



Security in knowledge

# DOXING AND ANTI-DOXING INFORMATION RECONNAISSANCE FOR THE STALKER AND THE STALKED

Jason Andress

[Redacted]

# What is Doxing?

- ▶ Documents -> docs -> dox -> doxing
- ▶ Doxing ~ = information reconnaissance, OSINT, cyberstalking, etc...
- ▶ Digging up personal info:

Name

Date of birth

Spouses, children, relatives

Pictures

Current and previous  
employment

Home and work addresses, phone  
numbers, email, etc...

Schools, degrees, certifications

Tax and mortgage information

Hobbies and interests

EVERYTHING else that they can find

# Why do People do This?

- ▶ Security awareness
- ▶ Security research
- ▶ Investigations
- ▶ Surveillance
- ▶ Hacktivism
- ▶ Public embarrassment/Harassment
- ▶ Idle curiosity/Random stalkery
- ▶ Not so random stalkery...



# Consequences of being Doxed

- ▶ Prosecution
- ▶ Identity theft
- ▶ Reputational damage
- ▶ Collateral damage
- ▶ Loss of livelihood
- ▶ Attacks against environments or services
- ▶ Just to name a few...

# Examples

- ▶ Mat Honan, Wired Magazine
  - ▶ Billing address from domain registration
  - ▶ Last 4 of credit card # from Amazon
  - ▶ Bypass security questions at Apple with Last 4 of CC#
  - ▶ Password reset emails from Google go to (compromised) Apple email
- ▶ US law enforcement data dump
  - ▶ Password reuse enables attackers to access servers housing law enforcement training data
  - ▶ Anonymous, in support of AntiSec doxes 77 different law enforcement agencies releases data on 7,000 individuals including: names, addresses, phone numbers, SSNs, and account credentials is released
  - ▶ FBI releases bulletin warning of the potential doxing threat
  - ▶ Another 7Gb of email and sensitive data is released

This is my doxing process. There are many like it, but this one is mine.



Security in knowledge

# Doxing Process

Basic Info:  
Name  
Username

Collect:  
Search engine data

Tools:  
Google  
Bing

# Doxing Process

Basic Info:  
Name  
Username

Location:

Collect:  
Search engine data

Collect:  
Geo IP  
Geo tag  
Employer  
Address  
Time zone

Tools:  
Google  
Bing

Tools:  
Facebook  
Peekyou  
Lullar  
Pipl  
IpInfoDB  
ExifTool



# Doxing Process

Basic Info:  
Name  
Username

Location:

Age:

Collect:  
Search engine data

Collect:  
Geo IP  
Geo tag  
Employer  
Address  
Time zone

Collect:  
Chat logs  
Pictures  
Comments  
Employment

Tools:  
Google  
Bing

Tools:  
Facebook  
Peekyou  
Lullar  
Pipl  
IpInfoDB  
ExifTool

Tools:  
IM  
Skype  
IRC  
TinEye

# Doxing Process

Basic Info:  
Name  
Username

Location:

Age:

Network info:

Collect:  
Search engine data

Collect:  
Geo IP  
Geo tag  
Employer  
Address  
Time zone

Collect:  
Chat logs  
Pictures  
Comments  
Employment

Collect:  
domains  
IPs

Tools:  
Google  
Bing

Tools:  
Facebook  
Peekyou  
Lullar  
Pipl  
IpInfoDB  
ExifTool

Tools:  
IM  
Skype  
IRC  
TinEye

Tools:  
whois  
netcraft  
dig  
DNSDigger

# Doxing Process

Basic Info:  
Name  
Username

Location:

Age:

Network info:

Email Addresses  
and accounts:

Collect:  
Search engine data

Collect:  
Geo IP  
Geo tag  
Employer  
Address  
Time zone

Collect:  
Chat logs  
Pictures  
Comments  
Employment

Collect:  
domains  
IPs

Collect:  
Online services

Tools:  
Google  
Bing

Tools:  
Facebook  
Peekyou  
Lullar  
Pipl  
IpInfoDB  
ExifTool

Tools:  
IM  
Skype  
IRC  
TinEye

Tools:  
whois  
netcraft  
dig  
DNSDigger

Tools:  
check usernames  
knowem

# Doxing Process

Basic Info:  
Name  
Username

Location:

Age:

Network info:

Email Addresses  
and accounts:

Bio Info:

Collect:  
Search engine data

Collect:  
Geo IP  
Geo tag  
Employer  
Address  
Time zone

Collect:  
Chat logs  
Pictures  
Comments  
Employment

Collect:  
domains  
IPs

Collect:  
Online services

Collect:  
Public records

Tools:  
Google  
Bing

Tools:  
Facebook  
Peekyou  
Lullar  
Pipl  
IpInfoDB  
ExifTool

Tools:  
IM  
Skype  
IRC  
TinEye

Tools:  
whois  
netcraft  
dig  
DNSDigger

Tools:  
check usernames  
knowem

Tools:  
Specific to location

# Doxing Process

Basic Info:  
Name  
Username

Location:

Age:

Network info:

Email Addresses  
and accounts:

Bio Info:

Munge data:

Collect:  
Search engine data

Collect:  
Geo IP  
Geo tag  
Employer  
Address  
Time zone

Collect:  
Chat logs  
Pictures  
Comments  
Employment

Collect:  
domains  
IPs

Collect:  
Online services

Collect:  
Public records

Analyze:  
Update records  
Rinse and repeat

Tools:  
Google  
Bing

Tools:  
Facebook  
Peekyou  
Lullar  
Pipl  
IpInfoDB  
ExifTool

Tools:  
IM  
Skype  
IRC  
TinEye

Tools:  
whois  
netcraft  
dig  
DNSDigger

Tools:  
check usernames  
knowem

Tools:  
Specific to location

Tools:  
Text editor  
Spreadsheet  
Database

# How do we Mitigate Doxing?



# Doxing Process

Basic Info:  
Name  
Username

Collect:  
Search engine data

Tools:  
Google  
Bing

- ▶ Name and username uniqueness is the major problem here
- ▶ Make this information less unique by using common names where possible or growing cover

# Doxing Process

Location:

Collect:  
Geo IP  
Geo tag  
Employer  
Address  
Time zone

Tools:  
Facebook  
Peekyou  
Lullar  
Pipl  
IpInfoDB  
ExifTool

- ▶ Be careful what you post online
- ▶ Minimize social networking usage
- ▶ Remove information from online information brokerage sources where possible



# Doxing Process

Age:

Collect:  
Chat logs  
Pictures  
Comments  
Employment

Tools:  
IM  
Skype  
IRC  
TinEye

- ▶ Don't post pictures online
- ▶ Be very careful what info you expose in online chats (this is hard)

# Doxing Process

Network info:

Collect:  
domains  
IPs

Tools:  
whois  
netcraft  
dig  
DNSDigger

- ▶ Use private domain registrations
- ▶ Secure DNS servers properly
- ▶ Use VPNs for internet access to hide location

# Doxing Process

- ▶ Use strong account names
- ▶ Use unique account names between services
- ▶ Use strong passwords!!

Email Addresses  
and accounts:

Collect:  
Online services

Tools:  
check usernames  
knowem

# Doxing Process

- ▶ Remove info from public records collection sources where possible
- ▶ Stay out of the news and news media

Bio Info:

Collect:  
Public records

Tools:  
Specific to location

# Doxing Process

- ▶ This step is somewhat difficult to mitigate
- ▶ We can make analysis more difficult by deliberately seeding false paths and information that stand out more than the real information

Munge data:

Analyze:  
Update records  
Rinse and repeat

Tools:  
Text editor  
Spreadsheet  
Database

# What can we do to Mitigate Information that has already been Exposed?



# Mitigating exposed information

- ▶ Can't put the genie back in the bottle
  - ▶ Once info gets out on the internet, it generally doesn't go away
  - ▶ Information of a sensitive/interesting nature will be very likely to be copied and propagated further
  - ▶ Media coverage of a major exposure will only make this worse

# Mitigating exposed information

- ▶ Get a new set of data
  - ▶ Drop social media accounts
  - ▶ Change online services
  - ▶ Change account names
  - ▶ Change email addresses
  - ▶ Change physical locations
  - ▶ Investigate anti-stalking/harassment services in your area



# Mitigating exposed information

- ▶ Grow more cover
  - ▶ Seeding false/misleading information
  - ▶ We can do this beforehand as a preventative measure also

# Wrapping Up

- ▶ Doxing is one of the many aspects of information reconnaissance
- ▶ Doxing is often used as a precursor to attack
- ▶ There is a general process for doxing
  - ▶ We may see some variations in the process and tools used
- ▶ Once we have a handle on the process used, we can take steps to defeat it
- ▶ Once doxed information has been exposed, we have problems, although there are mitigating steps that we can take

- ▶ Questions?
- ▶ I can be reached via:
  - ▶ [Jason@polyhack.com](mailto:Jason@polyhack.com)
  - ▶ @jason\_andress on twitter