2022-08-31 (WEDNESDAY) - ICEDID (BOKBOT) WITH COBALT STRIKE

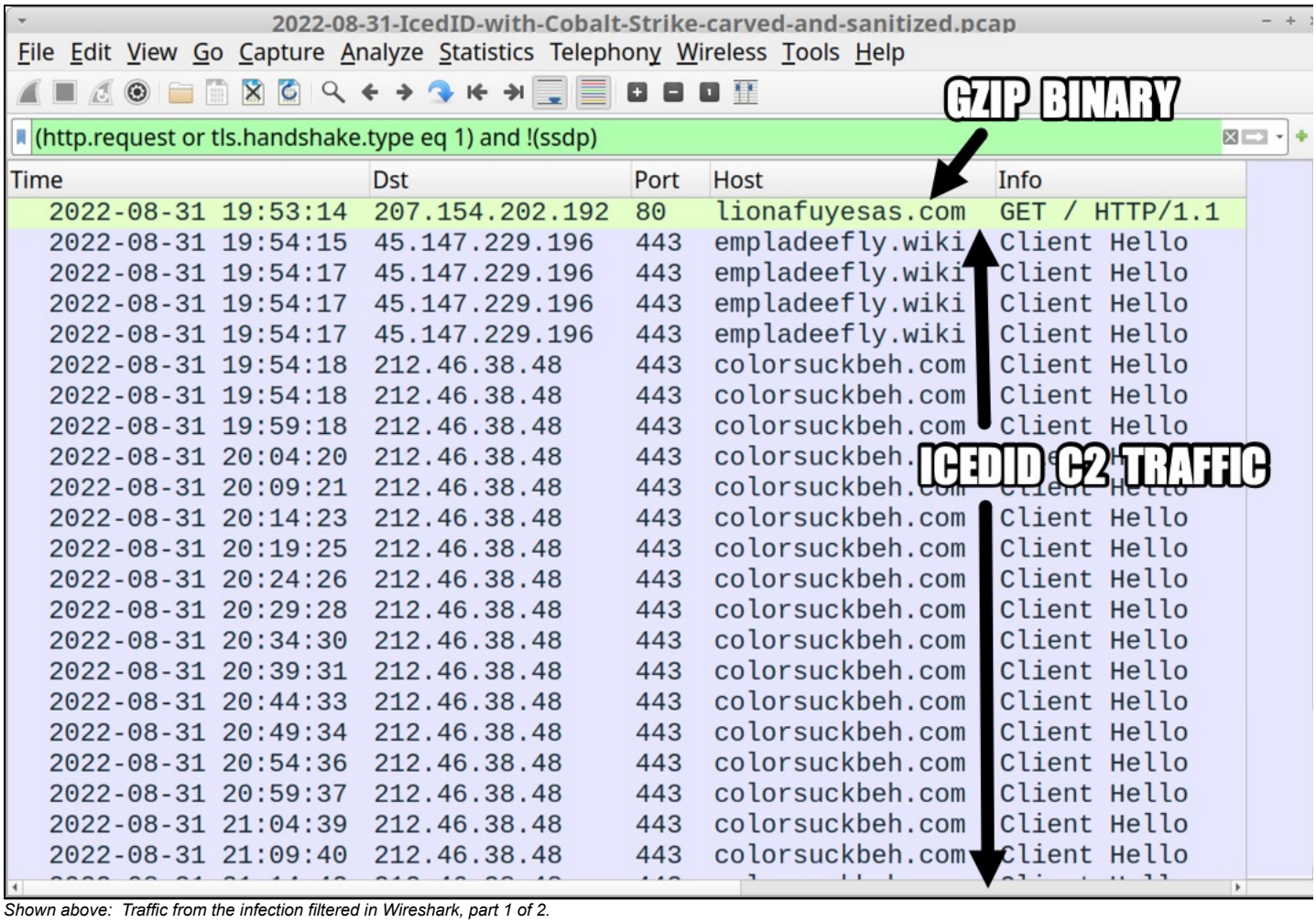
NOTES:

- Started the infection on Wednesday 2022-08-31 and saw Cobalt Strike the next day, more than 17 hours later, on Thursday 2022-09-01.
- Zip files are password-protected. If you don't know the password, see the "about" page of this website.

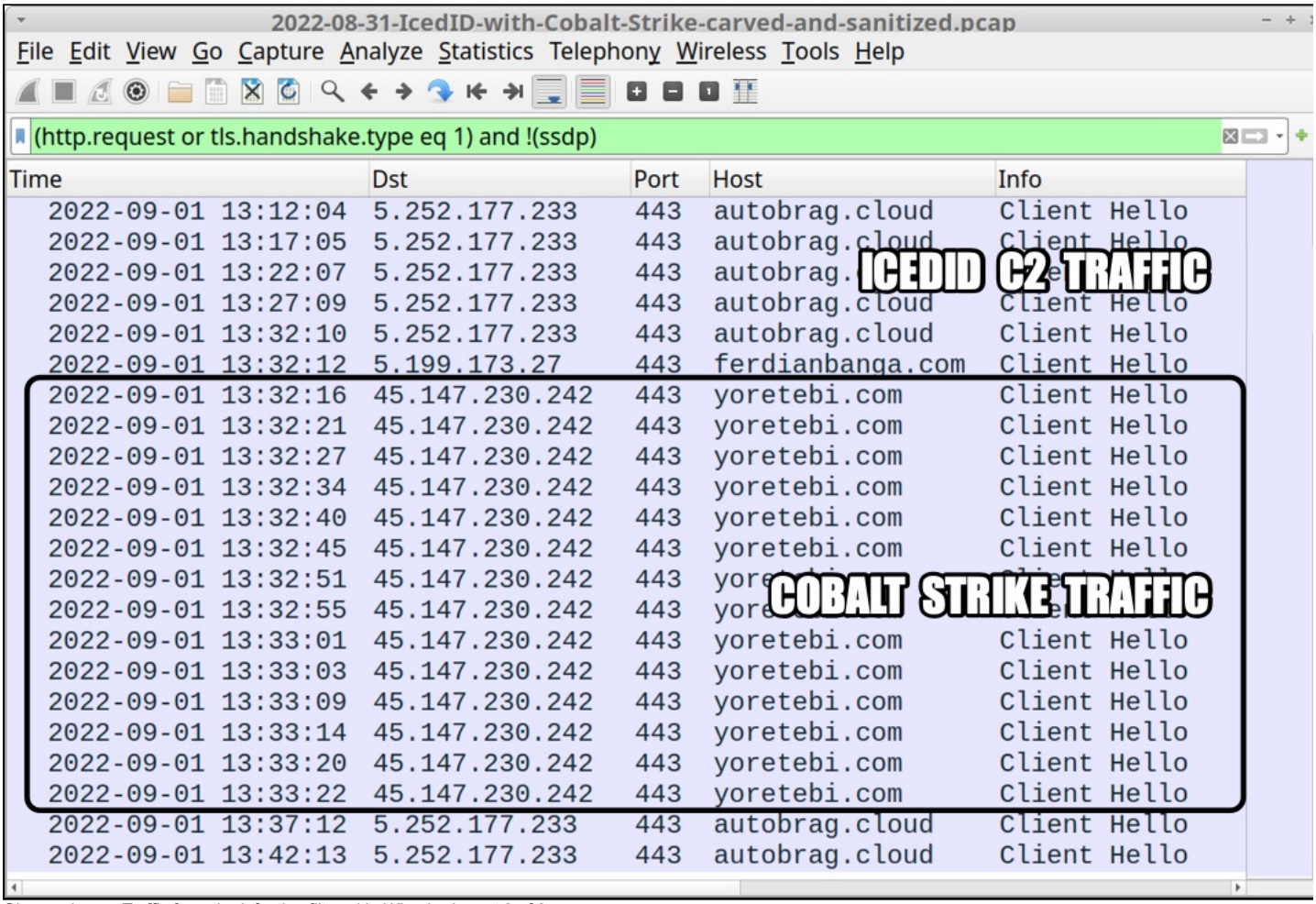
ASSOCIATED FILES:

- **2022-08-31-IcedID-with-Cobalt-Strike-carved-and-sanitized.pcap.zip** 1.7 MB (1,713,677 bytes)
- **2022-08-31-IcedID-malware-and-artifacts.zip** 1.5 MB (1,538,604 bytes)

IMAGES



Shown above: Traffic from the infection filtered in Wireshark, part 1 of 2.



Shown above: Traffic from the infection filtered in Wireshark, part 2 of 2.

INDICATORS

INFECTION TRAFFIC:

HTTP TRAFFIC FOR GZIP BINARY:

- 207.154.202.192 port 80 - **lionafuyesas.com** - GET / HTTP/1.1

ICEDID C2:

- 45.147.229.196 port 443 - **empladeefly.wiki** - HTTPS traffic
- 212.46.38.48 port 443 - **colorsuckbeh.com** - HTTPS traffic
- 128.199.120.41 port 443 - **dromfiregreti.com** - HTTPS traffic
- 5.252.177.233 port 443 - **autobrag.cloud** - HTTPS traffic
- 5.199.173.27 port 443 - **ferdianbanga.com** - HTTPS traffic

COBALT STRIKE C2:

- 45.147.230.242 port 443 - **yoretebi.com** - HTTPS traffic

MALWARE AND ARTIFACTS:

PASSWORD PROTECTED ZIP AND EXTRACTED ISO:

- SHA256 hash: 9977013ff25deb2c9162232b3f0a82136b4d10d63161e1ddc8696c26bfdf0025
- File size: 114,431 bytes
- File name: Invoice_unpaid_08-31_documents_265.zip
- File description: Password-protected zip archive
- Password: 35942

- SHA256 hash: 272221763511b6eb09d62e9b18b48b682eb7940cdc7206c2bee472b46f4a6943
- File size: 1,900,544 bytes
- File name: Invoice_unpaid_08-31_documents_265.iso
- File description: ISO image extracted from password-protected zip archive

CONTENTS OF ISO IMAGE:

- SHA256 hash: 2c4c46deadeee55e74cbdf788485b418397c3bbfc599c0126beb2d211f538ce1
- File size: 1,218 bytes
- File location in ISO image: Document.lnk
- File description: Windows shortcut, only visible file in ISO image

- SHA256 hash: 604fb39be96c1d28c3b0d8e34c270059e2a4452782fa7f211a825e1761ea8497

- File size: 1,167 bytes
- File location in ISO image: sad\lexicon.bat
- File description: Batch file run by above Windows shortcut

- SHA256 hash: 38fa1fc2a23d94e17784eb807d98bb836713aec7db1c28aad0ab4b6e5764bf7e
- File size: 421,376 bytes
- File location in ISO image: sad\dumbfoundering.dll
- File description: 64-bit DLL installer for IcedID run by the above batch file
- Run method: rundll32.exe *[filename]*,#1

FILES SEEN FOR THIS INFECTION:

- SHA256 hash: 338065f662d4096f2d6abc94e93c1d706404aad4ce4b192b4f295437c6f42b38
- File size: 754,107 bytes
- File location: hxxp://lionafuyesas.com/
- File description: Gzip file retrieved by IcedID DLL installer, used to create licence.dat & persistent IcedID DLL

- SHA256 hash: 1de8b101cf9f0fabc9f086bddb662c89d92c903c5db107910b3898537d4aa8e7
- File size: 342,218 bytes
- File location: C:\Users*[username]*\AppData\Roaming\ErodeWeb\license.dat
- File description: data binary used to run persistent IcedID DLL
- Note: First submitted to VirusTotal on 2022-07-15
- Note: Different directory name under *AppData**Roaming*\ for each infection

- SHA256 hash: 3e8db60887adfbf7af20f7611b527f11620785e9eaeac188b0758c7ba82d3cf3
- File size: 411,136 bytes
- File location: C:\Users*[username]*\AppData\Local\acucri*[username]*\Epukcb1.dll
- File description: Persistent 64-bit DLL for IcedID
- Run method: rundll32.exe *[filename]*,#1 --feul="*[path to license.dat]*"
- Note: Different file hash for each infection
- Note: Different filename and directory path under *AppData**Local*\ or *AppData**Roaming*\ for each infection

Click here to return to the main page.
