Let’s Talk About Passwords

Security is hard so go get yourself a password manager

June 14-16, 2017

Nick Lozano

Director of Technology

The Council

CFO & FINANCE MANAGERS Conference

Lots of Stuff is Getting Hacked

- Recent Breaches where user name and passwords were stolen.
- Each of these has been dumped publicly and is readily available via various sites on the web.
  - MySpace 359,420,698
  - LinkedIn 164,611,595
  - Adobe 152,445,165
  - Dropbox 68,648,009
  - Ashley Madison 30,811,934
  - Experian 7,196,890
  - Vtech 4,833,678

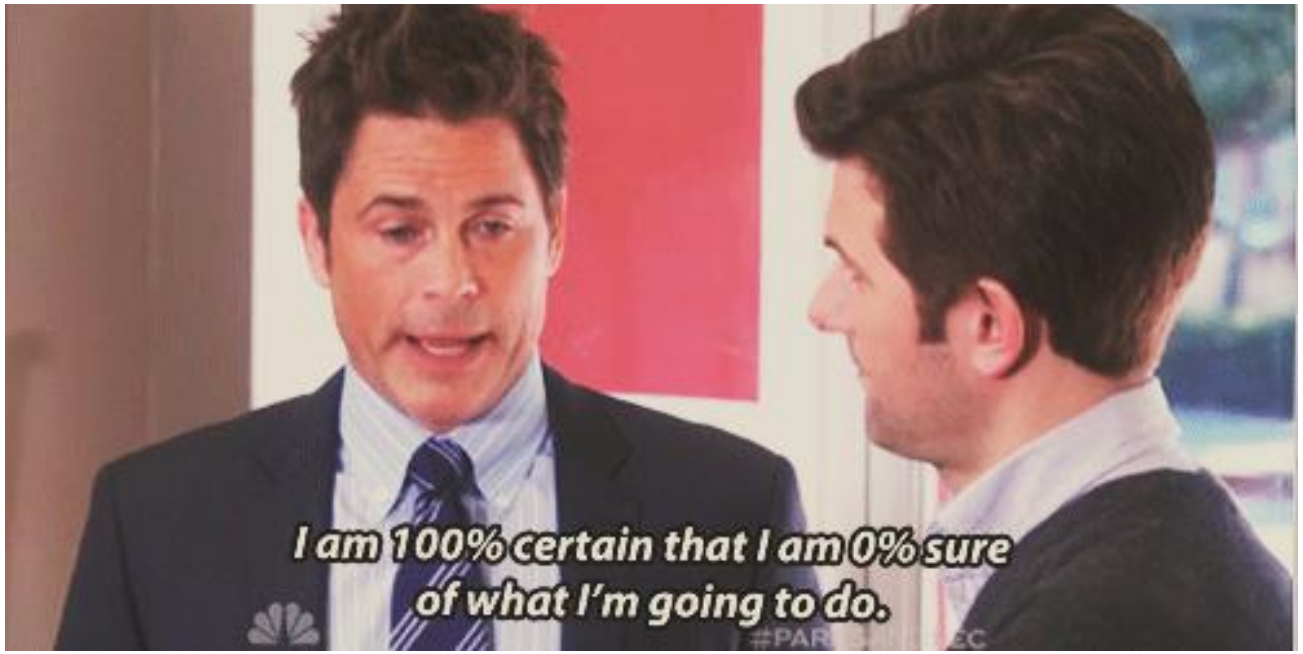
Source: https://haveibeenpwned.com/PwnedWebsites

How Are Hackers Obtaining Credentials?

- Breaching website or online service
- WiFi traffic monitoring
- Phishing attacks
  - Email
  - Phone calls
- Brute Force
- Security is hard and development mistakes happen

Website Hack demo

- http://hackyourselffirst.troyhunt.com/



Why the Breaches are a Big Deal

- **Password Reuse**

Hacked By OurMine Team - R…

Hey , we are just testing your security ,please dm us for contact! twitter: https://twitter.com/_OurMine_

3	6	2	13.2k	127
Boards	Pins	Likes	Followers	Following

Top 20 Passwords

- 123456
- password
- 12345678
- qwerty
- 123456789
- 12345
- 1234
- 111111
- 1234567
- dragon
- 123123
- baseball
- abc123
- football
- monkey
- letmein
- 696969
- shadow
- master
- 666666

Source: https://github.com/danielmiessler/SecLists/blob/master/Passwords/10_million_password_list_top_100.txt

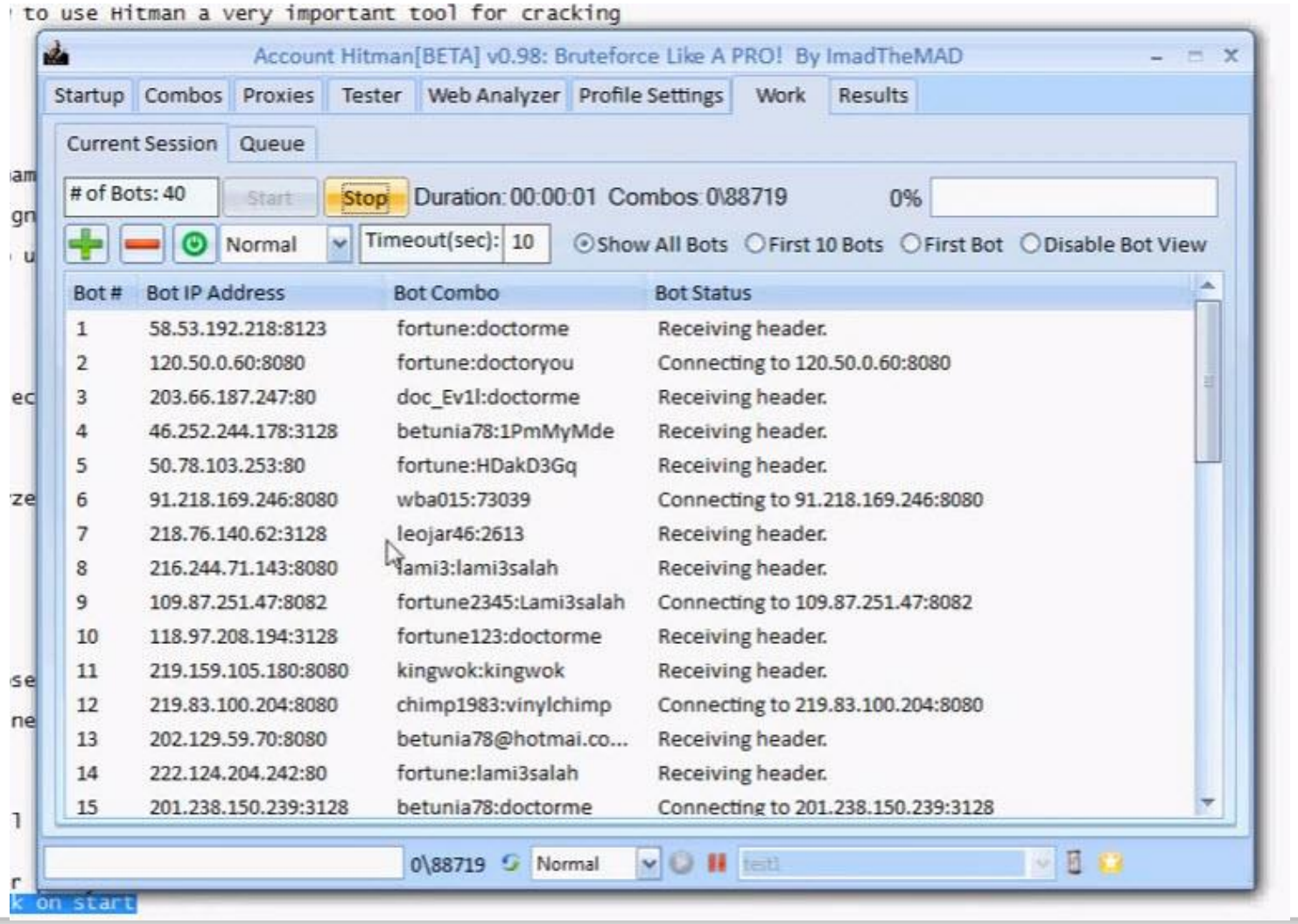
Why is Password Reuse Bad?

- Hackers can use “Credential Stuffing”
  - Credential stuffing is the automated injection of breached username/password pairs in order to fraudulently gain access to user accounts. This is a subset of the brute force attack category: large numbers of spilled credentials are automatically entered into websites until they are potentially matched to an existing account, which the attacker can then hijack for their own purposes.

Credential Stuffing

- Very effective due to the password reuse problem
- Hard for organizations to defend against because a successful "attack" is someone logging on with legitimate credentials
- Very easily automatable; you simply need software which will reproduce the logon process against a target website
- There are readily available tools and credential lists that enable anyone to try their hand at credential stuffing

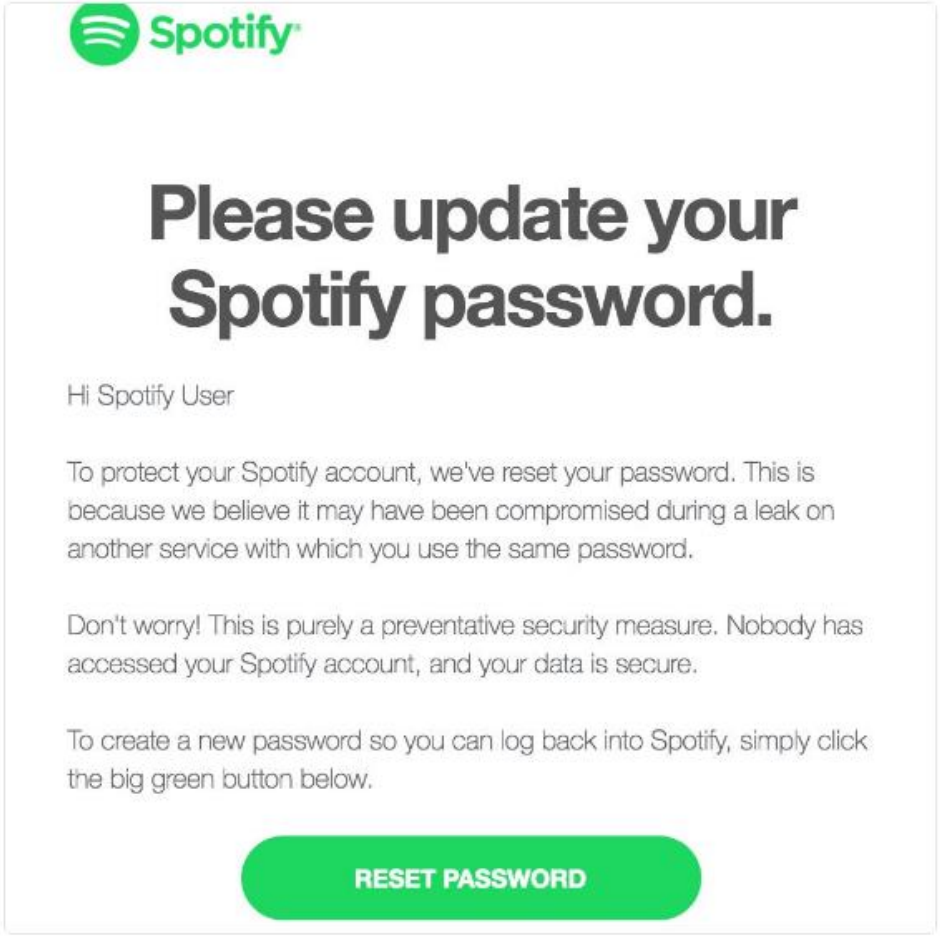
Credential Stuffing Software



What Tech Companies are Doing

- Proactive in looking for risks associated with credential stuffing
- Searching the web for account dumps
- Proactively resetting passwords

Spotify Proactive password Reset



Credential Stuffing Prevention

- Multi-Factor Authentication
- Multi-Step Login Process
- IP blacklists
- Device Fingerprinting
- Disallow Email Addresses as User IDs

Source: The Open Web Application Security Project

What can you do to protect yourself

- Use a password manager
  - Lastpass
  - 1Password
  - Keepass
- Generate a secure password for every account
- Be vigilant of Phishing scams

Remember Nothing is Ever Perfect