JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Organizational Intelligence

THREAT MANAGEMENT

Organizational Intelligence

- Your organization has an online profile, whether you know it or not…
- This can be used by an attacker against you…
- In a penetration test, we act as the attacker, so we must use this information too!

Organizational Data

- Locations (of facilities and buildings)
  - Your physical security posture
  - Business hours
- Work routine of the organization
- Organizational charts
  - Relationships between departments and people
- Documents (contains metadata)
- Financial data
- Personal information of your employees

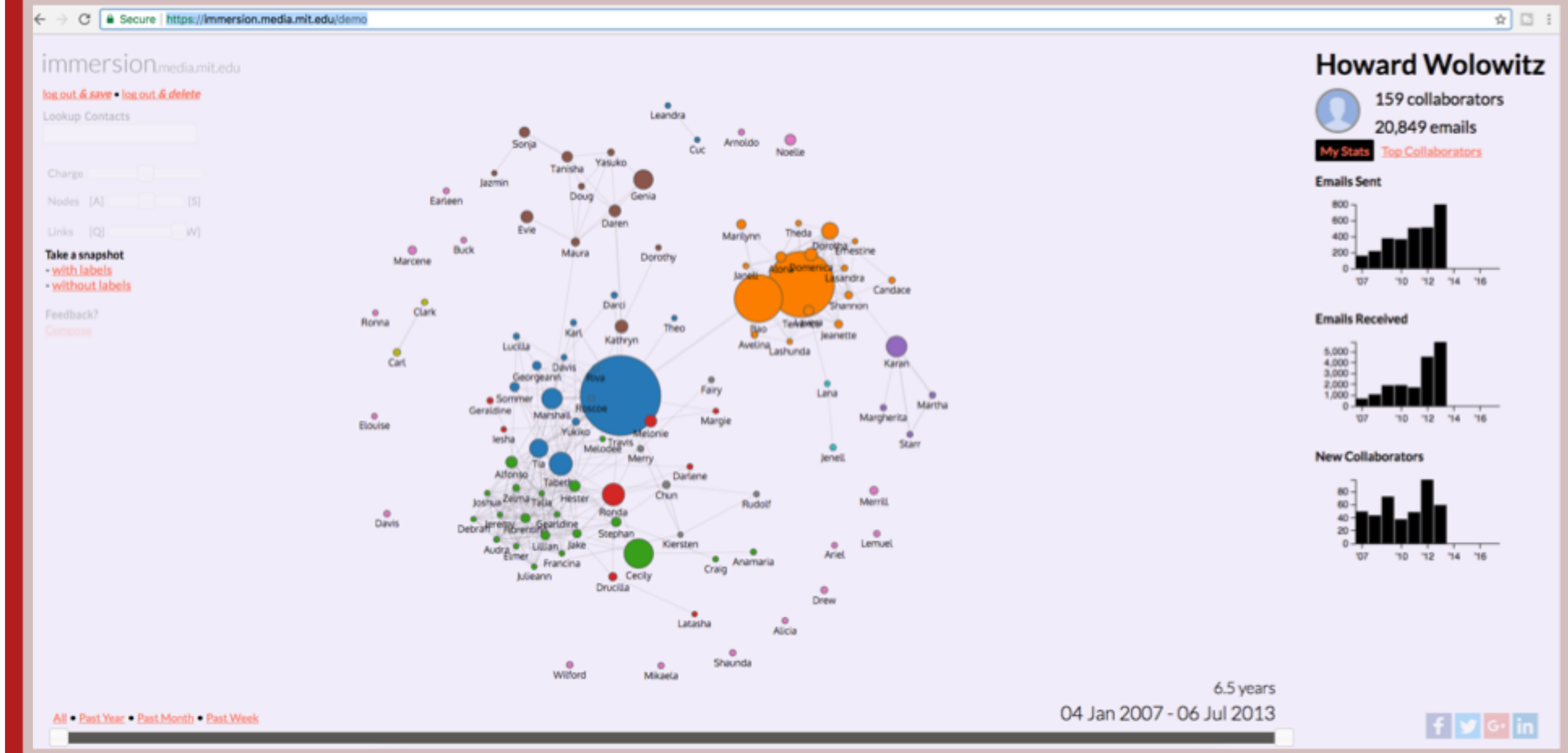
* Useful during social engineering *

Document Harvesting

- Metadata
  - Contains author’s name and software version used
- EXIF data
  - Photos could contain geolocation coordinates
- It is important to scrub metadata and EXIF data from documents posted on the web
- Emails
  - Can you be used to perform contact chaining and conduct social engineering campaigns

Immersion

https://immersion.media.mit.edu/demo



Where Can I Get Documents?

- Organizations are getting smarter and posted less sensitive information online

…on the Internet nothing is ever gone!

- The Internet Archive
  - archive.org
- Time Travel Service
  - timetravel.mementoweb.org
- Google Cache View
- Cachedview.com

Where Can I Get More?

- Social media is great to find details about the organization’s employees

- Many people post what companies they work for and don’t set their privacy settings up properly

- Paid public record searches, like Zaba Search, NETR Online, etc.

The Threat: Social Engineering

- Exploits the human element of security
- Occurs via phone, email, social media, or even in person
- Social Engineering Toolkit (SET)
- Creepy (geolocation tool)
- Metasploit (phishing and other tools)