The Economics of Cybersecurity — Lecture 9 Notes

Adam Hastings

March 19, 2024

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

- What is *targeted* attacking?
  - How is it different from untargeted attacking?
  - How common is it? I don't know.
  - Which one is more profitable? I don't know.
- 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.

1.1 Setup

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?

1.2 Hack for Hire Playbook

What were the key findings?

- No brute force efforts, attempts to contact directly by Facebook, attempts to communicate with affiliated personas.
- 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 e.g. www.googlesupporthelpdesk.com)
  - Easily bypassed 2FA by phishing for codes.
  - What's the name for this style of attack? Man-in-the-middle (or monkey-in-the-middle if we'd like to be gender inclusive. Or given Alice/Bob/Eve/Mallory, should be Woman in the middle IMO!)
  - Can this be defended against using technology? Yes, FIDO2 authenticators sign a challenge given by requesting protocol and encrypt it using TLS and the signing key is authenticated by a certificate. So it defeats this man-in-the-middle attack. But they cost \$40.
- Malware attempt was hilariously low-effort (sent a RAR hoping victim would click on it. Didn't work and the attackers gave up).

1.3 Real Victims & Market Activity

- Google was able to analyze attack patterns (details are lacking)
  - Services A, B, and E targeted 372 attacks during a seven-month period (lower bound, unsuccessful attacks unknown). Which averages out to 4 a week per service.
  - Let's ignore the overhead involved in hacking, since they are probably pretty small anyway.
  - Recall that the average cost is \$200/compromise. I.e. attackers are making \$800/week
  - Some quick internet searching found me that the median weekly wage in Russia is about \$300/week

  - And the median monthly wages in China is about $100.
  - For reference, the median weekly wage in the United States is about $1000/week.
  - You often hear about Russian or Chinese hackers, and I think this is why. It financially does not make sense to be a hacker (or at least this type of hacker) in the United States. It pays less than the median wage, when you could be making much more working in tech!
  - But if you're in a poorer country, you could be making several times the national weekly wage by being a scammer. (Again there are overheads, but probably small? What might they be?)
  - What are the solutions? We can't pressure their governments to go after them (safe harbor in some cases!) Should we give them all work visas?

- Can we use market prices as an estimation of a product or service's security posture?
  - E.g. it costs four times as much to attack a Gmail account than a Mail.ru account. Is Gmail four times as secure? Why or why not?
  - Recall last class when we talked about the cyber insurance underwriting process. From what we know, it seems like cyber insurers are hilariously bad at estimating their customers' security posture (recall very basic questionnaires?). Whereas black market prices may in fact represent the true cost of a breach. What do we think?
- The authors don't actually name the platforms or services they used to connect with hackers. Presumably to make it harder for people to find. What do we think? Should they have named where they actually found the hackers? My understanding is that most of this happens on the dark web (TOR) or maybe these days over private e2e messaging services like Telegram (but I don't really know).

1.4 Discussion

Let's talk about the economics implications 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?
- 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.
    - The authors remarked that they thought this was a fledgling, immature market with poor customer service. How does that compare to what we read about with the Conti ransomware group? They had health insurance!
    - By comparison, the authors remarked that markets for CAPTCHA solving, Twitter spam, and other activities had better customer service and more established pricing, which may indicate a more mature market, and that account compromise may be a "side hustle". After all, they were only compromising four account a week on average.
    - What were the trends on business email compromise? Anyone remember? It's increased from 2019 (but actually decreased from last year! Just checked the new IC3 report).

2 ContiLeaks

2.1 Part I: Evasion

- Who's the author? (Brian Krebs, a longtime cybercrime reporter and investigator. Not a technical backgroud, but still a widely-read resource in the field)
- What is a botnet?
- Who was/is Conti? Russian cybercrime group. Focused on ransomware. $100M in annual revenue with 100 salaried employees. That's $1M an employee!!! (For reference—Fortune #500 has revenue of $7B. Only off by one order of magnitude.)
- Interesting mix of technology and geopolitics. Conti said they were not aligned with any government and condemn the war, but will "use our resources to strike back if the well being and safety of peaceful citizens will be a stake due to American cyber aggression".
- We often hear about hackers from Russia, China, Iran, North Korea. What about the US? Is Conti's complaint here valid? If this were a class on cybersecurity economics in Russia, would we be talking about American hackers?
    - I don't know. The economics of it don't really make sense (see above). But we know the US Government is a cyber superpower and snoops around in other countries. Do they target civilians? I don't know.
- Where did this data come from?
    - One researcher said that the "the person who leaked the information is not a former Conti affiliate as many on Twitter have assumed. Rather, he said, the leaker is a Ukrainian security researcher who has chosen to stay in his country and fight."
    - "The person releasing this is a Ukrainian and a patriot, Holden said. Hes seeing that Conti is supporting Russia in its invasion of Ukraine, and this is his way to stop them in his mind at least."
    - Leaks are from a six-month period in 2020
- Some of the things I found interesting:

  - “The one who made this garbage did it very well” (on NSA interruption of Trickbot botnet). US is a cyber superpower! Clearly know how to reverse attackers’ code/high level of technical sophistication. Had clever way of taking down hacked botnets.
  - What do we think about this? Tax-funded disruption efforts. Is this cost effective? Probably!! Any other concerns?
  - They targeted USA healthcare services because the USA interferes in their actions. Thoughts?
  - Hired legal defense for an arrested worker Alla Witte
  - Arrest of 14 people working for REvil. Krebs cites experts “believe the crackdown was part of a cynical ploy to assuage (or distract)” before invasion of Ukraine. So...safe harbor or not? Challenges prior assumptions.

2.2 Part II: The Office

- Conti ran like a small business—budgets, schedules, HR department!!
- Departments—Coders, testers, Administrators, Reverse Engineers, Pen Testers/Hackers
- Ads on Russian-language cybercrime forums — $1–2k salary (monthly—not specified) = $12k–$24k annually, internally believed $5-10k salary (monthly) (up to $120k annually). Recall that Russian median wages are about $16k. An OK job. But most of the money going to the top bosses ($180M revenue!!)
- Employees complained about boring and repetitive work, and not being able to take time off
- Despite the organization, still seemed quite disorganized (can’t keep track of alive bots, etc.)

2.3 Part III: Weaponry

- Paid for EDR antivirus!
- Heavily budgeted for OSINT tools
- Set ransom payments to be a percentage of victim’s annual revenues!!!! [CITE IN PAPER]
- How can an illegitimate business buy a license to Cobalt Strike? Have another legitimate company purchase it on their behalf
- Also invested in security research—finding and exploiting vulnerabilities (reversing Patch Tuesday patches?)
- Pros and cons of attacking insured companies (more likely to pay out, less likely to pay huge ransoms)
- “Double extortion” — pay to decrypt, pay to keep data secret. Attackers need to build up a reputation of keeping their word!

2.4 Part IV: Cryptocrime

- (Idea: Distract cryptohackers by “heavenbanning” them)
- There was interest in smart contracts. What’s a smart contract?
- Interest in crypto market manipulation