PHYS ORG

Massive cyberattack poses policy dilemma, scholar says

October 25 2016, by Clifton B. Parker

The coordinated cyber attack that crippled parts of the internet on Friday highlighted key policy problems, a Stanford cybersecurity scholar said.

And while the problems were clear, there are no easy solutions, said Herbert Lin, a senior research scholar for cyberpolicy and security at Stanford's Center for International Security and Cooperation. A research fellow at the Hoover Institution, Lin serves on the President's Commission on Enhancing National Cybersecurity.

Beginning early Friday morning, several major websites including Twitter and Amazon went down for most of the day, and many other sites were inaccessible. The FBI and the Department of Homeland Security are investigating what is described as a DDoS (distributed denial-of-service) attack. The attacks mainly focused on Dyn, one of the companies that run the internet's domain name system (DNS).

The Stanford News Service interviewed Lin about the issue:

What happened on Oct. 21?

It was a distributed denial-of-service attack on a major internet services provider. The company operates much of the internet's infrastructure. It's not a consumer-facing company, but is in between the user and a company like, say, Amazon. These attacks centered on the domain name system (DNS), which is the service that translates something like a

Stanford email address into a numerical IP address. People remember Amazon-dot-com, but they don't remember the numerical IP address (which is actually where a company like Dyn sends web users going to a site like Amazon). What a DOS attack involves is the flooding of this (Dyn) company's servers with millions of fake requests from sources for service to go to those web sites. Being forced to process all these requests, the company can't service real people trying to use web sites. On Friday, the millions of sources making these requests appear to have been part of the Internet of Things.

What is the Internet of Things, and how did it factor into the cyberattack?

In this case, they weren't, by and large, products like your computer or mine, but were mostly smaller things like surveillance cameras, baby monitors and home routers [everyday objects that have network connectivity to the internet]. What makes these things particularly vulnerable is that they are small, they don't have much computational power in them, and they don't include many, if any, security features. In fact, a Chinese company just admitted that it didn't pay enough attention to security, and they recommend users do some things to improve security. But they shipped their products without paying much attention to security, and that's why this was a vulnerability.

What new public policies could lessen the likelihood of this happening to such a degree again?

The primary policy recommendation is that we need policy that encourages – or mandates, depending on how strong you want to be about it – at least minimal security measures for devices that connect to the internet, even Internet of Things devices. How you actually promote, encourage or incentivize that without a legal mandate is problematic, however, because nobody quite knows what the market will accept. Also, if you're going to force manufacturers to pay attention to security, you're going to reduce the rate of innovation for these products. Then there's the question of who's going to buy them, because the unsecure ones will probably be cheaper. The fundamental problem here is that guys who use the Internet of Things, like surveillance cameras, will find those cameras work perfectly fine, even if they were compromised. So they don't care about security. They have no incentive to do so. Why should they pay more to protect me?

Does this show that our November election is even more vulnerable to hacking?

At this point, it looks unrelated … But I don't know, it is all just speculation.

Provided by Stanford University

Citation: Massive cyberattack poses policy dilemma, scholar says (2016, October 25) retrieved 9 April 2024 from https://phys.org/news/2016-10-massive-cyberattack-poses-policy-dilemma.html