November 2016

The Amazon Outage: Was it Hacking or… Something Else?

It was Something Else. As usual, the mainstream press got it wrong again. The big Amazon outage on October 21 was not a Hacking attempt, and it wasn't directed at Amazon. It was a "DDoS" attack. "DDoS" is the acronym for "Distributed Denial of Services". You might say "yeah, but what does all that jargon really mean? And "what's the difference"?

I'll give a short example: let's say you have 1,000 friends, and something big happens like you won the lottery. All 1,000 friends call your cellphone to congratulate you at the same time. Will they all get through? No. Will they all get your voicemail? No. One thousand calls at once will overload any single phone number, so most will get a busy signal. 1 person will get through, maybe 2 or 3 will get voicemail, but the rest are out of luck. Did someone hack your phone? No, but the same result (busy signal) happened from too much traffic. That is essentially what happened to Amazon – but not directly.

The real target was a domain name provider named DynDNS. DynDNS provides the domain name translator servers that convert web domain names like amazon.com, Netflix.com, twitter.com into server addresses that can deliver web pages. In essence, domain name services take the domain name you type (example: "twitter.com") and convert it to a server address like: 199.59.150.7. This is done so you don't have to remember a number, just the site name. DynDNS converts it for you. Nice. Easy.

Well, Ok. **Now let's pretend you are DynDNS and your website has excellent hacking protection, but someone has a gripe with your company.** How could they take down your very well-protected website without having to spend weeks or months trying to hack in the hard way? Easy, hack someone else who isn't protected and arrange for a flood of traffic so big that your website can't handle it all. That is exactly what happened – someone, or a couple of "someones" arranged for millions of computers and connected devices (more on connected devices later) to bombard DynDNS.com with so much traffic it could not handle it anymore, which in turn took down most of DynDNS's customers too, like Amazon, NetFlix, Twitter, and many more. Like the previous phone example, at some point there's just too many web requests to handle, and things break down.

Now, more about "Connected Devices". Connected Devices can be almost any non-computer "thing" connected to the internet, such as Web Cams, DVRs, Smart TVs, Smart Refrigerator, Smart AirConditioners, and so on. These are lumped together in a category named the "Internet of Things" or IoT for short. The next question is so how did these IoT devices attack? Easy, and you don't need to be a professional hacker: most of those IoT devices are easily discoverable on the internet, and nearly all of them run a form of the Linux operating system, which most hackers use anyway. Even worse, most of the IoT devices are set up without changing the as-delivered default passwords: "admin" or "password".

Add that all up, and you have potentially millions of connected devices ripe for the picking, and that is exactly what happened: the hackers implanted a small Linux program on unprotected DVD players, thermostats, and smart TV's that flooded DynDNS with so much traffic their system was knocked offline for 8 hours. **The challenge for DynDNS** and other service providers is how to separate junk traffic from good traffic: seconds down cost millions, and it won't be easy.

The challenge for all of us who have web-connected devices is simple: when you take your new web Thermostat, Webcam, DVR, Smart Fridge, or Smart TV out of the box, change the default password to something new…

-John Becker