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! And fake buyers, of course)
    - 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?)
  - Setup: Monitoring Infrastructure
    - Email Monitoring, Login Monitoring, Phone Monitoring, Website Monitoring
    - Anything else tney should have monitored?
  - Setup: Hacking services
    - Most communication not in English. Surprising?
    - A common piece of advice in corporate security trainings is to look out for emails with bad grammar or spelling. What do we think about this? Is it fair? (Probably, yes)
  - Setup: Legal and ethical issues
    - What did the class think?
    - Let's talk about the legal aspect (IANAL).

      - The big law that affect hacking is the Computer Fraud and Abuse Act (CFAA) whic prohibits "unauthorized access". They don't violate the CFAA though because they the targets are under their own control and are hence not "unauthorized".
      - The other legal aspect is that they explicitly gained permission from Google to knowingly break GMail Terms of Service.
      - Why do you think Google's legal team allowed this exception? (probably because the results benefit Google—either they learn something new from the research, or they look good to the community by allowing such research.)
      - Look up Van Buren vs. United States for a 2021 ruling on the Computer Fraud and Abuse Act (CFAA)
    - "Not considered human subjects research by our IRB" — surprising? Because "it focuses on measuring organizational behaviors and not those of individuals." (sound a bit like Linux PR fiasco cop-out)
    - Nonetheless it does seem like they at least consulted their IRB.
    - Ethics of funding criminal enterprises? What do we think?
    - What about the ethics of harming criminals? If their actions are identifiable. Recently there's been a bit of reporting on "pig butchering" scams (confidence scams typically invovling cryptocurrencies) and it turns out that many of the scammers on the other end are themselves the victims of trafficking or extortion and are working under fear of retaliation from various criminal organizations. Should we be concerned about these people's welfare in our studies?
  - What were the key findings?
    - 4 out of 5 relied on phishing. Is this in line with what we saw in the ransomware reports? Yes—the majority of exploits start with some kind of social engineering (and FWIW, the malware attack failed!)
    - Technical exploits exist, and systems are often unpatched, and may be more reliable than social engineering. So why did most attackers still choose to use social engineering? (Answers: It's cheap; don't need technical sophistication; don't need to "burn" 0-days on low-value targets; Some services (Gmail, Windows) already do a fair amount of virus scanning/spam detection/automatic patching)
    - Keep in mind—these are probably not the more elite of the elite crew of hackers here.
    - Most efforts started with sending emails.
    - What were some of the lures? (personal associates, banks, government, Google). Google makes sense since the attackers were after the Gmail account (same login info).
    - What did the attackers do to trick people? (Fake URLS a la www.googlesupporthelpdesk.com or even phony 2FA flow!)
    -

- 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.