Stanford eCorner

Ominous Threats Create Opportunities

Jay Kaplan, *Synack*

December 07, 2016

Video URL: http://ecorner.stanford.edu/videos/4868/Ominous-Threats-Create-Opportunities

Jay Kaplan, co-founder and CEO of cybersecurity startup Synack, describes the immense need for technology experts to combat the ubiquitous threat of malicious hackers. He mentions high-profile attacks on major businesses and organizations, but also demonstrates how even an inconspicuous online account can be attacked within minutes by automated hacking programs.

Transcript

- Cyber security's a really big problem today. Company after company is getting compromised, getting breached. You hear about the Target breach, you hear about the Anthem breach, you hear about Sony, JPMorgan Chase, you're hearing lately about these hospitals who are getting hacked and then hackers are basically locking down their systems and saying, unless you pay us this ransom, we're not gonna unlock any of the systems. It's a big problem, and I think you guys are very aware of it now because it has gained such mainstream media adoption that it's something that we might've not thought about before, but everyone's thinking about it today. And the threats are really everywhere. The real problem here is that the actual cyber security talent is not. We have a huge shortage in this industry. Right now there's over 1,000,000 cyber security jobs that remain unfilled, and over 70% of the security professionals within the organizations trying to hire for these positions are saying that this shortage does direct and measurable damage to the organization itself. Frankly guys, it's way too easy today to break into any organization's network, application, whatever you're trying to break into, if you have the right resources, expertise, and motivation. Definitely learned that in my time at the NSA.

I was focused on the counter terrorism mission. Basically tasked with targeting foreign terrorist communications and so forth. It was an incredible job, but it definitely opens your eyes and gives you a pretty unique perspective on this space. Today it's like bringing a knife to a gun fight right? The attackers are well-resourced, they have very, they have a lot of motivation, they have a lot of money. Different states are ultimately funding this, right. So how does an organization that might even be smaller defend against these attacks? It's just not fair right? Clearly there's a need, and it's a need that we saw. So you're probably thinking to yourself, okay yeah this is a problem for big companies right, big enterprises, JPMorgan, Anthem, all of these companies are huge. So who would want to attack a smaller company? Or who would want to attack maybe one of you guys? We did a little bit of an experiment. We said why don't we put just a random box on the internet, not attribute it to anyone or anything. And we said this is called a honeypot, in the cyber security space.

And we said let's watch what happens to this box. Put down some tools, let's monitor their traffic, let's see what people are potentially doing from the outside world. We opened up Port 22, which is the, basically the port used to connect to that remote machine from the outside, and within five minutes we started to see unauthorized login attempts. We actually registered almost 100,000 login attempts on that machine. What does that say? It means that there's automated attackers all over the world just looking for anything that's vulnerable on the open internet, right? You can kinda see here, it's a little bit hard to see, but they're running through a dictionary attack. So basically going through the entire dictionary and trying to login using just you know random usernames and passwords.