Crossing the Digital Divide Volume 36

"DDoS"
By Joseph Feigon
For the Observer

*In computing, a **distributed-denial-of-service** (**DDoS**) **attack** is a cyber-attack where the perpetrator(s) seeks to make a website or network service unavailable. Denial of service is typically accomplished by flooding the targeted website or resource with superfluous requests (packets of information) in an attempt to overload systems and prevent legitimate requests from being fulfilled. It is analogous to a group of people crowding the entry door or gate to a shop or business, effectively blocking legitimate customers, and disrupting normal operations. (Reference: Wikipedia)*

Last week, many of us experienced Internet slowdowns and non-responsive websites as a result of a DDoS attack primarily targeting East Coast and European server farms supporting Netflix, Etsy, Spotify, AirBNB, Paypal and Amazon. While not the biggest or most sophisticated attack in recent times, these events are increasing in occurrence and severity. Last year, DDoS attacks crippled GitHub (large repository of public software), Spamhaus, a large, European-based anti-spam/junkmail vendor, BBC (British Broadcasting Company), and Hong Kong (the entire island).

The sites being attacked are large companies, all of which have professional network and security engineers, on payroll, working every day. Hackers responsible for the most recent Dyn DDoS attack took advantage of rogue malware Mirai. This malware can be found on exposed/unpatched personal computers as well as IoT devices.

One such IoT electronic manufacturer is Chinese firm Hangzhou Xiongmai Technology. Xiongmai Technology learned that its products, specifically their DVRs and internet-connected cameras, inadvertently played a role in Friday's massive cyber attack against DynDNS. Xiongmai Technology is now recalling thousands of Internet accessible network-video-recorders and cameras. How many other Mirai infected devices will we learn about in the weeks to come?

A DDoS attack requires the attackers have a number of "compromised" end-points to successfully launch the deluge of information "packets" required to overwhelm a web-server. These end-points, most often, are home electronics (PC's, TV's, Camera's, HVAC controllers, garage door openers, etc.) that have never been, or are rarely updated.

The Internet has dramatically changed our daily lives, some say for the better, some say otherwise. How many can honestly say: "I can go without accessing the Internet for day/week/month" without serious withdrawals.

We live in an age and time of near instant access to entertainment, news, and dialog. DDoS attacks are inconvenient, and often costly. You can help, it's easier than you think. Update your PC, weekly, and learn how to update the firmware on any "smart" device you have in your home. One less endpoint will not limit a DDoS attack, but 1,000's less can. Don't help those who want to disrupt our conveniences – patch today!