IcedID (Bokbot) with Dark VNC and Cobalt Strike - SANS ISC

By SANS Internet Storm Center

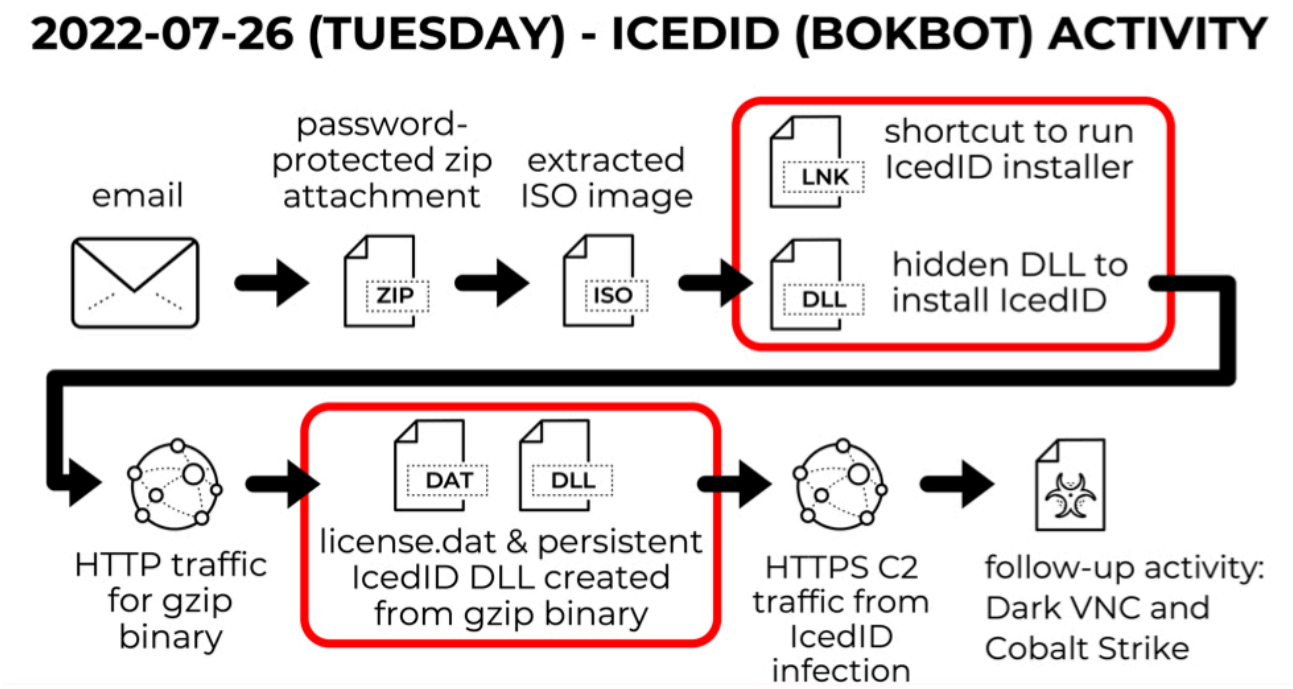
Archived: 2026-04-05 17:38:21 UTC

Introduction

As early as April 2022, a long-running threat actor known as **TA551** (designated by Proofpoint), **Monster Libra** (designated by Palo Alto Networks), or Shathak (??) started distributing **SVCReady** malware. Since then, we've sometimes seen this same threat actor also push IcedID (Bokbot) malware.

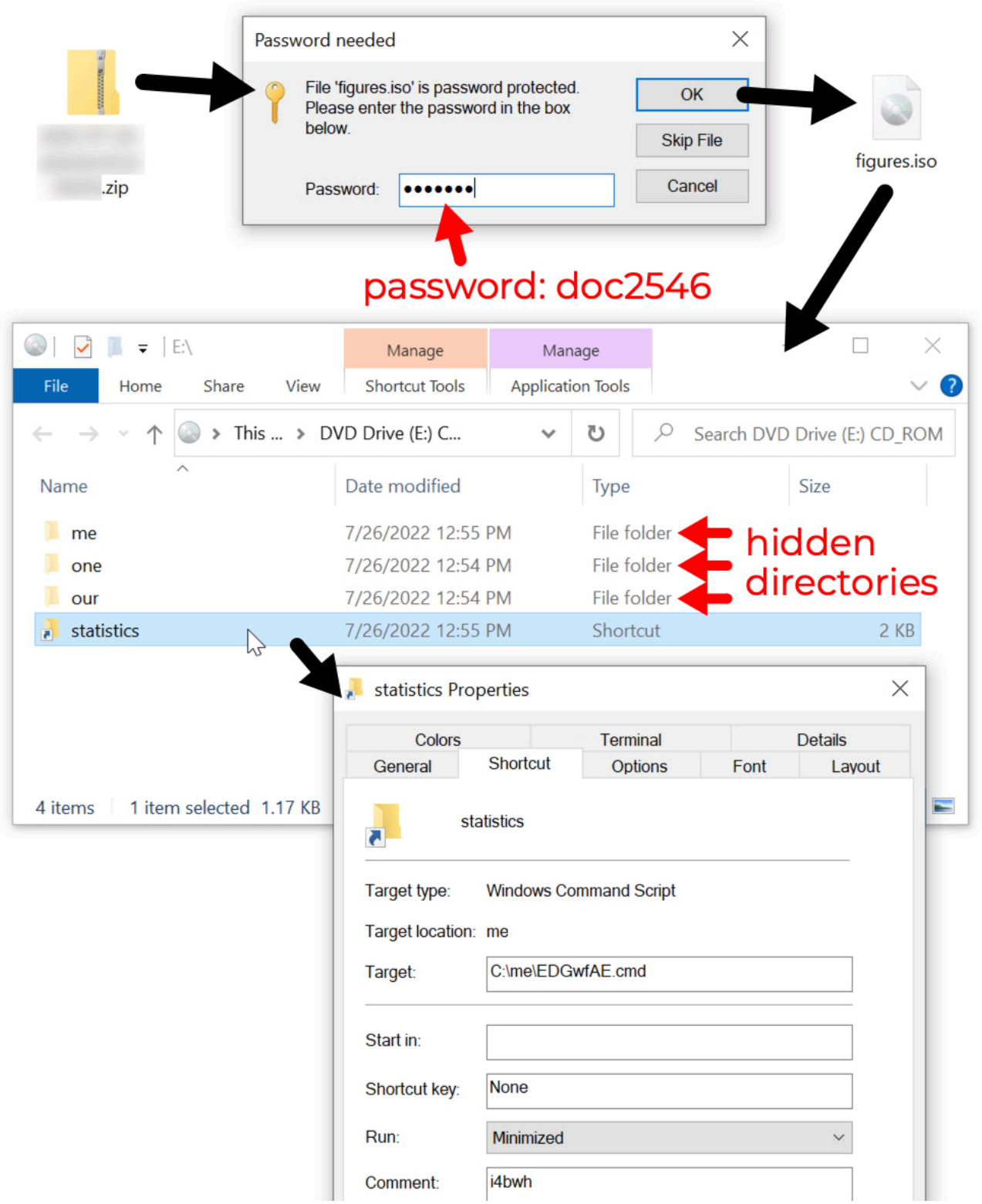
On Tuesday 2022-07-26 during a recent **wave of SVCReady malware** from Monster Libra/TA551 targeting Italy, **@k3dg3** tweeted indicators of **IcedID malware from the same threat actor**.

Today's diary reviews an IcedD infection generated from a password-protected zip archive sent by Monster Libra/TA551. This IcedID infection led to Dark VNC activity and Cobalt Strike malware.

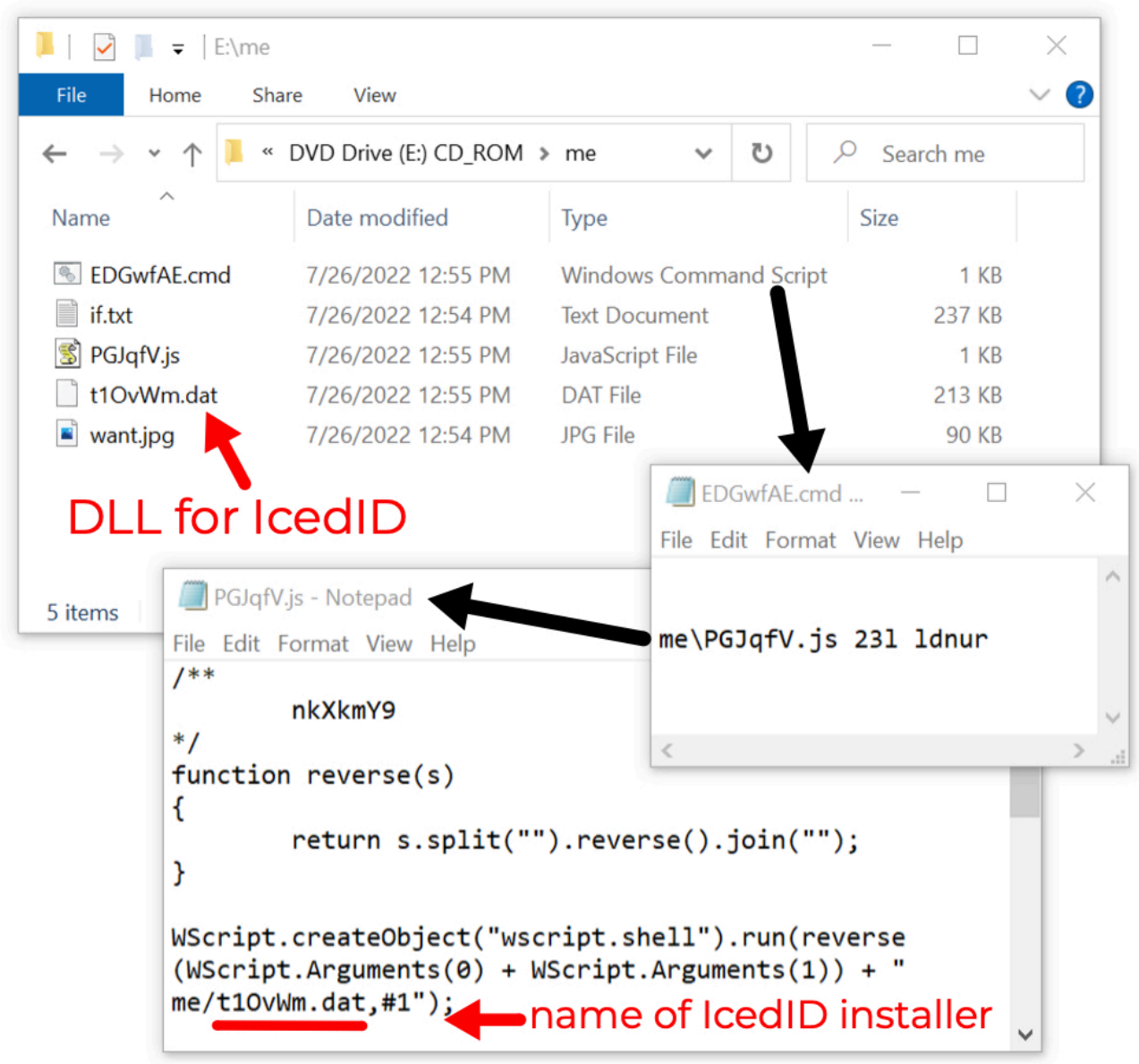


Shown above: Flow chart for IcedID infection on Tuesday 2022-07-26.

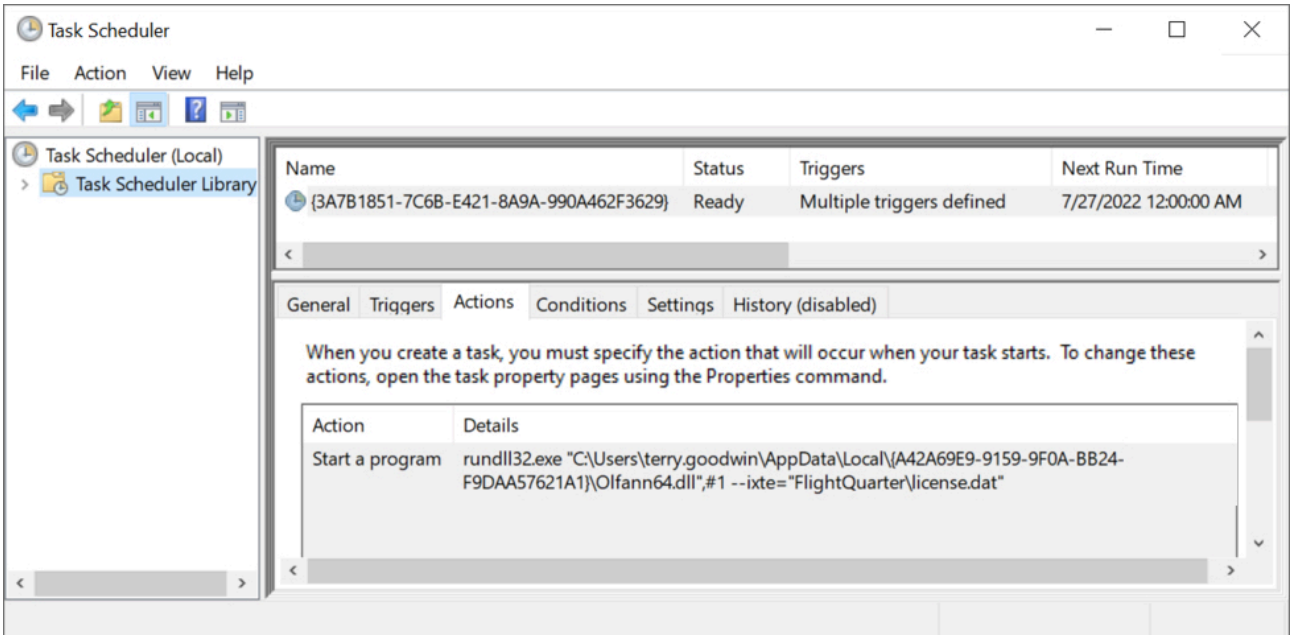
Images From the Infection



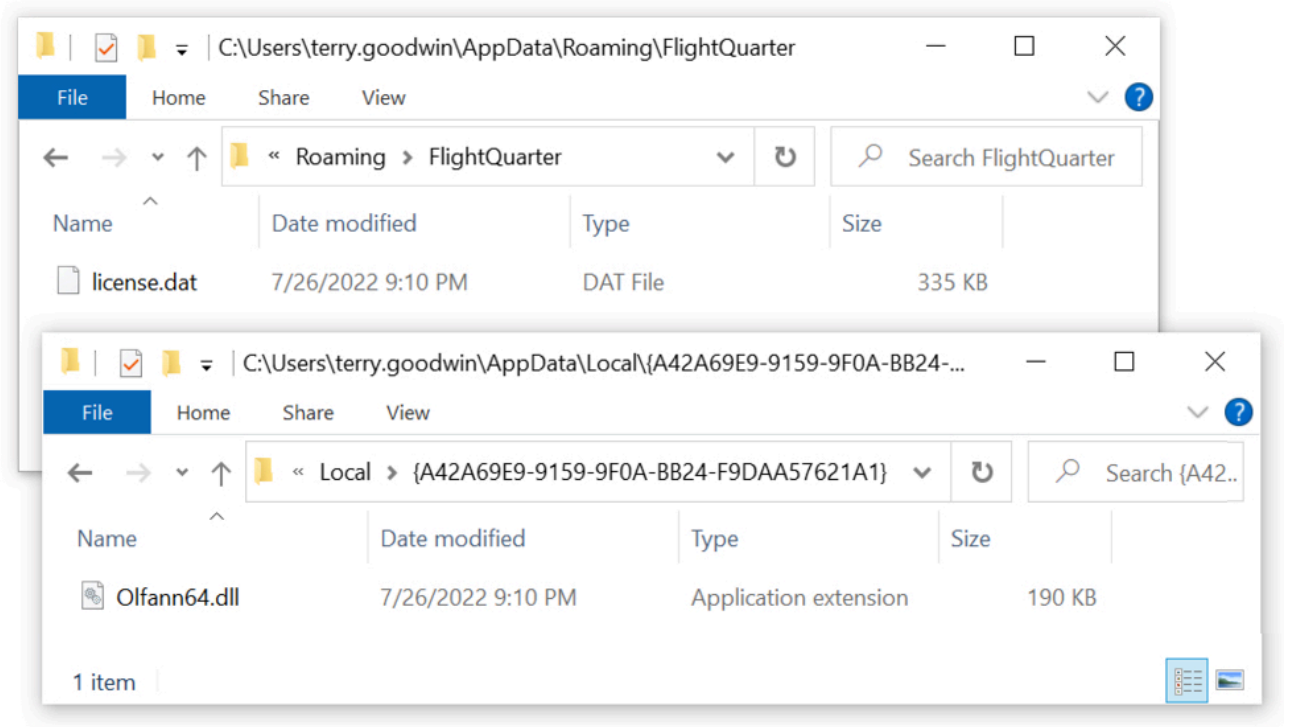
Shown above: Password-protected zip archive found through VirusTotal contains ISO file with shortcut to run command script.



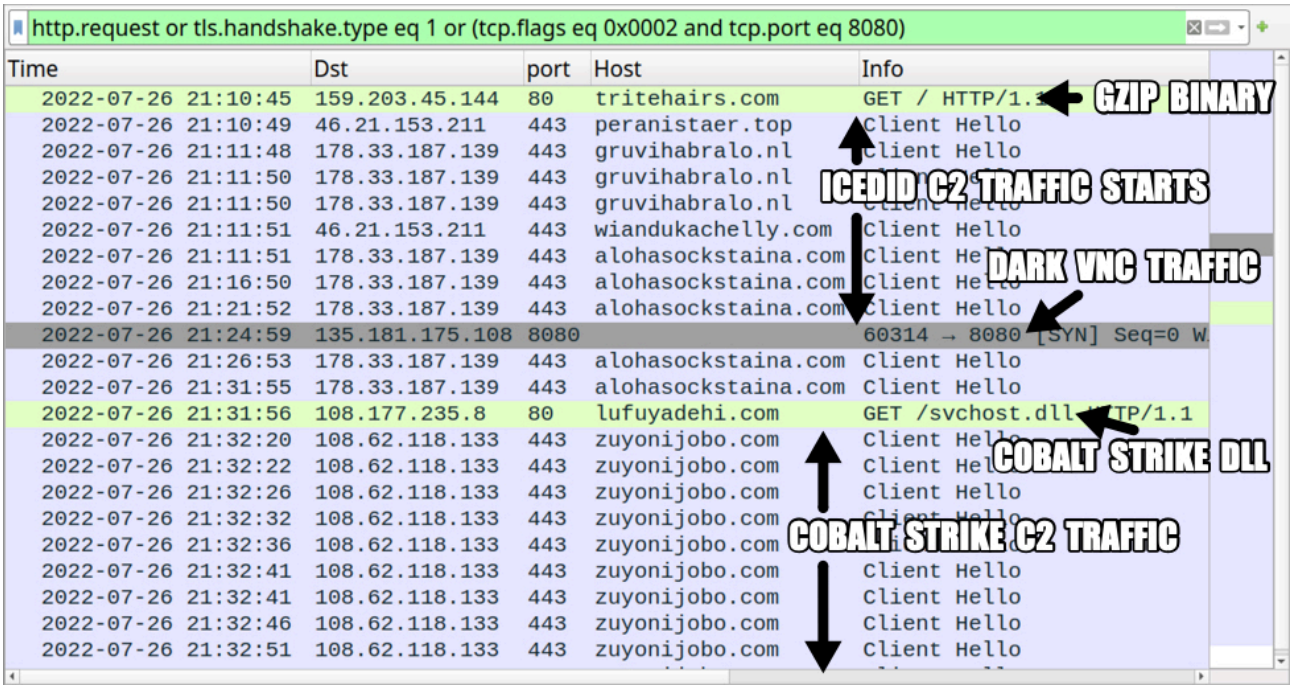
Shown above: Windows shortcut runs .js file, which then runs a DLL to install IcedID malware.



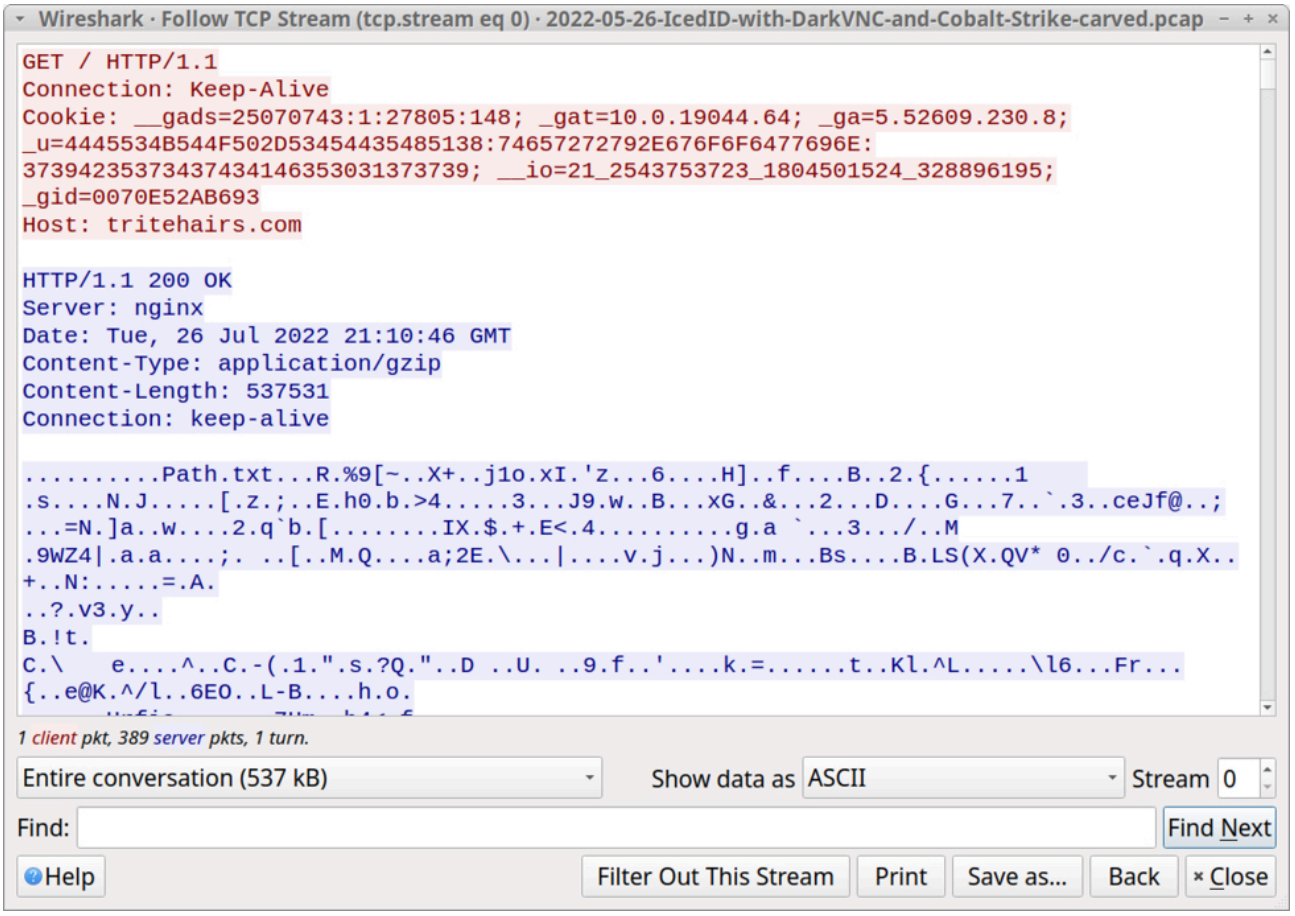
Shown above: Scheduled task after IcedID is persistent on the infected Windows host.



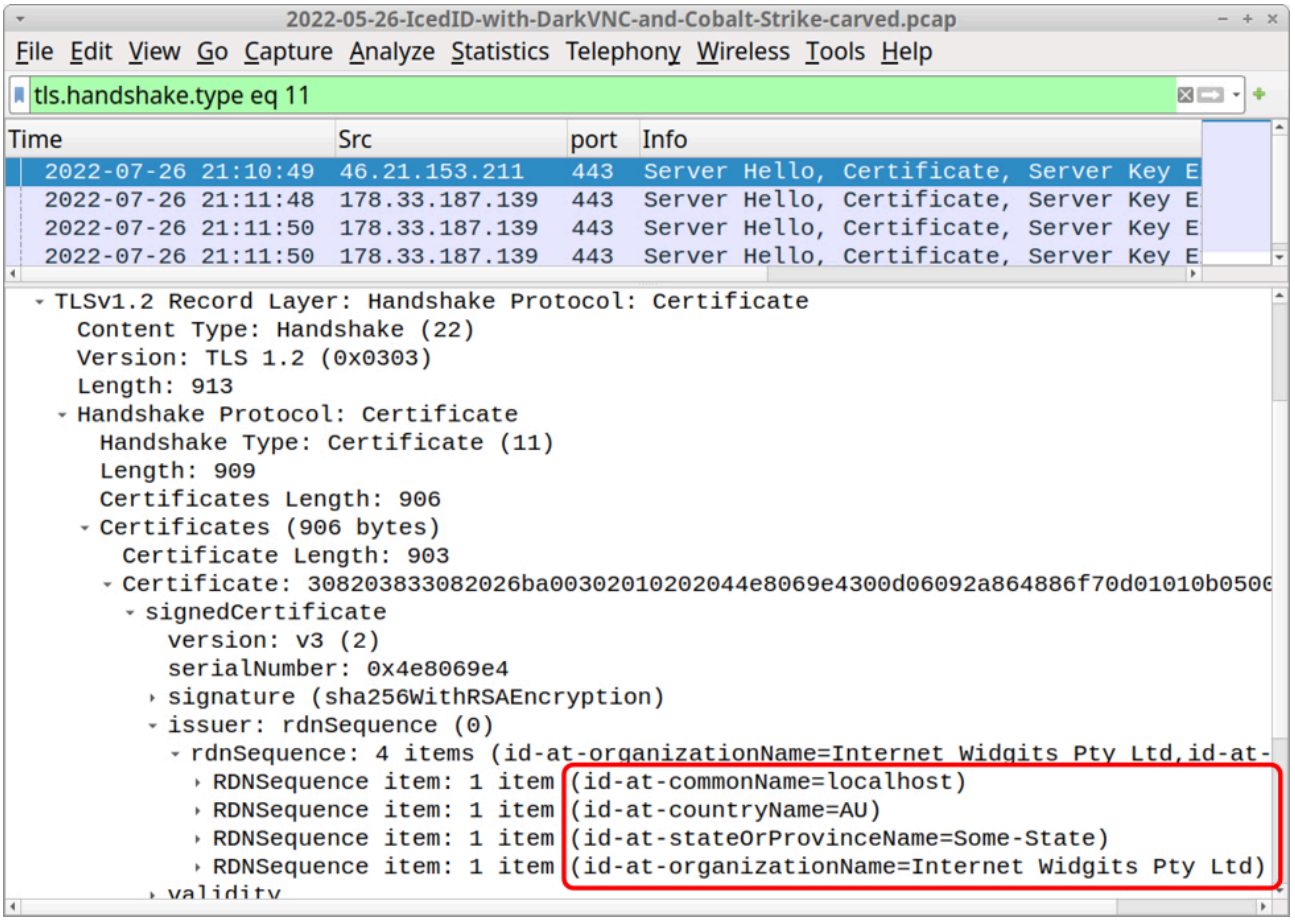
Shown above: Persistent IcedID malware DLL and license.dat binary needed to run the DLL.



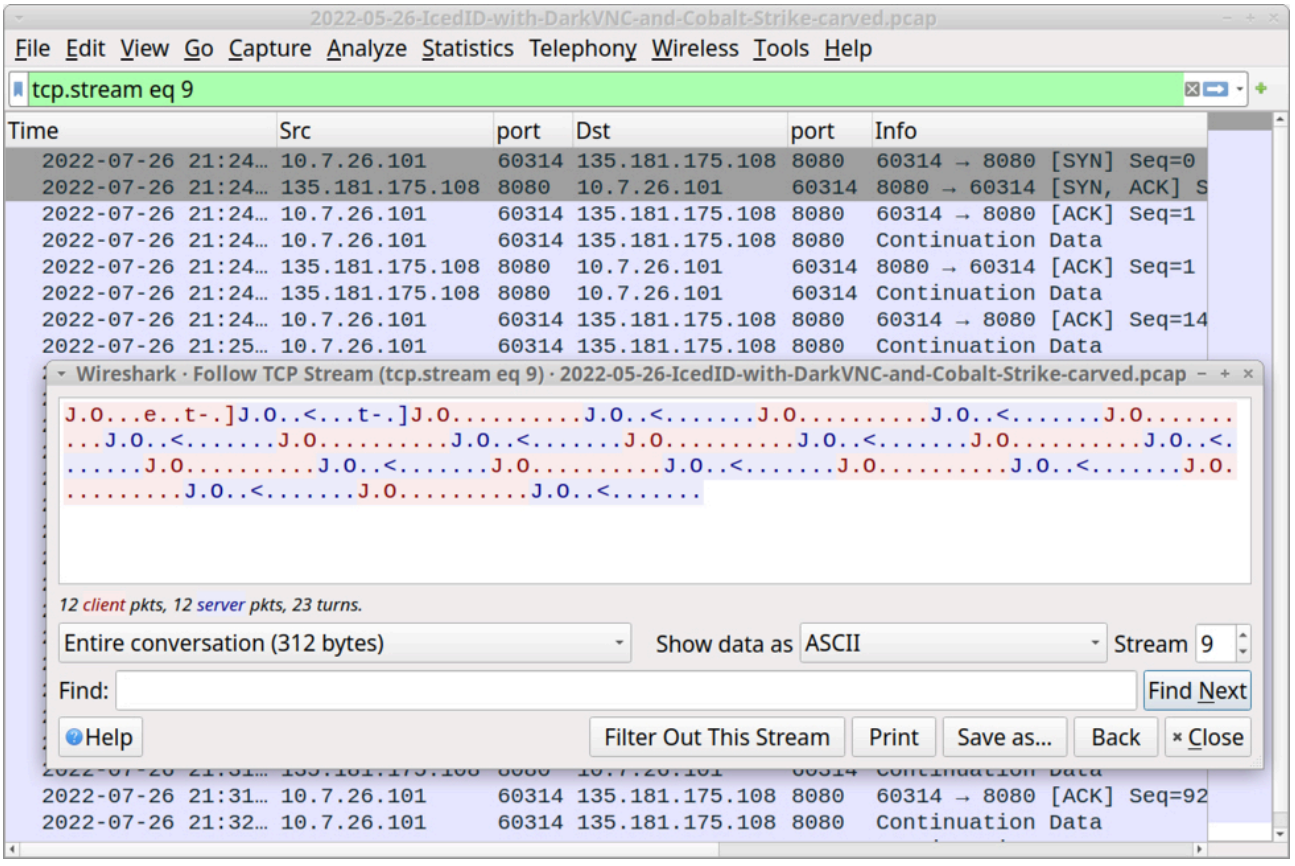
Shown above: Traffic from the infection filtered in Wireshark.



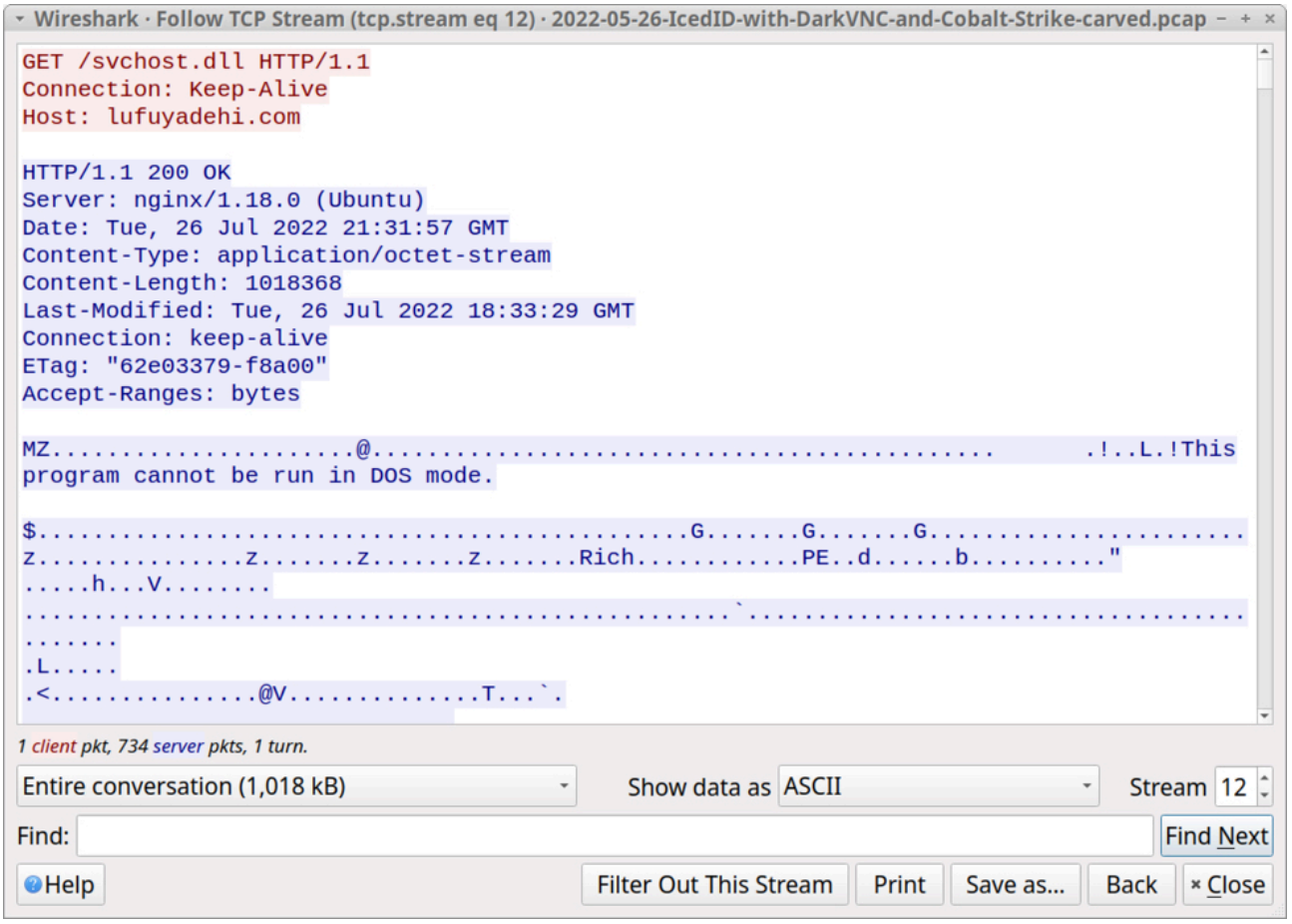
Shown above: HTTP traffic generated by the IcedID installer returned a gzip binary.



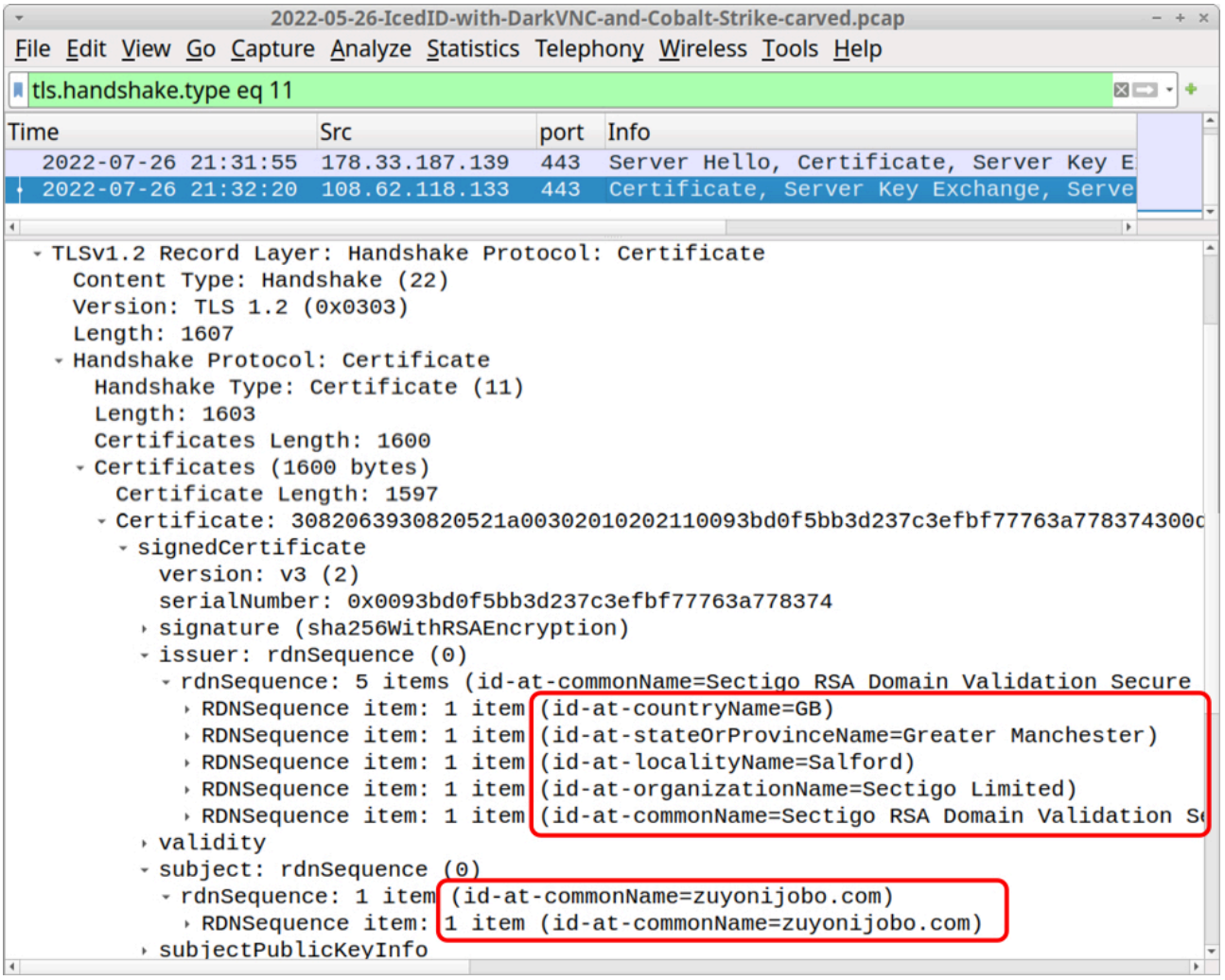
Shown above: HTTPS C2 traffic for IcedID uses self-signed certificates as shown here in Wireshark.



Shown above: Encoded/encrypted traffic generated by DarkVNC malware appears after the IcedID infection.



Shown above: Infected Windows host retrieves DLL for Cobalt Strike.



Shown above: Cobalt Strike HTTPS C2 traffic uses a legitimate certificate from Sectigo.

Indicators of Compromise (IOCs)

SHA256 hash: **4b86c52424564e720a809dca94f5540fcddac10cb57618b44d693e49fd38c0a5**

- File size: 420,425 bytes
- File description: password-protected zip archive containing malicious ISO image
- Password: doc2546

SHA256 hash: **d9a7ce532ee39918815f9dd03d0b4961ef85dddfd2498759b868e9ed8858a532**

- File size: 1,267,712 bytes
- File name: figures.iso
- File description: malicious ISO image containing files for IcedID infection

SHA256 hash: **4661a789c199544197a7d3ccfedb51ec95393641fb44875c92cf6c2c4a40fc1d**

- File size: 1,205 bytes

- File name: statistics.lnk
- File description: Windows shortcut to run IcedID installer. Only immediately visible file within the ISO image.

SHA256 hash: **eef2684a47bbadf954f3bc06b3611989447f1b5cfd47cdeacb38321987b3565c**

- File size: 30 bytes
- File location in ISO image: me\EDGwfAE.cmd
- File description: run by above shortcut, this command script runs the below JS file

SHA256 hash: **df66d308065919c5d45f6c9b718b1a7c58f9e461488bbef850c924728f053b14**

- File size: 263 bytes
- File location in ISO image: me\PGJqfV.js
- File description: run by the above command script, this JS file runs the below IcedID installer DLL

SHA256 hash: **f53321d9a70050759f1d3d21e4748f6e9432bf2bc476f294e6345f67e6c56c3e**

- File size: 217,600 bytes
- File location in ISO image: me\t1OvWm.dat
- File description: run by the above JS file, this 64-bit DLL installs IcedID
- Run method: rundll32.exe *[filename]*,#1

SHA256 hash: **a15ae5482b31140220bb75ce2e6c53aaafe3dc702784a0d235a77668e3b0a69a**

- File size: 217,600 bytes
- File location in ISO image: one\jGv5XFIe.dat
- File description: another 64-bit DLL to install IcedID, not used for this infection
- Run method: rundll32.exe *[filename]*,#1

SHA256 hash: **ee0379ef06a74b3c810b4f757097cd0534ec5c4ebf0d92875b07421fe1a5dd55**

- File size: 537,531 bytes
- File location: hxxp://tritehairs[.]com/
- File description: gzip binary from tritehairs[.]com used to create persistent IcedID 64-bit DLL and license.dat

SHA256 hash: **e512027d42d829fad95d14aa4c48f3ce30089e5c200681a2bded67068b8973f4**

- File size: 194,560 bytes

- File location: C:\Users*[username]*\AppData\Local\{A42A69E9-9159-9F0A-BB24-F9DAA57621A1}\Olfann64.dll
- File description: persistent IcedID 64-bit DLL
- Run method: rundll32.exe *[filename]*,#1 --ixte="*[path to license.dat]*"

SHA256 hash: **1de8b101cf9f0fabc9f086bddb662c89d92c903c5db107910b3898537d4aa8e7**

- File size: 342,218 bytes
- File location: C:\Users*[username]*\AppData\Roaming\FlightQuarter\license.dat
- File description: data binary used to run the persistent IcedID DLL

SHA256 hash: **a7a0025d77b576bcdaf8b05df362e53a748b64b51dd5ec5d20cf289a38e38d56**

- File size: 1,018,368 bytes
- File location: hxxp://lufuyadehi[.]com/svchost.dll
- File location: C:\Users*[username]*\AppData\Local\Temp\Yuicku32.dll
- File description: 64-bit DLL for Cobalt Strike
- Run method: regsvr32.exe *[filename]*

Traffic from an infected Windows host:

Traffic for gzip binary:

- 159.203.45[.]144:80 - tritehairs[.]com - GET /

IcedID HTTPS C2 traffic:

- 46.21.153[.]211:443 - peranistaer[.]top - HTTPS traffic
- 46.21.153[.]211:443 - wiandukachelly[.]com - HTTPS traffic
- 178.33.187[.]139:443 - alohasockstaina[.]com - HTTPS traffic
- 178.33.187[.]139:443 - gruvihabralo[.]nl - HTTPS traffic

DarkVNC traffic:

- 135.181.175[.]108:8080 - Encoded/encrypted traffic

Cobalt Strike traffic:

- 108.177.235[.]8:80 - lufuyadehi[.]com - GET /svchost.dll
- 108.62.118[.]133:443 - zuyonijobo[.]com - HTTPS traffic

Final Words

A packet capture (pcap) of the infection traffic, along with the associated malware and artifacts can be found **here**.

Brad Duncan
brad [at] malware-traffic-analysis.net
