Josh Huff, @Baywolf88
https://www.learnallthethings.net

- OSINT Analyst
- Digital Forensics
- Former Private Investigator
- Information Security Conference Speaker
- Blogger
Breach Data – What is it?

Ethics - Is it OK for OSINT?

OpSec – What can it teach us?

OH MY!
Breach Data Headlines

ASHLEY MADISON
Life is short. Have an affair.

Over 39,118,000 anonymous members!

Hacked By #GOP

Warning:
We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secret
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM (GMT).

Data Link:
https://www.sonypicturesstockfootage.com/SPEData.zip
https://dmplauewh36.sps.sony.com/SPEData.zip
http://www.ntcru.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebelemtech.com.br/SPEData.zip
What is Breach Data?

**OSINT:**
Information in the public domain or accessible from public sources

**Data Breach:**
An incident where information is stolen or taken from a system without the knowledge or authorization of the system’s owner
Data Types

**OSINT Data:**
Email, Username, DOB, Photos, Phone Numbers, Physical Address, LinkedIn Bio, Instagram photos, Facebook Info

**Breach Data:**
Credit Card Numbers, Email, Passwords, IP address, Username, Physical Address, SSN, DOB, Site Context
Breach data is typically things you wouldn’t want to be online
Ashley Madison
What does it look like?
32 million user login details

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>am_an.dmp</td>
<td>9/22/2015 9:59 PM</td>
<td>DUMP File</td>
<td>9,923,020 KB</td>
</tr>
<tr>
<td>member_login.dmp</td>
<td>7/11/2015 8:04 PM</td>
<td>DUMP File</td>
<td>4,379,309 KB</td>
</tr>
<tr>
<td>member_details.dmp</td>
<td>7/12/2015 7:57 AM</td>
<td>DUMP File</td>
<td>2,379,944 KB</td>
</tr>
<tr>
<td>am_november_member_email.dmp</td>
<td>7/11/2015 11:03 PM</td>
<td>DUMP File</td>
<td>1,741,160 KB</td>
</tr>
<tr>
<td>swappernet_User_Table.7z</td>
<td>7/9/2015 12:25 PM</td>
<td>7Z File</td>
<td>16,868 KB</td>
</tr>
<tr>
<td>ALM - January 2015 - Company Overview</td>
<td>7/7/2015 12:14 PM</td>
<td>Microsoft PowerPoint</td>
<td>8,171 KB</td>
</tr>
<tr>
<td>Copies of Option Agreements</td>
<td>10/20/2012 12:23 ...</td>
<td>Chrome HTML Document</td>
<td>6,197 KB</td>
</tr>
<tr>
<td>2015-01-06_downloaded</td>
<td>7/17/2015 8:44 AM</td>
<td>Microsoft Excel</td>
<td>3,483 KB</td>
</tr>
<tr>
<td>2015-06-02_downloaded</td>
<td>7/17/2015 8:45 AM</td>
<td>Microsoft Excel</td>
<td>3,397 KB</td>
</tr>
</tbody>
</table>

Size: 20.0 GB (21,517,024,042 bytes)
Size on disk: 20.0 GB (21,522,546,688 bytes)
Contains: 2,678 Files, 1 Folders
Ashley Madison
4 dump files had identifying user number.
Nulled.IO

What does it look like?

- 536K user accounts
- 800K personal user messages
- 5,582 purchase records
- 2.2 million posts from the forum
Nulled.IO

L),(3685810,0,NULL,525987,'mahut1000',1,1,'109.150.104.112',1455620638,<'p'>Anyone here totally addicted to CoC ? I'm so addicted to it that i have no friends anymore and my Wife has left me, but crikey its brilliant.....</p>

anyone and my Wife has left me, but crikey its brilliant.....</p>

Anyone here totally addicted to CoC ? I'm so addicted to it that i have no friends anymore and my Wife has left me, but crikey its brilliant.....</p>

Anyone here totally addicted to CoC ? I'm so addicted to it that i have no friends anymore and my Wife has left me, but crikey its brilliant.....</p>

Anyone here totally addicted to CoC ? I'm so addicted to it that i have no friends anymore and my Wife has left me, but crikey its brilliant.....</p>

Anyone here totally addicted to CoC ? I'm so addicted to it that i have no friends anymore and my Wife has left me, but crikey its brilliant.....</p>

Anyone here totally addicted to CoC ? I'm so addicted to it that i have no friends anymore and my Wife has left me, but crikey its brilliant.....</p>

Anyone here totally addicted to CoC ? I'm so addicted to it that i have no friends anymore and my Wife has left me, but crikey its brilliant.....</p>

Anyone here totally addicted to CoC ? I'm so addicted to it that i have no friends anymore and my Wife has left me, but crikey its brilliant.....</p>

Anyone here totally addicted to CoC ? I'm so addicted to it that i have no friends anymore and my Wife has left me, but crikey its brilliant.....</p>
So let’s talk about ethics... but first

I'M NOT YOUR LAWYER

BUT I DID STAY AT A HOLIDAY INN EXPRESS LAST NIGHT
Ethics

Breach data includes PII...

Before using breach data, consult your legal department/supervisor/compliance teams.

If you are conducting OSINT for a pen test is breach data “in scope” for the client?
OSINT Professionals generate reports

What type of report are you going to create?

Situational Awareness Vs. Legal affidavit for court.

Does your organization interface with Law Enforcement?
Ethics

How did you reach the conclusions in your report?

Can you duplicate the research?

Will you have to testify in court?

Will your research be shown to the subject of investigation?
HACKERS
GONNA HACK
Breach Data resources – Haveibeenpwned.com
### Breach Data resources – Hacked-emails.com

Here we list all data leaks in our database. Each of them has been made publicly available by the attackers themselves or by those affected through different websites. All this information can also be followed by RSS.

**Important:** Hacked Emails monitors data dumps found in the Deep & Dark Web with intent to verify them. By no means, we state that this is a true breach nor attempt to attribute it.

<table>
<thead>
<tr>
<th>Date detected</th>
<th>Title</th>
<th>Author</th>
<th>Emails found</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan - 2019</td>
<td>randi.org</td>
<td>anon</td>
<td>2,202</td>
<td>2.7 MB</td>
</tr>
<tr>
<td>Jan - 2019</td>
<td>safeskyhacks.com</td>
<td>anon</td>
<td>9,472</td>
<td>910.8 KB</td>
</tr>
<tr>
<td>Jan - 2019</td>
<td>webmaster.in</td>
<td>anon</td>
<td>7,035</td>
<td>711.8 KB</td>
</tr>
<tr>
<td>Jan - 2019</td>
<td>zum-flohmarkt.de</td>
<td>anon</td>
<td>20,419</td>
<td>632.0 KB</td>
</tr>
<tr>
<td>Jan - 2019</td>
<td>forum.woliera.com</td>
<td>anon</td>
<td>6,706</td>
<td>409.3 KB</td>
</tr>
<tr>
<td>Jan - 2019</td>
<td>onlinenutrition.com.au</td>
<td>anon</td>
<td>3,667</td>
<td>342.0 KB</td>
</tr>
<tr>
<td>Jan - 2019</td>
<td>korearafting.org</td>
<td>anon</td>
<td>9,845</td>
<td>282.9 KB</td>
</tr>
<tr>
<td>Jan - 2019</td>
<td>irg-listings.com</td>
<td>anon</td>
<td>8,173</td>
<td>281.0 KB</td>
</tr>
</tbody>
</table>
Breach Data resources – Dehashed.com
Breach Data resources – Many Others

https://osintframework.com

OSINT Framework

- Username
- Email Address
- Domain Name
- IP Address
- Images / Videos / Docs
- Social Networks
- Instant Messaging
- People Search Engines

- Email Search
- Common Email Formats
- Email Verification
- Breach Data
- Spam Reputation Lists
- Mail Blacklists

- PwnedList.com
- Have I been pwned?
- DeHashed
- Intelligence X
- Vigilante.pw
- Breach or Clear
- Ashley Madison Emails
What can we do with Breach Data?
Nulled.IO breach

Member info included: username, email, encrypted passwords
Registration dates, registered with IP.

Site Context – what was the user talking about, promoting etc.
Breaking OpSec with Breach Data

OSINT Research → Breach Data → Bitcoin Forum

Email → Email Match → Bitcoin Wallet

Username → Username Match → Alias Name/Email

Region

Bitcoin Wallet

City

Discussion of Bitcoin exchanger
Ashley Madison Breach

Contained DOB, username, Email, IP, bio details
Credit card info, addresses
Breaking OpSec with Breach Data

OSINT Research: Email → Email Match

Breach Data: Username Match

Dating Site: Profile information → Alias Name/Email → Profile Photo

Email Match

Username

City

Facebook page
Password Correlation

Breaking OpSec with password correlation
Collection 1-5 - 2.2 billion unique usernames and passwords

These types of mega collections are becoming more available

So our own privacy and OpSec becomes very important.
What type of info do you supply when signing up for websites?

Name, Email, DOB, City, phone number (SMS verified)
Privacy and OpSec

Disinformation to Protect research accounts
**Privacy and OpSec**

**Web registration**
- **Name**
  - ALIAS NAME
- **Email**
  - THROWAWAY EMAIL (encrypted)
- **Password**
  - UNIQUE PASSWORDS
  - PASSWORD MANAGER

**Verification**
- **SMS text**
  - (cell phone)
- **VOIP APP (BURNER)**

**Web Page Backend**
- **IP address**
- **VPN SERVICE**
- **Timestamp**
- **Device Fingerprint**
  - VIRTUAL MACHINE
  - DEDICATED RESEARCH MACHINE
  - SILO’D WEB BROWSING SERVICE
What do we do to protect ourselves?

OSINT yourself

What breach data is out there for your personal/research accounts?
Conclusions

OSINT / Breach data Similar

Is your org ok with Breach data?

OpSec / Privacy

Links at:
Learnallthethings.net/osint-summit

Questions?
Josh@Learnallthethings.net
@baywolf88