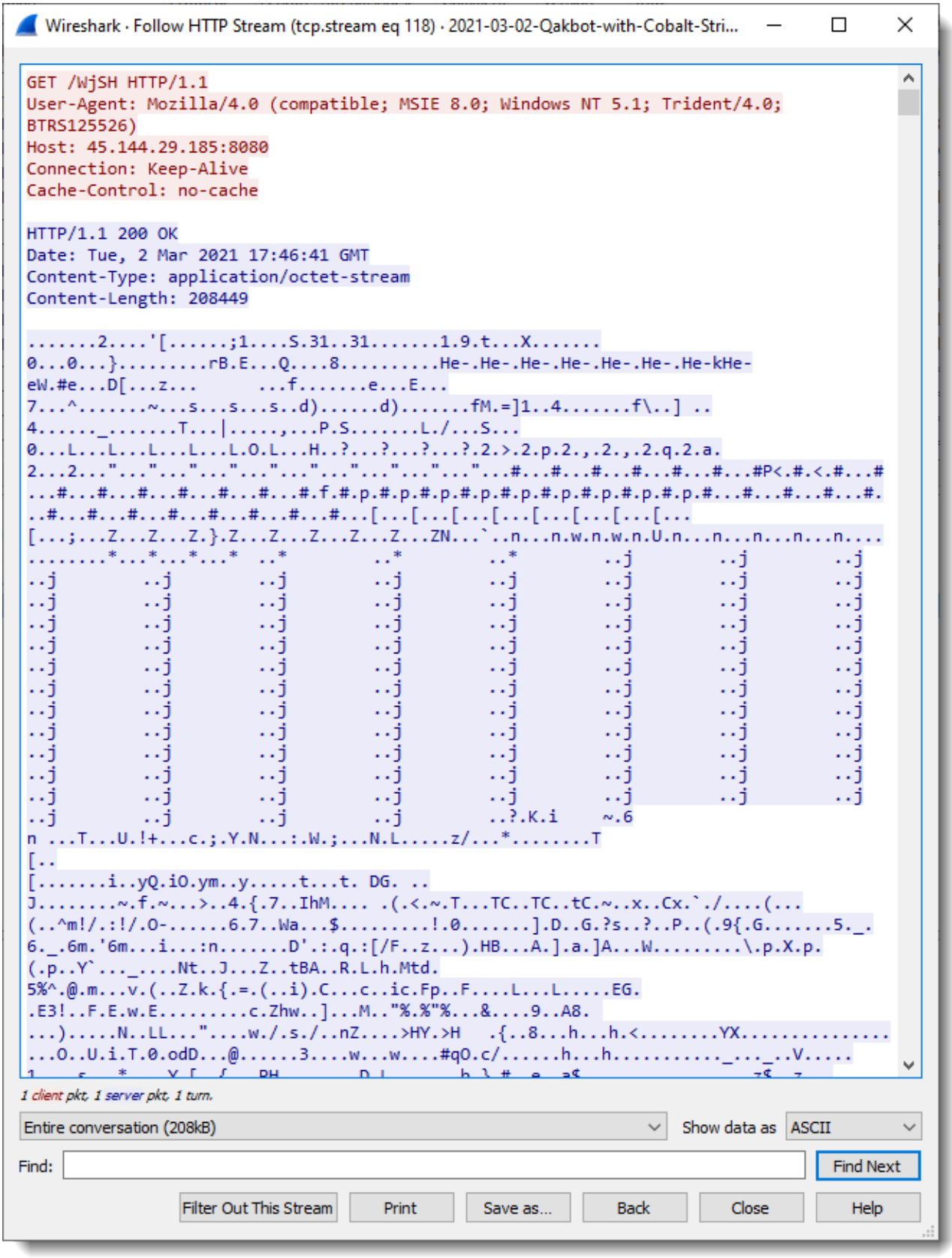
Archived: 2026-04-05 13:56:21 UTC

I like taking a closer look at captures files posted by Brad. In his latest diary entry, we have a capture file with Cobalt Strike traffic.

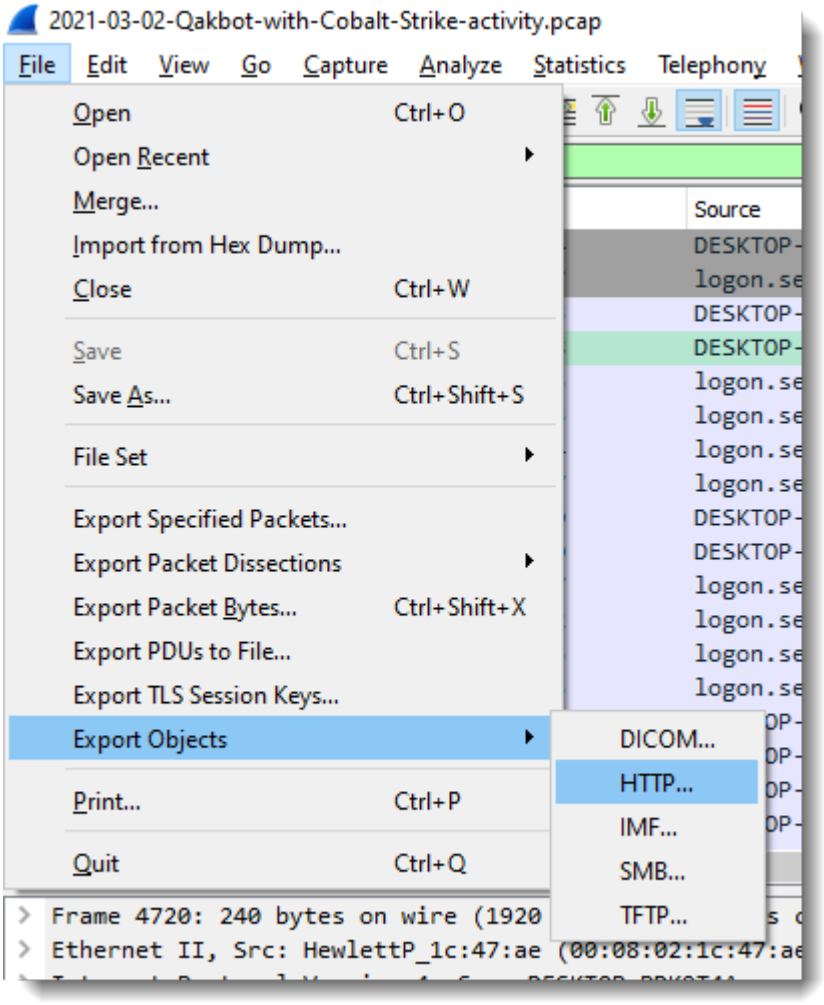
With regular expression "^/....$" I look for URIs that are typical for Cobalt Strike shellcode (and Metasploit too):

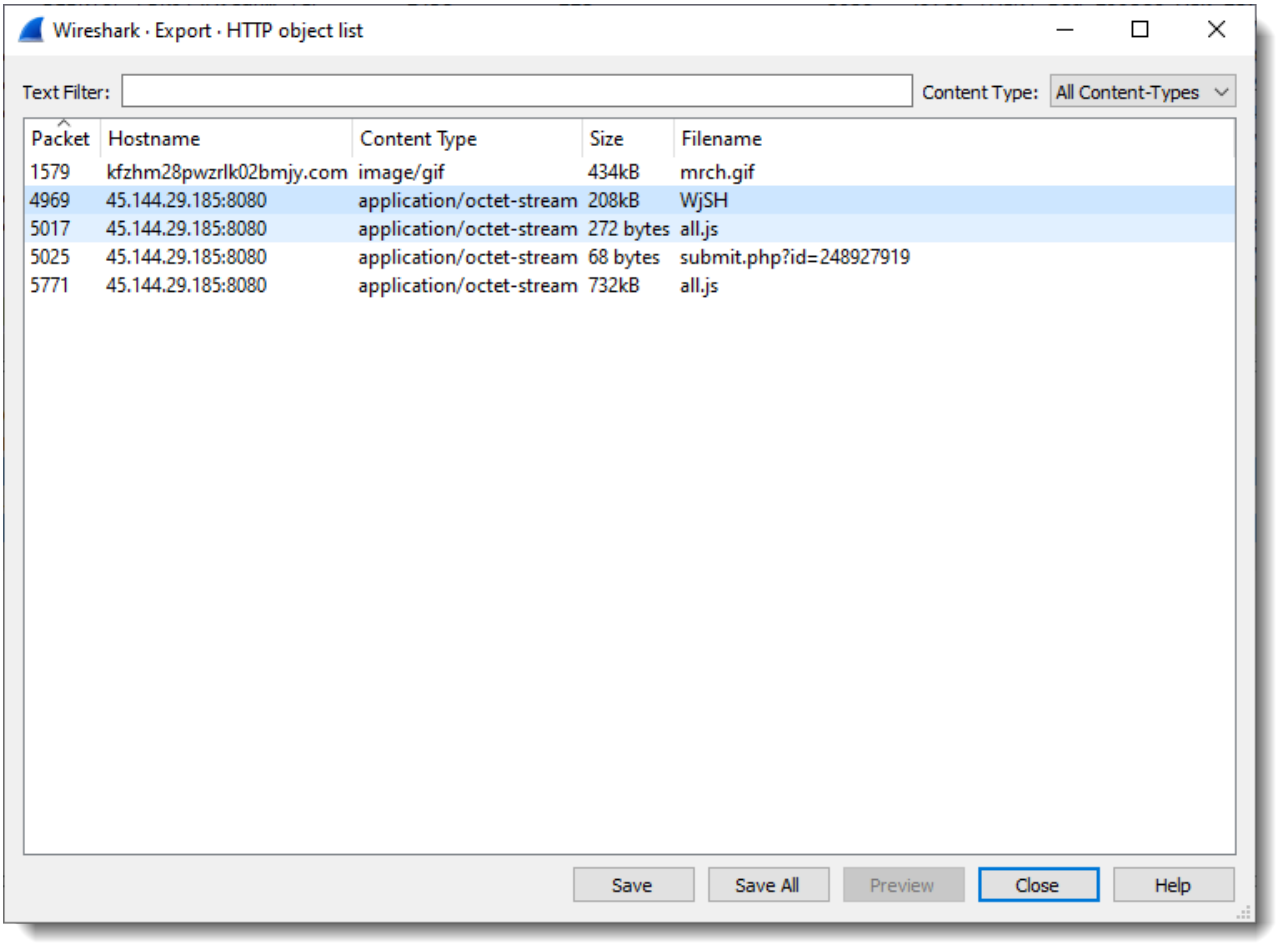


Following this HTTP stream, I see data that looks encoded and has some repetitions, so this might be some kind of XOR encoding:

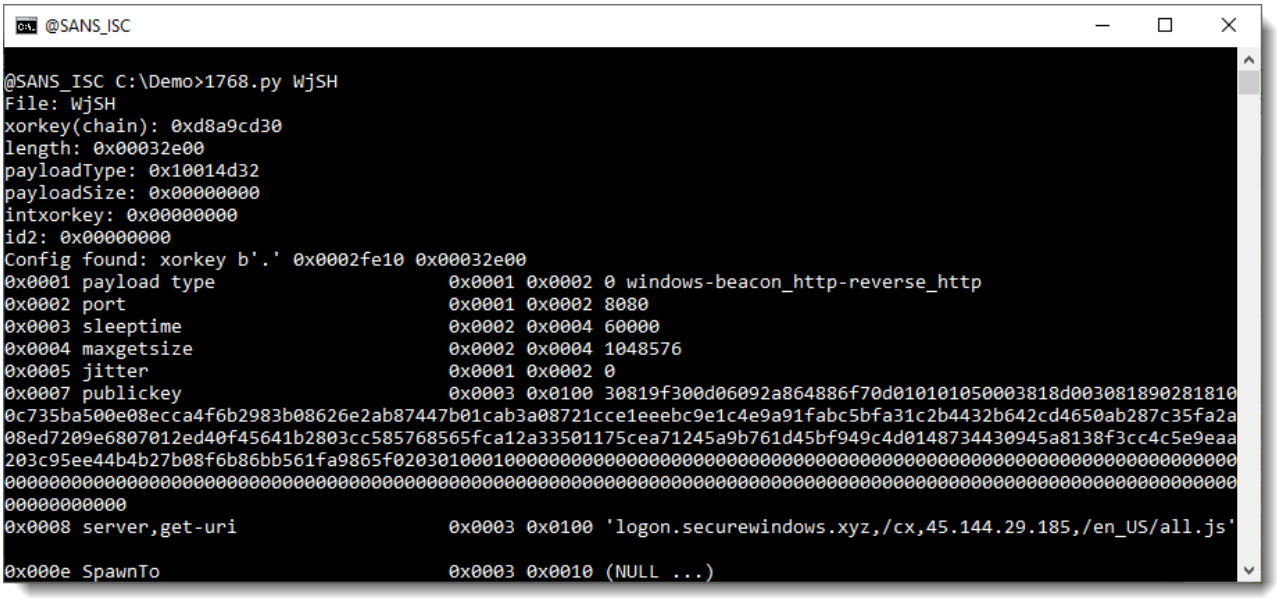


I export this data stream as a file:


2021-03-02-Qakbot-with-Cobalt-Strike-activity.pcap
File Edit View Go Capture Analyze Statistics Telephony
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
HTTP...
IMF...
SMB...
TFTP...
Source
DESKTOP-
logon.se
Frame 4720: 240 bytes on wire (1920
Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae



Then pass it through my [1768.py] Cobalt Strike beacon analysis tool:



And this is indeed the configuration of a beacon.

Didier Stevens

Senior handler

Microsoft MVP
blog.DidierStevens.com DidierStevensLabs.com
