**LBMC Information Security Cybersecurity Sense Podcast Show Notes**
**Author:** Bill Dean
**Episode:** 7
**Date:** September 14, 2017

## Another Massive Data Email Breach

### DailyMail—Change You Email Password Now!

- More than 700 million email accounts and millions of associated passwords have been leaked in the biggest spambot dump ever.
- Troy Hunt was the first to raise the alarm.
- Troy runs the www.haveibeenpwned.com data breach lookup site.
    - Troy says it "makes it the largest single set of data I've ever loaded into HIBP."
    - He added: "Just for a sense of scale, that's almost one address for every single man, woman, and child in all of Europe."
    - He also added: "The first place to start is with an uncomfortable truth: My email address is in there. Twice."
- The data leak is believed to have originated with a Dutch spambot called Onliner.
- The information was leaked after cyber criminals allowed visitors onto their servers to download their database without needing a username or password.
- The bot behind it is designed to spread malware that steals bank details and causes people's devices to transmit the virus, as well as pumping out spam messages used by internet criminals in online scams.

### Risks

- Breaches of this scale and impact are not new (DropBox in 2012, LinkedIn last year, and Adobe quickly come to mind). They came to mind quickly as I quickly ran my personal account through www.haveibeenpowned.com to see that I was impacted and the technical details of each breach.
- Although this was not your organization, what is the risk to your organization?
    - Shocker: Your users reuse passwords. This includes the passwords they use at your organization, and there is nothing you can do about it.
        - With a little bit of work, it is not difficult to match users to employers.
        - This was especially the case with LinkedIn.
        - Believe it or not, some users use work addresses to register.
            - In working through some branding concerns, myself and another colleague reviewed the Ashley Madison breach. We were shocked at how many users registered with their work email accounts.
    - I must give another plug for multi-factor authentication here.
    - Attackers use this information for phishing and spear phishing targets.
        - With the LinkedIn breach email addresses publicly available, why look anywhere else?

        - With this data, we no longer need to spend extensive time researching email targets since most all of the addresses we want are in this database.
        - With the time savings on compiling email addresses for the target organization, we invest that time on better phish messages, infrastructure, and developing harder-to-detect malware to embed into our attachments. You can be certain that true attackers are doing the same.
- Let's discuss the obvious risks to you, your family, and friends from a personal perspective:
    - Check and see if your address was part of the breach at www.haveibeenpwned.com.
        - Yes, it is safe.
        - For the future, set alerts for yourself and your family.
    - Another site I use is: breachorclear.jesterscourt.cc.
    - Change your password to a unique password for each site.
        - I know this is a pain, but so is getting hacked.
    - For your "important" online accounts (Apple, Gmail, Amazon, etc.), configure additional security:
        - Multi-factor authentication
        - Alerts for failed excessive failed logins
    - Try not to save your password in the browser.
        - Malware can extract these saved passwords from your browser.
        - To demonstrate how simple, check out the Nirsoft tools at http://www.nirsoft.net/utils/web_browser_password.html.
        - There are also some other very cool forensics types tools there that are free to use.

**Key Takeaways:**

- One of the largest email data breaches just hit the Internet.
- While it was not your organization directly, there are risks to your organization.
- There are obvious personal risks that you should address for you, your family, and your friends.

*Bill Dean is a Senior Manager at LBMC Information Security. While involved in various aspects of LBMC's security services, he is also the practice lead for the organization's incident response, forensics, and litigation support practice.*

**References:**


http://www.dailymail.co.uk/sciencetech/article-4836496/More-700-million-email-addresses-leaked-spammers.html

https://haveibeenpwned.com/

https://twitter.com/haveibeenpwned

https://twitter.com/troyhunt

http://breachorclear.jesterscourt.cc