11/9/2016
10:00 AM

The Big Lesson We Must Learn From The Dyn DDoS Attack

The vulnerabilities that make Io botnet also make them the perf clouds.

Nathaniel Gleicher, Commentary

Connect Dire

0 COMME
COMMENT NO

Lessons From the Dyn DDoS Attack

A week ago Friday, someone took down numerous popular websites in a massive distributed denial-of-service (DDoS) attack against the domain name provider Dyn. DDoS attacks are neither new nor sophisticated. The attacker sends a massive amount of traffic, causing the victim's system to slow to a crawl and eventually crash. There are more or less clever variants, but basically, it's a datapipe-size apacity to receive and process data, ctim can process, he or she will win.

It is much smarter to recruit millions rt of the DDoS attack, and pretty t computers around the internet and single victim.

Dyn DDoS attack exposes soft underbelly of the cloud

The DDoS attack against Dyn affected numerous websites, but the victims are the enterprises that rely on SaaS for critical business op

RECENT NEWS

October 21, 2016

Dyn

How can we **secure our own IoT networks** and **prevent unwilling participation** in **botnets?**


KANA
SHI

- Member of your IoT network.
- **Detects unauthorized**, **malicious** outbound **traffic** from your devices.
- Keeps the internet safe.

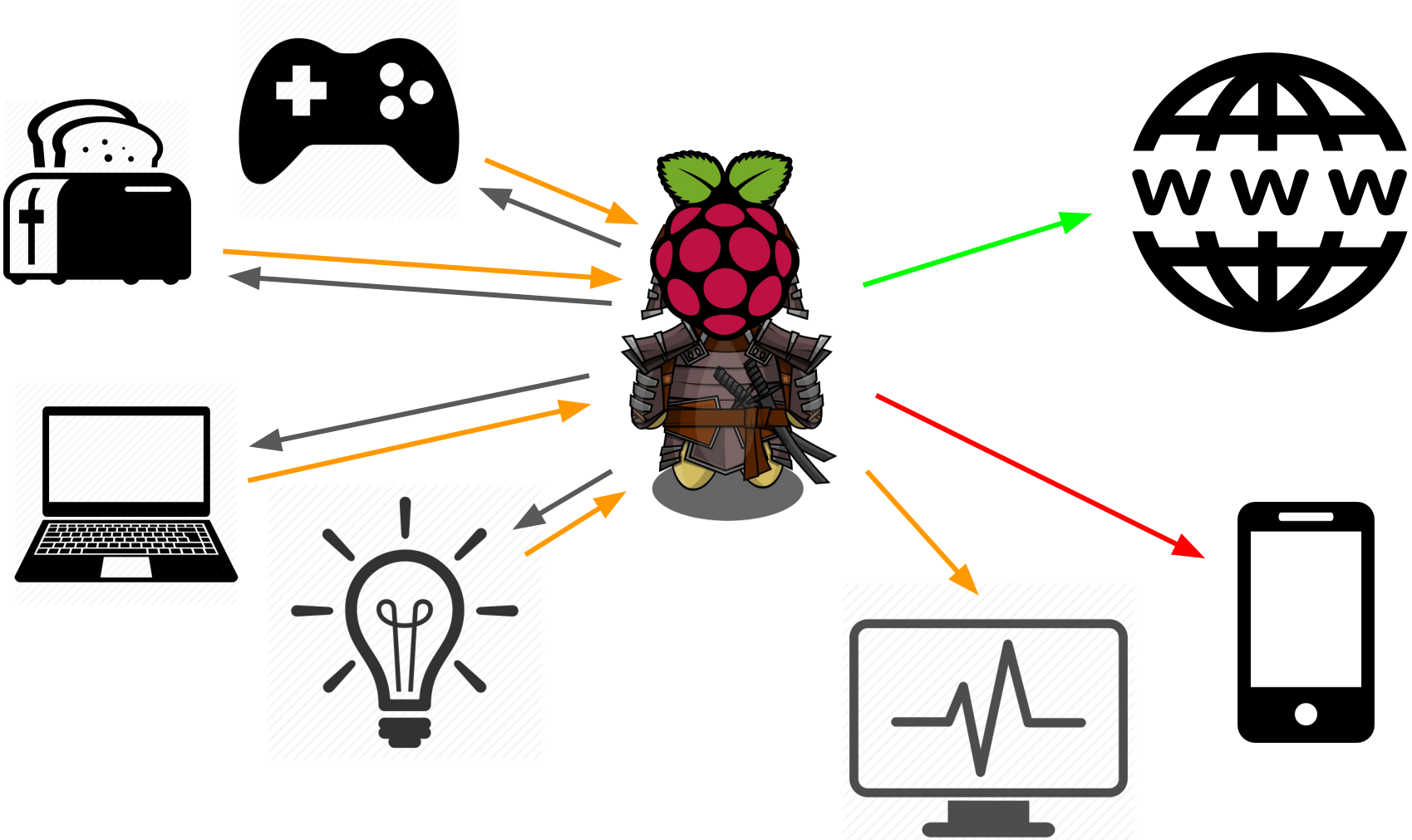
Kanashi acts as a guardian for your **outbound packets.**

FILTERING:

Malicious packet

ACTIVITY ALERTS

- **Web application**
- **SMS**


WWW