



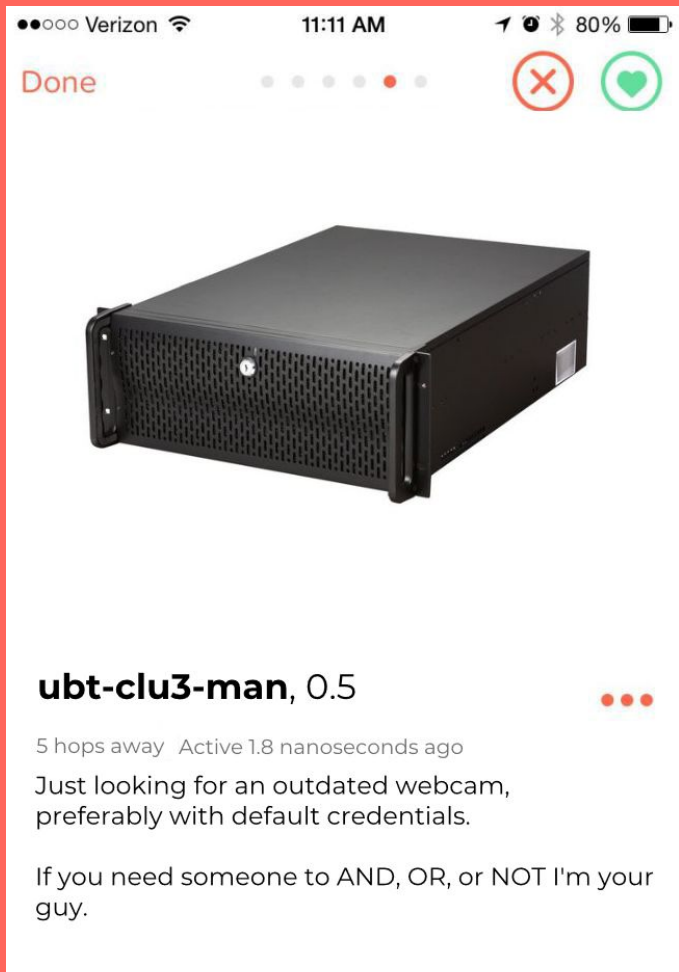
A Date with Data

Botnet Command and Control Through
Tinder



A Date with Data

Botnet Command and Control Through
Tinder (Almost)



\$whoami

Nathaniel Beckstead

Interests

Blue team

Homelab

Network Security

Find Me

github.com/becksteadn

scriptingis.life

Intercept Requests

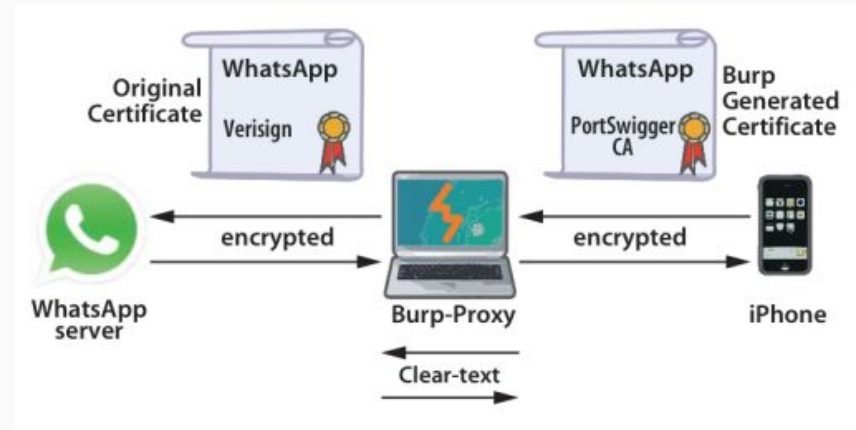


Certificate Pinning

Provides relative certainty of the host's (server's) identity

App has a list of certificates it trusts.

Does not establish a connection if the certificate is not in the pinset.

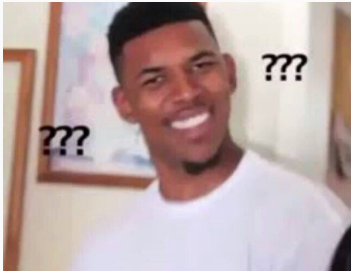


Certificate Pinning

Tinder: Are you Buzz Lightyear?

Burp Suite: Yeah, I'm Buzz Lightyear.

Tinder:



Cert Pinning Bypass



Decompile, Alter, Recompile

Thank you Chaim and Anders.

Sadly outdated.

Code is now obfuscated.



RIT Computing Security Blog

Bypassing Certificate Pinning (on Tinder)

[« Previous](#) / [Next »](#)

[ritsec](#) / [December 11, 2016](#) / [Uncategorized](#)

```
apktool d tinder-1.apk -o tinder_apk_disassembled
```

By Anders Kursar =

Decompile, Alter, Recompile

```
nathaniel@thehackmachine:~/Documents/Projects/Tinder-C2/tinder.apk_disassembled$ grep -ir X509TrustManager . | grep method
./smali_classes2/com/mapbox/android/telemetry/TelemetryClientSettings.smali:.method private isSocketFactoryUnset(Ljavax/net/ssl/SSLSocketFactory;Lja
./smali_classes2/com/mapbox/android/telemetry/TelemetryClientSettings$Builder.smali:.method x509TrustManager(Ljavax/net/ssl/X509TrustManager;)Lcom/m
./smali/com/foursquare/internal/network/b.smali:.method private static g()Ljavax/net/ssl/X509TrustManager;
./smali_classes5/okhttp3/o.smali:.method private A()Ljavax/net/ssl/X509TrustManager;
./smali_classes5/okhttp3/o.smali:.method private a(Ljavax/net/ssl/X509TrustManager;)Ljavax/net/ssl/SSLSocketFactory;
./smali_classes5/okhttp3/internal/b/a$b.smali:.method constructor <init>(Ljavax/net/ssl/X509TrustManager;Ljava/lang/reflect/Method;)V
./smali_classes5/okhttp3/internal/b/f.smali:.method public a(Ljavax/net/ssl/X509TrustManager;)Lokhttp3/internal/tls/c;
./smali_classes5/okhttp3/internal/b/f.smali:.method public b(Ljavax/net/ssl/X509TrustManager;)Lokhttp3/internal/tls/TrustRootIndex;
./smali_classes5/okhttp3/internal/b/a.smali:.method public a(Ljavax/net/ssl/X509TrustManager;)Lokhttp3/internal/tls/c;
./smali_classes5/okhttp3/internal/b/a.smali:.method public b(Ljavax/net/ssl/X509TrustManager;)Lokhttp3/internal/tls/TrustRootIndex;
./smali_classes5/okhttp3/internal/tls/c.smali:.method public static a(Ljavax/net/ssl/X509TrustManager;)Lokhttp3/internal/tls/c;
./smali_classes5/okhttp3/o$a.smali:.method public a(Ljavax/net/ssl/SSLSocketFactory;Ljavax/net/ssl/X509TrustManager;)Lokhttp3/o$a;
```

```
al/b/f.smali:.method public a(Ljavax,
al/b/f.smali:.method public b(Ljavax,
al/b/a.smali:.method public a(Ljavax,
al/b/a.smali:.method public b(Ljavax,
al/tls/c.smali:.method public static
ali:.method public a(Ljavax/net/ssl/
```

Decompile, Alter, Recompile

Search files for functions using X509TrustManager.

Add 'return-void' to the top and bottom.

```
.method public checkClientTrusted([Ljava/security/cert/X509Certificate;Ljava/lang/String;)V
    return-void
    .locals 2
    .annotation system Ldalvik/annotation/Throws;
        value = {
            Ljava/security/cert/CertificateException;
        }
    .end annotation

    .prologue
    .line 166
    new-instance v0, Ljava/security/cert/CertificateException;

    const-string v1, "Client certificates not supported!"

    invoke-direct {v0, v1}, Ljava/security/cert/CertificateException;-><init>(Ljava/lang/String;)V

    throw v0
    return-void
.end method
```

Cert Pinning Bypass Bypass



The API

All the hard work is done.

Translate to Python requests module.

Use Postman to test.

The API

Endpoint	Purpose	Data?	Method
<code>/auth</code>	For authenticating	<code>{'facebook_token': INSERT_HERE, 'facebook_id': INSERT_HERE}</code>	POST
<code>/auth/login/accountkit</code>	For SMS authentication (two-factor)	<code>{'token': INSERT_HERE, 'id': INSERT_HERE, 'client_version':'9.0.1'}</code>	POST
<code>/user/recs</code>	Get match recommendations	<code>{}</code>	GET
<code>/user/matches/_id</code>	Send Message to that id	<code>{"message": TEXT GOES HERE}</code>	POST
<code>/user/_id</code>	Get a user's profile data	<code>{}</code>	GET

<https://github.com/fbessez/Tinder>

The API

fb_auth_token.py - Uses robobrowser to log in using username/password and gets FB token and UID.

tinder_api.py - Authenticates to Tinder using FB token and UID and returns token.

The API

Host: api.gotinder.com

X-Auth-Token: 4a7f[REDACTED]

User-Agent: Tinder/7.5.3 (iPhone; iOS 10.3.2; Scale/2.00)

```
1 {
2   "_id": "5b9dc7f1db977726ed3d440",
3   "age_filter_max": 37,
4   "age_filter_min": 18,
5   "birth_date": "1991-04-09T00:00:00.000Z",
6   "create_date": "2018-09-16T03:03:13.877Z",
7   "distance_filter": 50,
8   "email": "burgnerd42@gmail.com",
9   "email_settings": {
10    "new_matches": true,
11    "messages": true,
12    "promotions": true
13  },
14  "facebook_id": "117115519248695",
15  "gender": 1,
16  "gender_filter": 0,
17  "interested_in": [
18    0
```

<https://github.com/fbessez/Tinder>

Command and Control



Command and Control

Endpoint	Description	Data	Method
/like/_id	Like someone a.k.a swipe right		GET
/user/matches/_id	Send message to _id	{"message": TEXT GOES HERE}	POST
/user/_id	Get a user's profile data		GET

Facebook Security



Facebook and Bots

Facebook works with Republican and Democratic groups to fight fake election news

9to5Mac • today

- Facebook expands measures to slow down the global spread of fake news
Firstpost • today



[View more](#) ▾

This fake news generator is a head-turning troll machine

The Daily Dot • today



Facebook might finally be making progress against fake news—but Twitter needs to do more

MIT Technology Review • 3 days ago

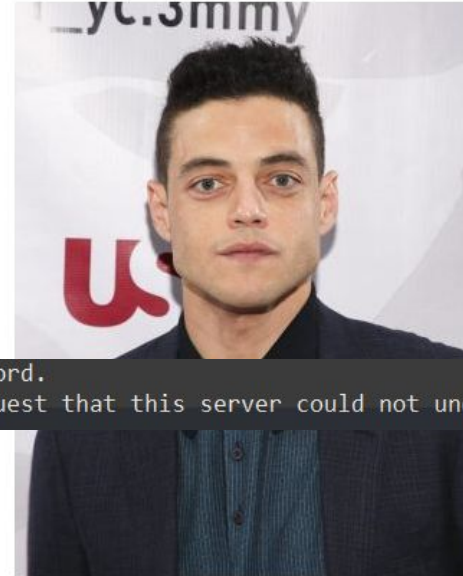


Facebook and Bots

Upload a Photo of Yourself

To get back on Facebook, upload a photo that clearly shows your face. Make sure the photo is well-lit and isn't blurry. Don't include other people in the shot.

Once we've confirmed it's you, we'll permanently delete the photo. It won't appear on your profile.



×jon_rasputin.jpg

```
access token could not be retrieved. Check your username and password.  
Official error: 400 Bad Request: The browser (or proxy) sent a request that this server could not understand.
```

Facebook and Bots


Your Account Has Been Disabled

For more information, or if you think your account was disabled by mistake, please visit the Help Center.

[Go To Help Center](#)

[Download Your Information](#)

Up Next: Workplace?

 Nicholas O'Brien