Daubenspeck and Associates
180 N. Stetson Avenue • Suite 1935
Chicago, IL 60601
(312) 297 4100

www.daubenspeck.com

Cybersecurity and the Internet of Things:

Section One - The Mirai Botnet Attack

JANUARY 8, 2018
By: Ken Daubenspeck

On October 21st, 2016, a type of malware known as a botnet was able to successfully disrupt many of the internet's most recognizable brands, including Amazon, Netflix, Paypal, and Twitter.

The botnet, called "Mirai", accomplished its attack by forcing hundreds of thousands of hijacked internet-connected devices to send massive amounts of junk data at a common third-party service provider. The assault, called a "denial of service attack" (DdoS), overwhelmed the provider and successfully disrupted the services of the firms using it.

The Mirai attack, which Symantec called "just the beginning," is a stark illustration of the "Internet of Things" (IoT) as a dangerous new frontier for cybersecurity. In the coming years, businesses will increasingly rely on IoT technology to spur advances in analytics, automation, and other value-generating processes. The most conservative growth forecasts estimate that 20 billion objects will be connected to networks by 2020, yet many of these devices have been designed with terrible security.

"Catastrophic levels of vulnerability will enter the economy if significant security improvements are not made to this rapidly growing industry."

Weak security is endemic to the internet of things, an expansive term that refers to any object with functions that can be controlled or monitored through a network. It includes a range of technology, from self-driving vehicles to sensor-filled "smart concrete", and is often divided into sub-sectors such as the "industrial internet of things," which has become important to manufacturing. Catastrophic levels of vulnerability will enter the economy if significant security improvements are not made to this rapidly growing industry.

The poor state of current IoT security is demonstrated by the simplistic method of attack Mirai used. The program simply scanned the internet for vulnerable devices and tried to enter 62 common username/password combinations on each one that it found. Because many devices ship with unchangeable default logins—and because many logins that can be changed never are—Mirai was able to infect hundreds of thousands of devices this way. IoT devices function with minimal user input, and so few device owners ever realized they were compromised.

Mirai is a symptom of a larger problem—malware that targets connected devices is now an ever-present threat. Johannes Ullrich of the SANS Technology Institute has shown that it takes an average of only two minutes for an internet-connected DVR to be

found and compromised by malware armed with the DVR's default password. In other words, a vulnerable device can now be found and hacked almost instantly.

The systemic risk associated with the internet of things has become severe enough that cybersecurity firms are now advising insurers to factor cyber-attack liability into nearly all of their major commercial insurance lines. As IoT embeds itself throughout the economy, organizations will need to take proactive steps to protect themselves from the systemic vulnerabilities created by this technology. The ability of business to effectively leverage the benefits of IoT depends on successful cybersecurity, because as one technology magazine put it, "the botnet that broke the internet isn't going away".