eklektika
Language Means Business

Taking down the Internet

Level C1/C2

Warm-up. Consider the following questions:

- Do you remember what life was like when the Internet and the World Wide Web were not around?
- What would happen if the entire Internet infrastructure were disabled for a few hours? For a few days? Think about the impact on yourself, the economy, government etc.
- How likely is such an event? How could it come about?

Someone Is Learning How to Take Down the Internet

http://www.schneier.com

By Bruce Schneier   September 13, 2016

Over the past year or two, someone has been probing the defenses of the companies that run critical pieces of the Internet. These probes take the form of precisely calibrated attacks designed to determine exactly how well these companies can defend themselves, and what would be required to take them down. We don't know who is doing this, but it feels like a large nation state. China or Russia would be my first guesses.

First, a little background. If you want to take a network off the Internet, the easiest way to do it is with a distributed denial-of-service attack (DDoS). Like the name says, this is an attack designed to prevent legitimate users from getting to the site. There are subtleties, but basically it means blasting so much data at the site that it's overwhelmed. These attacks are not new: hackers do this to sites they don't like, and criminals have done it as a method of extortion. There is an entire industry, with an arsenal of technologies, devoted to DDoS defense. But largely it's a matter of bandwidth. If the attacker has a bigger fire hose of data than the defender has, the attacker wins.

Recently, some of the major companies that provide the basic infrastructure that makes the Internet work have seen an increase in DDoS attacks against them. Moreover, they have seen a certain profile of attacks. These attacks are significantly larger than the ones they're used to seeing. They last longer. They're more sophisticated. And they look like probing. One week, the attack would start at a particular level of attack and slowly ramp up before stopping. The next week, it would start at that higher point and continue. And so on, along those lines, as if the attacker were looking for the exact point of failure.

The attacks are also configured in such a way as to see what the company's total defenses are. There are many different ways to launch a DDoS attack. The more attack vectors you employ simultaneously, the more different defenses the defender has to counter with. These companies are seeing more attacks using three or four different vectors. This means that the companies have to use everything they've got to defend themselves. They can't hold anything back. They're forced to demonstrate their defense capabilities for the attacker.

I am unable to give details, because these companies spoke with me under condition of anonymity. But this all is consistent with what Verisign is reporting. Verisign is the registrar for many popular top-level Internet domains, like .com and .net. If it goes down, there's a global blackout of all websites and e-mail addresses in the most common top-level domains. Every quarter, Verisign publishes a DDoS trends report. While its publication doesn't have the level of detail I heard from the companies I spoke with, the trends are the same: "in Q2 2016, attacks continued to become more frequent, persistent, and complex."

There's more. One company told me about a variety of probing attacks in addition to the DDoS attacks: testing the ability to manipulate Internet addresses and routes, seeing how long it takes the defenders to respond, and so on. Someone is extensively testing the core defensive capabilities of the companies that provide critical Internet services.

Who would do this? It doesn't seem like something an activist, criminal, or researcher would do. Profiling core infrastructure is common practice in espionage and intelligence gathering. It's not normal for companies to do that. Furthermore, the size and scale of these probes -- and especially their persistence -- points to state actors. It feels like a nation's military cybercommand trying to calibrate its weaponry in the case of cyberwar. It reminds me of the US's Cold War program of flying high-altitude planes over the Soviet Union to force their air-defense systems to turn on, to map their capabilities.

What can we do about this? Nothing, really. We don't know where the attacks come from. The data I see suggests China, an assessment shared by the people I spoke with. On the other hand, it's possible to disguise the country of origin for these sorts of attacks. The NSA, which has more surveillance in the Internet backbone than everyone else combined, probably has a better idea, but unless the US decides to make an international incident over this, we won't see any attribution.

But this is happening. And people should know.

Comprehension / discussion. Consider the following questions:

- What evidence is there for the claim made in the title of the article?
- What evidence is there that ‘state actors’ are behind these attacks?
- If this is the case, what could be their motives?
- How alarming do you think these revelations are?
- The author states that ‘nothing’ can be done. Do you agree?

- Consider the following comments on Schneier's revelations that some experts have made. What do you think about their arguments? Which is the closest to your position?

  "Risk levels haven't changed. It's an interesting hypothesis that needs more data points, but watch out for confirmation bias going forward."

  Sam Curry, chief product officer at Cybereason

  "Cyberwar has become like real war, except you can wage it, and possibly win it, in the sense that you can extract political concessions not to fight it at all. And the capital investment is tiny – no tanks, no fuel, just talent, time, food, and access."

  Dan Kaminsky, security researcher and chief scientist at White Ops

  "It has become easier to launch much larger DDoS attacks because so many internet of things (IoT) devices can be so easily compromised and used as part of a botnet. They are, protected with weak or hard-coded passwords. Most of these devices are available for sale on retail store shelves for less than $100, or – in the case of routers – are shipped by ISPs to their customers."

  Brian Krebs, security blogger

  "The internet is vulnerable, but it always has been. The threat is old and well known. The internet was built in a lab for eggheads who all trusted each other, and so it has no defense against its own users. But there's no way to break the Internet permanently, since the same activities that gave rise to it and which reinvent it every day will eventually recreate a new infrastructure that works mostly the same way the old one did."

  Paul Vixie, CEO of Farsight Security and previously president, chairman and founder of Internet Systems Consortium (ISC)

  "The internet was designed to survive a nuclear war. It was set up so the network could remain alive, even if parts of it get blown up. Even if the 'great server in the sky' got taken down, it would be replaced instantly."

  Gary McGraw, CTO of Cigital

DDoS attacks are escalating

https://www.youtube.com/watch?v=0wUNjy-w_GU

Comprehension / discussion. Consider the following questions:

- How have DDoS attacks changed over the years?
- Why was Akamei unable to protect Brian Krebs?
- What is Project Shield?
- What can be done to protect the Internet against the threat posed by Internet of Things developments?

John McAfee: This is why the US is losing the ‘cyber war’ to China and Russia

https://www.youtube.com/watch?v=CvfeYmdOSpo

Discussion. What do you think of John McAfee’s perspective on ‘cyberwar’ and the recommendation he gives to the US government?