Todd Crandall

Andrew and DJ

Devmountain Foundations-20

03/24/2022

Major Cybersecurity Breaches in the Last 20 Years

Despite being viewed by many as a field of study too dense to break into, Cybersecurity is and has been quite penetrable in the last two decades. The industry itself is really only 35 years old and is still experiencing growing pains as a well as a “maturation period” of sorts. Looking back at just a few of the largest breaches in the brief history of this industry will reveal “important milestones and lessons on where the industry is heading.”

The first of these attacks was on the internet domain as a whole. “In 2002, a malware attack nearly brought the entire Internet to its knees.” Domain root systems, of which there are thirteen(think .edu, .com, .org), allow access to websites. “Hackers target all [of] those domains, which are critical infrastructure for the internet, via a denial-of-service attack and made the Internet unusable.” The downed domains only lasted about an hour, but “the attack showed the possibility to affect the whole internet with a targeted cyberattack.”

Another large incident was the Stuxnet Virus. Discovered in 2010, “Stuxnet was a malicious computer worm designed to interfere with the industrial control systems, which controlled Iran's nuclear program at the time.” It was believed to have infected more than 200,000 computers and caused over 1,000 machines to physically degrade. “It was the first incident of using a computer virus to manipulate the physical world.”

One of the largest breaches in history, and the largest of its time, was the Yahoo breach in 2013. More than 3 billion users suffered from leaked information as it exposed the entirety of the database. It was a massive data breach that caused the general public to become aware of the need for cybersecurity since Yahoo was a leader in the early Internet and webmail services. This was one of the first breaches in security that affected people on a personal level.

A more recent breach that has an impossible number of victims is that of Apple’s iPhone. In 2019, a data breach was discovered that could bypass security certificates and access encrypted data like saved passwords, financial information, and pictures. Experts said that the breach had occurred a few years prior and it was impossible to know how many users were infected or how much data was compromised.

Finally, the most recent attack on this list was one that affected thousands. The target was the Colonial Pipeline. Essentially hackers ransomed the information and access to the pipeline, leaving thousands without gas and fuel. This set in the real-world implications of a cyber attack on something as necessary as gas for people's lives.

Each of these events show how much things can change in such a short time. From website denial to resource ransom. There will likely be additional cybersecurity attacks in the future ransoming common needs because those are things people will pay for to have restored. If anything can be learned from all of this, it’s that cybersecurity cannot be taken lightly. As technology and the creativity of the degenerate evolve, so must the ability to keep those people/groups out.