THE WAY I SEE IT
Editorial

Shutting Down the Internet of Things

Friday, October 21st, a DDOS attack on Dyn Inc., brought down several major sections of the Internet including large retailers, Amazon and Ebay, and PayPal. What was different about this attack was that it was conducted by a bot army made up of devices from the Internet of Things. About 500,000 wifi cameras, refrigerators, smart thermostats, and other devices were used, in three waves to throttle Dyn's servers and keep major websites from operating.

The US Government gave as its opinion, that it was not a state-sponsored actor (the Russians or Chinese) and that was given more weight after the attacks died down shortly following the release of a notice from WikiLeaks that the rumored death or kidnapping of Russian-sponsored hacker Julian Assange were incorrect and that he was safely in the Ecuadorian embassy, as before.

Aside from the tie between Assange's followers and Russian sponsored attempts to damage the campaign of Hillary Clinton and cast doubt on the validity of the US election process, the thing that is truly scary is that it is easily possible with open source code to do this again, using IoT devices as bots.

Comments? Talk to me!
waltboyes@spitzerandboyes.com

Read my Original Soundoff!! Blog:
http://waltboyes.livejournal.com

The question becomes, do we want our refrigerators spying on us for a foreign power, or maybe used to feed data illicitly obtained to our health insurer for the purpose of finding out what we eat, how much, and when...and that's so real it isn't funny anymore.

...the attacks died down shortly following the release of a notice from WikiLeaks that the rumored death or kidnapping of Russian-sponsored hacker Julian Assange were incorrect and that he was safely in the Ecuadorian embassy, as before.

Of course, the Industrial IoT is somewhat different, and is unlikely to be any great part of such an army of IoT device bots.

Why? Most of the field devices in manufacturing, so far, are not IP equipped, and are not directly connected to the Internet, as the botnet army was on the 21st. Cisco and Endress+Hauser, and their partner Rockwell Automation, have been preaching IP to the device, IP to the edge, for several years.

We might want to re-think that.

But more, we should re-think the way we protect our networks. Defense in depth has been shown to be essentially ineffective.

So, too, is the individual protection of each device. It isn't a great leap to imagine that a maintenance supervisor could go to Home Depot and buy an inexpensive IP wifi camera to use to look at a bad actor valve or motor. Suddenly, there's a window for IP based malware into the plant network and systems.

Would this happen? Nobody has been successful underestimating the actions of end-users. People continue to fall for phishing expeditions, and continue to click on malware in emails. We aren't going to be able to rely on education or even discipline to keep this sort of stuff from happening.

If we are behind the eight ball, what can we do?

What is needed, I believe, is a complete rethinking of the way industrial networks are architected, to include security built in at the chip set level. Secure data hand-off, from device to device, and perhaps along each cable, could be designed and should be designed.

The real issue is that end-users want better security but aren't willing to pay for it. I suppose it will take a huge incident, much bigger than the Dyn incident, to get people to accept that security costs money.