Exploitation of data breaches for executive protection

xorl.wordpress.com/2021/05/03/exploitation-of-data-breaches-for-executive-protection/

May 3, 2021

leave a comment »

People that know me or work with me are well aware of my efforts to expand the scope of threat intelligence functions beyond the cyber domain. I have published posts, presented use cases, and have done a lot practical application of that with various organizations in both the private and public sectors. And just to be clear, I'm not a lawyer so make sure you do your due diligence, and as always, everything mentioned here is my personal views and are not related by any means with my employer.

Now one topic I'd like to cover here is how can a threat intelligence capability exploit the incredible amount of breached data that are constantly appearing to improve Executive Protection (EP). I'll pick two examples here:

- Facebook data breach (533 million accounts)
- Dating & adult websites breaches (there are like a dozen in just Q1 2021)

Facebook use case

Data breaches almost always provide some information that you didn't have before. For example, the Facebook one allows high confidence correlation of an email with a phone number and a Facebook account (at a minimum). Here are two ideas on how to exploit this for actionable EP (also sometimes called protective) intelligence:

1. Look if details of your executives or their family members are leaked. If so, recommend them to change their phone numbers or be prepared to receive fake threats, phishing links, etc. If you implement proactive security controls on mobile phones (via some MDM solution), then you can even mark those as high risk accounts due to the discovered breached data.
2. Use the breached data to enrich your analysis on individuals threatening your executives. For example, search if the phone number corresponds to a Facebook or email account and vice versa. Once you have a lead, build a threat actor profile and share it with the appropriate law enforcement agency along with the threat your executive received.

DATING & ADULT WEBSITES use case

I had a quick look in two data sets from recent data breaches of such websites (one popular dating website and an adult content one) and identified over 3000 registered users with corporate email addresses, and even some from government email addresses. If I was a criminal or a foreign intelligence service, that would be a treasure trove. I could use that for extortion, recruitment, or any other malevolent action. Now, as a threat intelligence function we can also exploit this and here are a couple of ideas for that:

1. If you identified such records, proactively notify the victims with a carefully crafted explanation of how those data are likely to be used in the near future for sextortion scams, blackmail, or even recruitment pitches. Recommend them to change those contact details to avoid this threat altogether recommend the use of fake personas for such websites in the future.
2. If you identified a threat actor that was after your executives using any of those websites, then use it when building their psychological profile and exploit it as a lure to trick them into providing you more details (whether this is through elicitation or technical means).

I want to stress the fact that those two are just some examples. Each data breach provides another piece to the puzzle a person's online life, and given enough of them you can have an incredible amount of detail which could be utilized in dozens of threat intelligence areas. Here I focused on EP but the same data are priceless for:

- Attribution & de-anonymization
- Threat actor profiles
- Threat actor tracking
- Malware analysis enrichment
- Threat actors/groups correlation
- Fraud investigations enrichment
- etc.

Written by xorl

May 3, 2021 at 12:30

Posted in threat intelligence