The Economics of Cybersecurity — Lecture 9 Notes

Adam Hastings

March 19, 2024

1 Hack for Hire: Exploring the Emerging Market for Account Hijacking

- Let's revisit the key points from this paper.
  - What is a honeypot?
  - Setup: Creating fake personas
    - Victims were U.S.-based
    - Always used Gmail-based email address
    - The authors created victims in the native language of the hacking service ("Natasha Belkin"). Why?
    - How did the authors create the illusion that these were real email accounts? (Enron email corpus w/ changed dates & names)
    - How else did the authors create the illusion that these were real people? (Fake Facebook accounts, blogs, fictitious small business. Also fake associate personas as well!)
    - Do we think this worked? (The majority didn't even attack! Outright scam, or did they smell something was fishy? If the latter, how would they have known?)
  - What were the key findings?
    -
- What do we think about the fact that email is more or less considered the root of trust for most online activities?
  - Who benefits from this arrangement?
  - What are the risks?
  - What are the alternatives? (Hardware-backed tokens? What are the downsides here? The costs?)
  - Is it surprising that email compromise is a significant target for attackers? Probably not.
- What is *targeted* attacking?
  - How is it different from untargeted attacking?

  - How common is it?
  - Which one is more profitable?

- What are the economics of targeted attacking?

  -

- What can we learn from this style of research?

  - What are the ethical concerns here?
  - Could this data have been collected any other way?

- Let's talk about the economics elements of this work.

  - The authors found that attackers want to double their pay if the account hijack requires a 2FA bypass. Can we use this as a proxy for the "cost" that 2FA imposes on an attacker?
  - Why or why not?
  - If so, is this a reasonable method of doing cost-benefit analysis of security defenses? Can we rank the efficiency of defenses based on the ratio of (cost) : (cost to compromise)?
  - If so, can we do this for all types of defenses? Why or why not?
  - If so, who should pay for this type of research? Academia? Government? Industry? What if the attackers find out they've been honeypotted?

- If the average cost to compromise is $300, what are the implications?

  - The economics of the cost of this service mean that there must be a significant reward for doing so.
  - This means that either the financial reward must be big (maybe it's the email of a high-ranking business executive, and compromising their email can enable lucrative BEC scams)
  - OR you are not motivated by money. Maybe you are a spy agency trying to gain intelligence on someone.

- What can be done to reduce this type of crime?

  - As mentioned earlier, increase the adoption of authenticator devices.

- What has changed since 2019, when this paper was published?

  - Surprisingly little, it seems. I sort of remember SMS-2FA starting around 2016 maybe. And this still seems to be the status quo, eight years later.
  - I wouldn't be surprised if these results replicated today.