On Cybersecurity and Being Targeted

2016

3 min read • 570 words

Last month, I was the subject of a targeted cyber attack. Someone went through substantial lengths to attempt to gain access to my GitHub account, but were thankfully unsuccessful because two-factor authentication was enabled.

Account security is something that I've always considered myself to be rather pragmatic about — I use randomly generated passwords for extremely important accounts and services, like GitHub, especially if they are likely to be subject to systematic intrusion attempts.

In this instance, though, the attack vector was DNS. My account at the not-so-incredibly-common DNSimple.com did not use a highly secure password. I didn't think it was necessary, as in my mind, the only reason that the security of an account like that would be at risk would be if I was the explicit target of an attack. Once again, I thought to myself "That's something that only happens to other people".

What happened?

I was sitting at my computer in the evening one night, when I get an unexpected text message from GitHub, providing me with a one-time-use login token. I immediately started investigating.

- Received GitHub 2fa token via SMS.
- No longer able to access GitHub account (locked out).
- Contacted employer’s on-call security engineer, was successfully removed from the company GitHub org immediately.
- Contacted friend at GitHub, confirmed no access to the account had actually been made. Got an IP address. Confirmed with him that GitHub sent a password reset email, and that it was sent successfully (which I never received).
- DNS must be compromised. Logged into DNSsimple account, noticed all MX records from my personal domains had been removed.
- Immediately locked down the DNSsimple account with a highly secure password and restored MX records.

This all took place within ten minutes.

In the day or two that followed (it was the weekend), I monitored things closely to ensure that the threat had been mitigated. I got in touch with DNSsimple to confirm the times of any MX record changes, and get the source IP address (it was the same). Once I was confident that things were back to normal and secure, I reset my own GitHub password one again, so I could have access to it, and on Monday was added back into the company’s GitHub org.

What the hell?

Totally crazy. Someone went to extreme lengths, hacking DNS configuration to intercept a single password reset email (I received all other emails except that specific one), to gain authorization to my GitHub account. Why?

I have two best guesses:

1. They wanted access to my company's private code.
2. They wanted to maliciously modify the Requests codebase (or Certifi, the CA bundle that is shipped with Requests).

Unfortunately, it seems as though #2 is the most likely answer. A crafty entity (like a government, for example), could possibly create a vector into systems running in almost every major tech corporation by adding a special certificate key to the project.

Luckily, the process that we use to generate the bundle is well regulated, highly auditable, and extremely repeatable. Unless they were crafty beyond our imagination, we would have noticed.

But, one can only wonder.

Is this normal?

Well, it turns out this exact attack has occurred to at least one other person on the internet. However, the prize the attacker was after was not source code, but a Twitter handle, worth $50,000. They were successful.

Takeaways

- Knowing people is very useful.
- Turn on two-factor authentication. **Right now**.