TEAM NEBULA

NETWORK AND INFORMATION SECURITY MANAGEMENT

SEMINAR 5: DATA BREACH CASE STUDY

07/07/21

Breach Checklist – Part 1

Case Study: Adult Friend Finder breach, 2016

What types of data were affected?

- Email addresses, passwords, spoken languages and usernames.
- Historic data up to 20 years old was included, including deleted accounts.

What happened?

- 412 million accounts were impacted by the breach which was caused by an unpatched vulnerability which had recently been revealed (Local File Inclusion vulnerability).

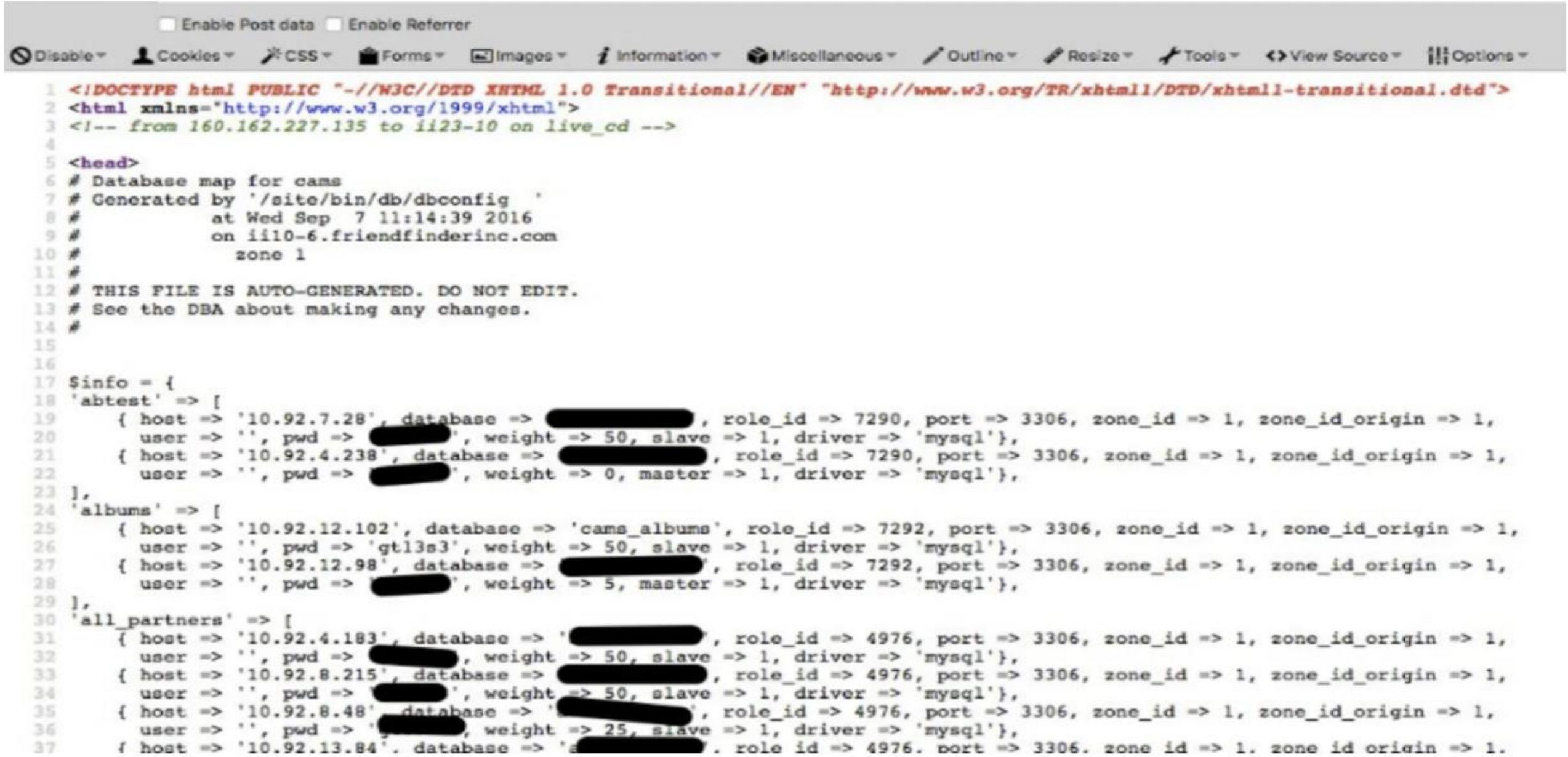
Who was responsible?

- The responsible party has not been publicly identified but the breach was discovered by a security researcher by the name of ‘Revolver’.

Were any escalation(s) stopped - how?

- Six databases containing the majority of account data were compromised so it is likely that lateral movement and escalation had already been achieved.

Researcher 1x0123 wrote: "F**kload of databases with same user/password + runing as root".



```
Enable Post data  Enable Referrer
Disable  Cookies  CSS  Forms  Images  Information  Miscellaneous  Outline  Resize  Tools  View Source  Options

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!-- from 160.162.227.135 to ii23-10 on live_cd -->

<head>
# Database map for cams
# Generated by '/site/bin/db/dbconfig  '
#            at Wed Sep  7 11:14:39 2016
#            on ii10-6.friendfinderinc.com
#              zone 1
#
# THIS FILE IS AUTO-GENERATED. DO NOT EDIT.
# See the DBA about making any changes.
#


$info = {
'abtest' => [
    { host => '10.92.7.28', database => [redacted], role_id => 7290, port => 3306, zone_id => 1, zone_id_origin => 1,
      user => '', pwd => [redacted], weight => 50, slave => 1, driver => 'mysql'},
    { host => '10.92.4.238', database => [redacted], role_id => 7290, port => 3306, zone_id => 1, zone_id_origin => 1,
      user => '', pwd => [redacted], weight => 0, master => 1, driver => 'mysql'},
],
'albums' => [
    { host => '10.92.12.102', database => 'cams_albums', role_id => 7292, port => 3306, zone_id => 1, zone_id_origin => 1,
      user => '', pwd => 'gt13s3', weight => 50, slave => 1, driver => 'mysql'},
    { host => '10.92.12.98', database => [redacted], role_id => 7292, port => 3306, zone_id => 1, zone_id_origin => 1,
      user => '', pwd => [redacted], weight => 5, master => 1, driver => 'mysql'},
],
'all_partners' => [
    { host => '10.92.4.183', database => [redacted], role_id => 4976, port => 3306, zone_id => 1, zone_id_origin => 1,
      user => '', pwd => [redacted], weight => 50, slave => 1, driver => 'mysql'},
    { host => '10.92.8.215', database => [redacted], role_id => 4976, port => 3306, zone_id => 1, zone_id_origin => 1,
      user => '', pwd => [redacted], weight => 50, slave => 1, driver => 'mysql'},
    { host => '10.92.8.48', database => [redacted], role_id => 4976, port => 3306, zone_id => 1, zone_id_origin => 1,
      user => '', pwd => [redacted], weight => 25, slave => 1, driver => 'mysql'},
    { host => '10.92.13.84', database => [redacted], role_id => 4976, port => 3306, zone_id => 1, zone_id_origin => 1,
```

Later he or she tweeted: "No reply from#adulfriendfinder.. time to get some sleep they will call it hoax

Breach Checklist – Part 2

Case Study: Adult Friend Finder breach, 2016

Was the Business Continuity Plan instigated?

- This has not been publicly shared.

Was the ICO notified?

- As this was pre-GDPR, the ICO would not have been informed of the breach as this was not a requirement.

Were affected individuals notified?

- AFF released a statement saying they were communicating with impacted account holders.

What were the social, legal and ethical implications of the decisions made?

- Sensitive data, including sexual orientation, with a potential for grave consequences on the data subject were released. Whilst there is no comment on the direct impact this breach had on data subjects, the Ashley Madison breach a year earlier revealed similar sensitive data and led to “resignations, divorces and suicides” (The Guardian, 2016).

Recommendations

- Encrypt data at rest using suitably strong algorithms (keys should be hardware secure)
- Hash and salt passwords to store them securely
- Implement suitable patching policy to ensure patches are rolled out without any delay
- Get IDS & IPS
- Improve firewall (firewall with proxy, that can drop SQLi even in encrypted packets)
- Conduct regular penetration tests as well as employing suitable security testing, e.g. SAST & DAST, as part of the software development lifecycle (SDLC)
- Segregate network to prevent lateral movement and consider a zero trust approach to protect sensitive personal data