The Scary Future of our Helpful Devices

Yosef Gamble

25 November 2016

The Internet of Things (IoT) will make life easier for all, giving the ability to do ordinary and extraordinary things, despite their physical condition. Over the last decade, we have seen a cornucopias amount of new technologies that help us turn our lights on, clean our houses, or secure and control our most prized possessions. But while each device is assumed safe and in our immediate control. Our homes and businesses will become more insecure than before.

I know for myself, I would benefit from the Internet-enabled refrigerator that orders food for me or reminds me to pick up items before I actually enter my house. But on the contrary, IoT devices increasing become a weapon used to steal my information, influence my politics, and disrupt my ability to access information.

For instance, the critical system for major news, entertainment, financial, and social media websites suddenly went offline last month. For over an hour, many people residing in the Eastern United States were suddenly cut off from large blocks of information that should've always been accessible at everyone's fingertips. Unknown to internet users at the time, their inability to watch Netflix or conduct PayPal transactions was due to a Denial of Service (DDoS) Attack. This massive onslaught of information, at the rate of 1.2 terabits per second, being spammed at a critical service called a critical Domain Name System (DNS), that helps route computers and devices to a website associated with its domain name. In perspective, 1.2 terabits per second are the equivalent of several hundred YouTube videos or an entire music collection of junk data overloading a computer at every single second. And how were they able to achieve it? By using a massive library of vulnerable cameras, baby monitors and DVRs that millions of people use to secure their businesses and families remotely. By using the openly available script called Mirai, hackers were able to send random bits of useless data in order to send servers crashing.[1][2]

DDoS attacks aren't new, but with the increase in our reliance on internet-connected devices, the chance of IoT devices becoming victim to hacking also increases. DDoS attacks have usually remained localized to a few websites or a small geographic region, such as Estonia and the country of Georgia. But Mirai has now demonstrated how the massive amount our helpful devices can now be used to widely affect the stability of an entire single or group of nations like we have never seen before.

As long as there are more devices and not enough individuals taking the steps to secure their devices through good password and software management, we may see more attacks like these that could result in a new form of censorship by individuals or state actors.

There were early guesses that suspected that the hacking collective Anonymous was trying to make a political point. So far, investigators have not been able to find the attackers. The style attack was already used earlier in order to attempt silencing cybersecurity journalist, Brian Krebs' investigation into illegal DDoS service sellers, but those involved were arrested before this latest attack. [3]

1: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

2: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/

3: https://krebsonsecurity.com/2016/10/iot-devices-as-proxies-for-cybercrime/