

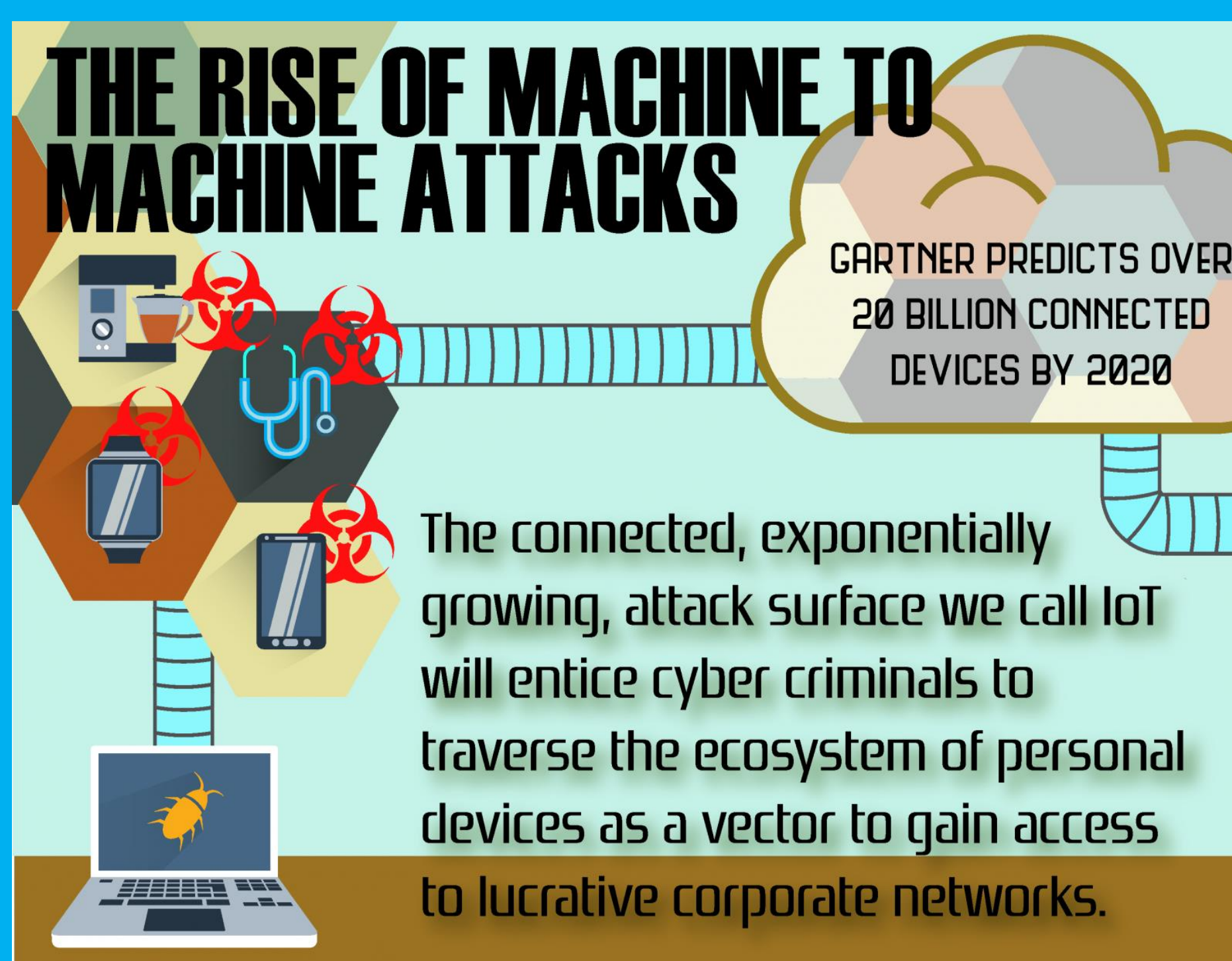
By: Andrej Suttles

Department of Computer Science, Furman University, Greenville, SC

## Introduction

My plan is to produce a group of people that is more aware of many different Computer Security issues that could directly affects them as well as provide a few tips on how to prevent these attacks.

## IoT Botnet:



- ◆ A group of hacked computers, smart appliances and Internet-connected devices that have been co-opted for illicit purposes.

## ◆ Main Categories:

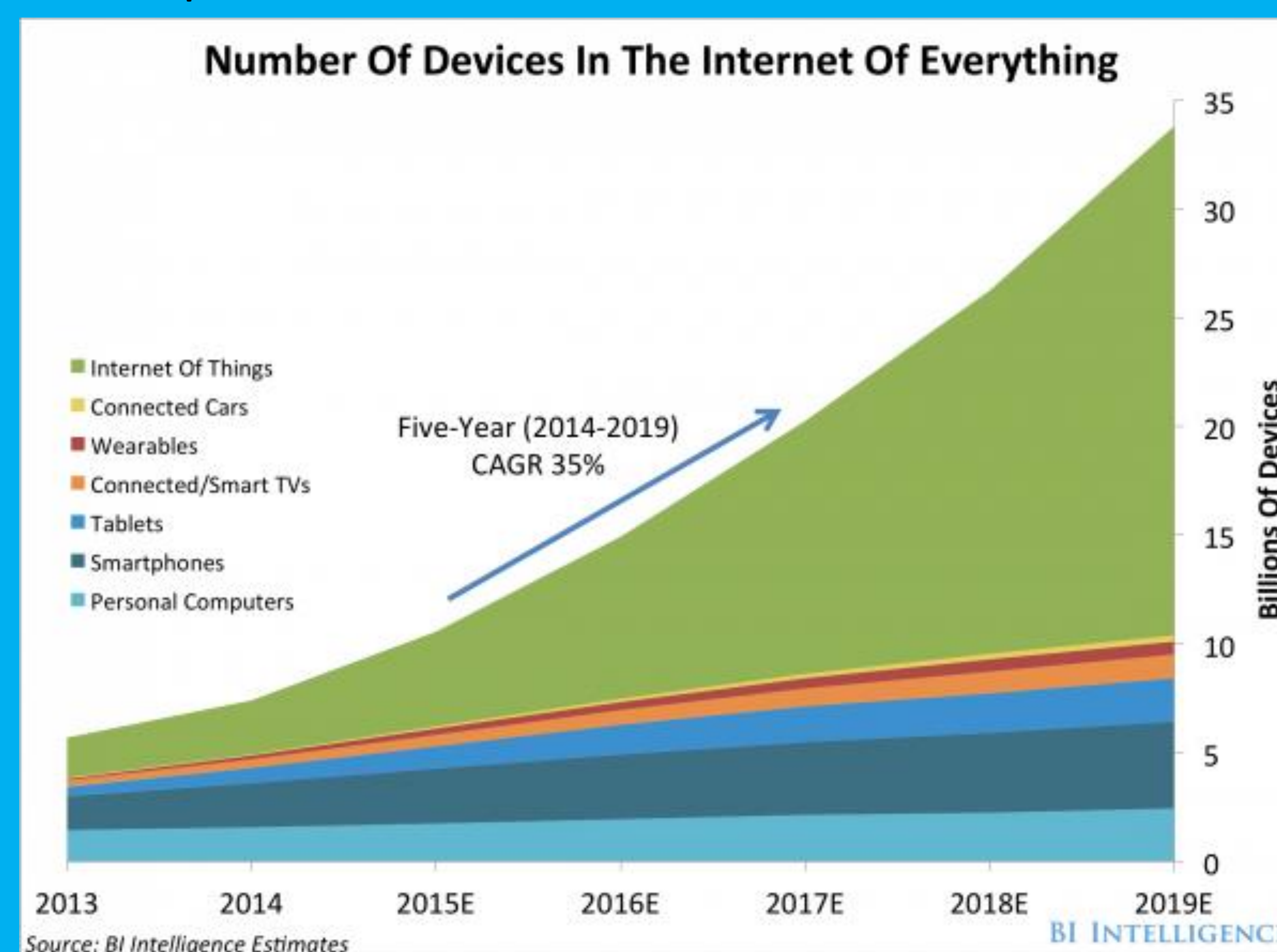
- ◆ Consumer Efficiency
  - ◆ Marriott Hotel
- ◆ Health care
  - ◆ Body equipment
- ◆ Transportation
  - ◆ San Francisco Cars/Parking

## Two-faced malware

- ◆ Specifically designed to evade detection in sandbox testing.
- ◆ Executes a benign task while in the sandbox
- ◆ Performs its malicious process once it passes the sandbox test

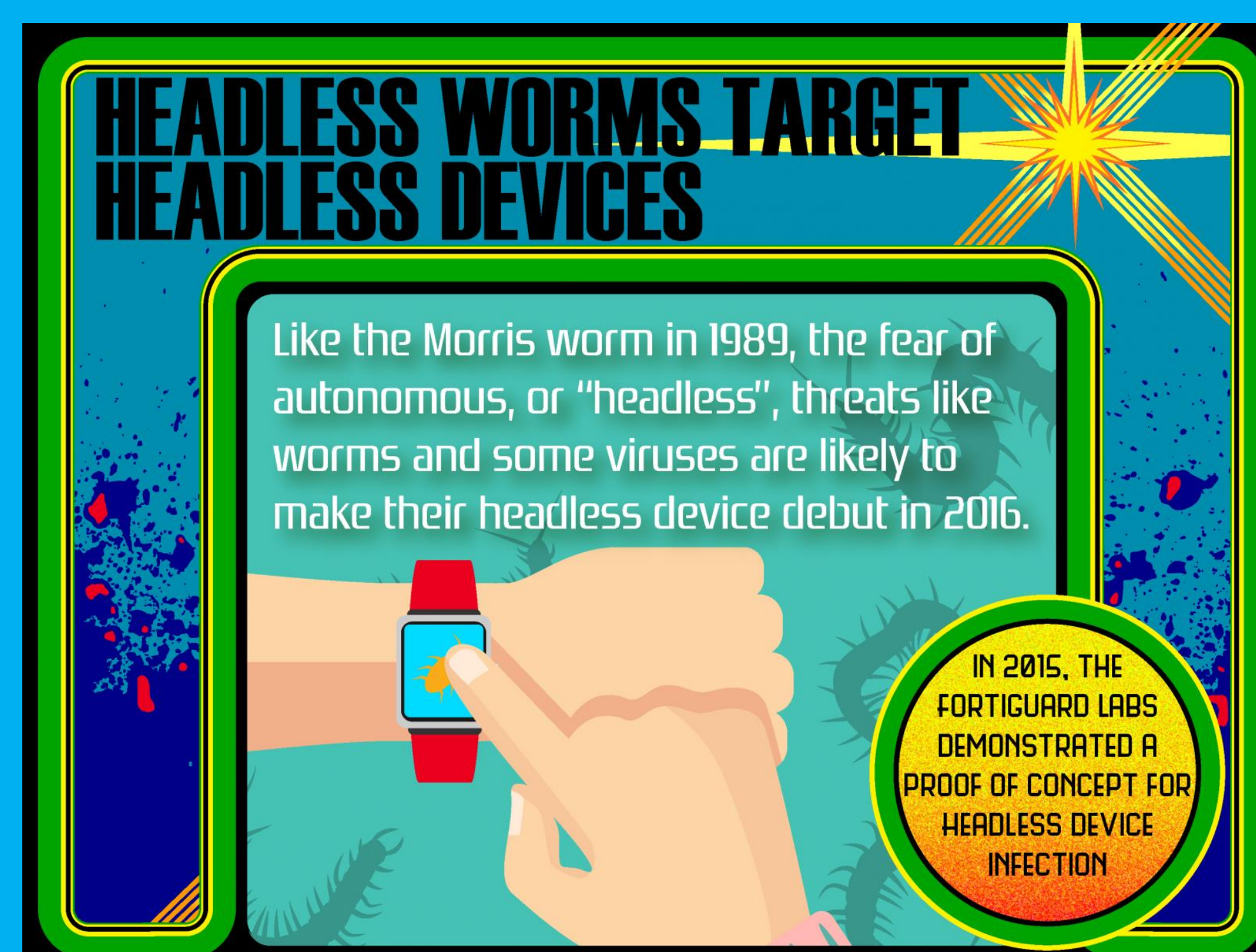
## What Is Computer Security?

(n.) In the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Computer Security is essentially the immune system of a computer.



## Headless Worms

- ◆ Malicious code used to capture and control devices
- ◆ Industrial machines, automobiles, medical equipment, cameras, household appliances, airplanes, vending machines and toys are among the countless possible hosts of embedded systems



## C.I.A

### Confidentiality

Primarily intended to ensure that no unauthorized access to information is permitted and that accidental disclosure of sensitive information is not an option

### Integrity

Integrity models keep data pure and trustworthy by protecting system data from intentional or accidental changes.

### Availability

Keep data and resources available for authorized use, especially during emergencies or disasters.



## Quick Tips:

- ◆ Backup frequently and use an off site device
- ◆ Destroy sensitive documents
- ◆ Antivirus, Email Alert System, Firewall, Software Patches, Frequent Backups
- ◆ User wireless encryption
- ◆ Implement device control, and a multi-user system
- ◆ Enforce a strict password policy: Long, no usernames, no dictionary words, passphrase, no public computers, etc