The Capital One breach is more complicated than it looks



On Monday night, Capital One and its customers got some very bad news. The company had been breached, spilling hundreds of thousands of social security numbers and account details into public view. The New York Attorney General is already investigating whether Capital One is negligent, but the broader story is familiar: a big company let a lot of sensitive data go missing, and customers bore most of the risk.

But the closer you look, the stranger the story is. The alleged hacker, Paige Thompson aka “Erratic,” was caught and charged at the same time the breach became public, and she didn’t seem interested in covering her tracks. We don’t know exactly what she did with the data once she got it, but she doesn’t fit the profile of most scammers, who tend to sell information like this on underground marketplaces as soon as they can. At the same time, the initial vulnerability seems to

have been more of a server misconfiguration than an out-and-out exploit, leading some to wonder if Thompson might have been a well-intentioned researcher who went a little too far. We still don't know what she was after in collecting this data, but there are still far more questions than answers.

"don't go to jail plz"

The biggest anomaly is how the breach was discovered in the first place. According to the federal complaint, the breach took place in stages across March and April of 2019. But Capital One only became aware of the problem on July 17th, when someone tipped the company that their private data had been uploaded to a public GitHub page. From there, it was straightforward for investigators to discover whose page it was and how they had obtained the data.

It's hard to overstate how unusual this is for a breach case. Usually the data is only discovered after it's passed through several intermediaries, and it's rarely so easy to pin down exactly when and how it was taken. It took years to track down all the various people involved in the Target breach, to pick one example. The prosecutions revealed a completely different kind of organization: one party making the software, another party using it to harvest credit card data, which was then sold to another group who used it to commit fraud. Prosecuting all those people meant a massive international effort, centered on Latvia and Eastern Europe. In contrast, Thompson was taken into custody less than a month after the initial tip.

We don't know why Thompson decided to post the data on a public GitHub page, but there's reason to think that she genuinely didn't see what she was doing as criminal. She openly described her techniques on Twitter (that's part of the reason we know so much about how it happened), and doesn't seem to have been shy about sharing information. The rest of what we know comes from a Slack room maintained by Thompson. I was able to gain access to that Slack room until it came

offline yesterday, along with a number of other reporters, and Thompson's conversations around the breach were alarmingly casual. Immediately after an account named "Erratic" listed the contents of the dump, a friend replied, "sketchy shit… don't go to jail plz."

Thompson seemed aware of some danger, but not the scale of the threat. "I wanna get it off my server, that's why I'm archiving all of it, lol," Erratic wrote back. "It's all encrypted. I just don't want it around, though."

The technical details of the breach make it more complicated still. What Thompson did was only possible because Capital One had misconfigured its Amazon server. Thompson had worked at Amazon years earlier, so she's been described by some as an "insider threat." But sniffing out this kind of misconfiguration is a common pastime for security researchers. (UpGuard Security in particular has built a good reputation just from scanning for misconfigured servers.) Those misconfigurations are so common and so easily fixed that they're usually not even considered a breach, although of course verifying those instances without violating any laws can be a delicate business.

It can be hard to tell the difference between security research and criminal enterprise from the outside. None of these facts are an indication that Thompson isn't guilty of what she's been charged with. As long as she took the data, the law doesn't care why she did it. We genuinely don't know why she took the data, or why she held onto it for months without reporting the issue to Capital One. We don't know if she tried to report it in some way, or if she tried to profit off the data in ways that haven't yet come to light. Thompson herself may have had trouble knowing which side of the law she was on. But as we describe Capital One's problems in the same terms as previous breaches, it's a reason to think this one is more complicated than it looks.

https://www.theverge.com/2019/7/31/20748886/capital-one-breach-hack-thompson-security-data