openHPI Course: Cyberthreats by Malware

Botnets

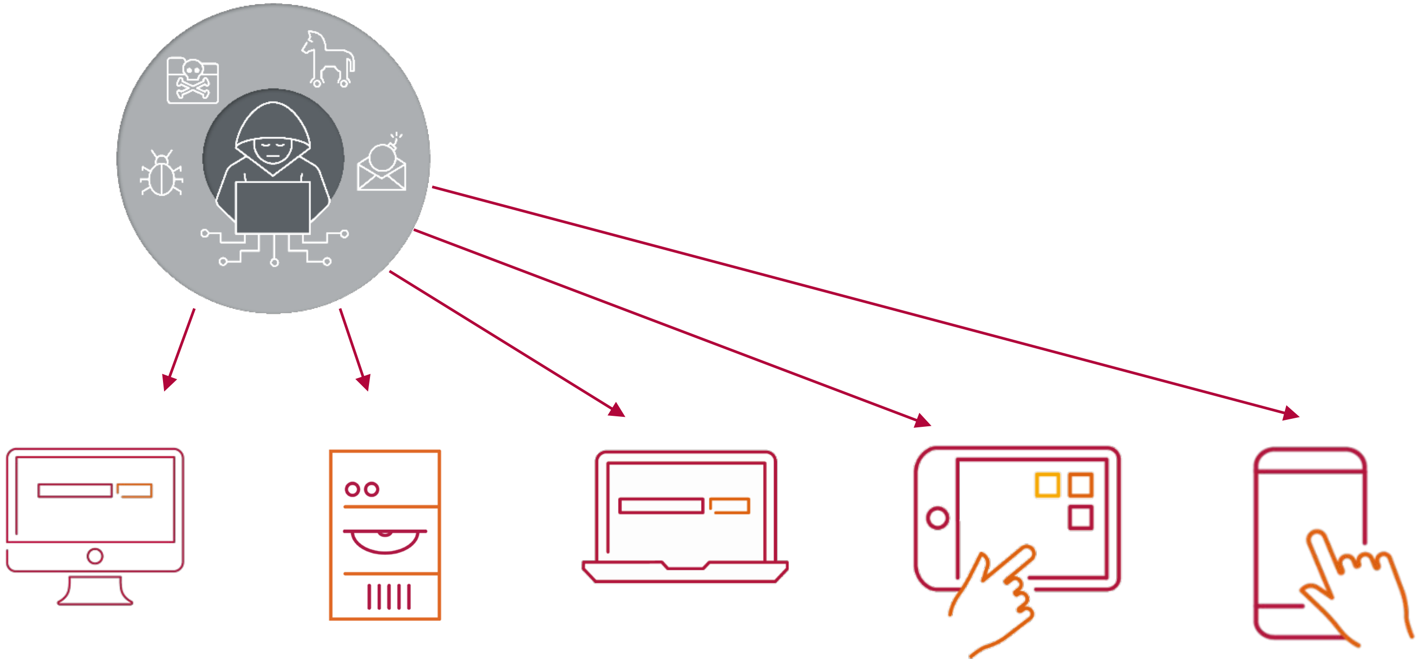
Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

Botnets – Basic Principle (1/2)

Botnet is a (huge) number of internet-connected devices whose security have been breached and are remotely controlled by attackers

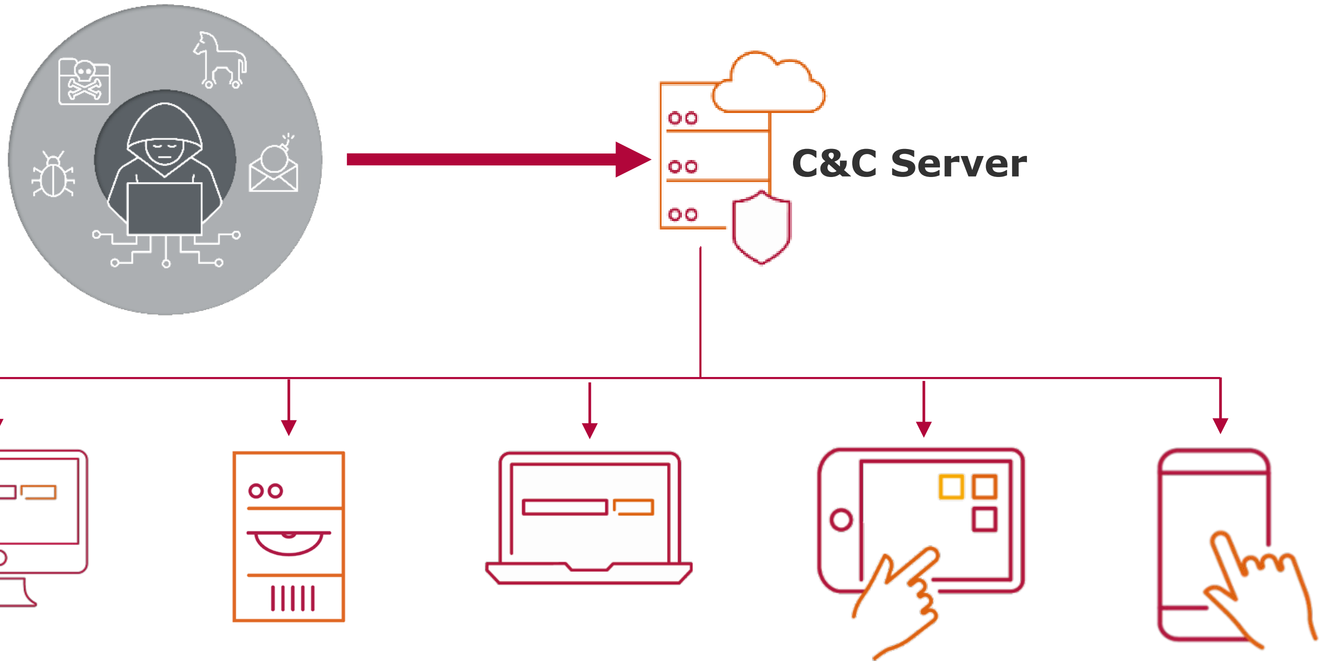
- Attackers infect different targets through malware
  - Trojans, worms, ...



Botnets – Basic Principle (2/2)

Command & Control (C&C) server controls and coordinates (millions of) bots

- Control of hijacked systems by C&C server is enabled by malware
- C&C server sends instructions and commands to the bots



Botnets – Attack Scenarios (1/2)

Examples of attack scenarios with Botnets

- **Sending spam emails**
  - allow attacker to send spam and malicious emails from victim’s system which bypass spam filters since they come from a trustful sender
- **Provision of illegal resources**
  - use the victim‘s storage system to host illegal content without direct danger to the attackers
- **Distributed denial-of-services** (**DDoS**)
  - send simultaneously a huge number of requests to a website and another online services to slow it down or make it completely unavailable

Botnets – Attack Scenarios (2/2)

Examples of attack scenarios with Botnets

- **Access online advertisements**
  - generate advertising revenue for the attacker
- **Cryptocurrency mining**
  - use victim‘s processor/graphics cards to mine cryptocurrency for the attacker, such as Bitcoin

Botnets – Some Known Examples

Zeus

- Estimated size: 3,600,000 bots
- Discovered: 2007

Conficker

- Estimated size: 9.000.000 bots
- Discovered: 2008

ZeroAccess

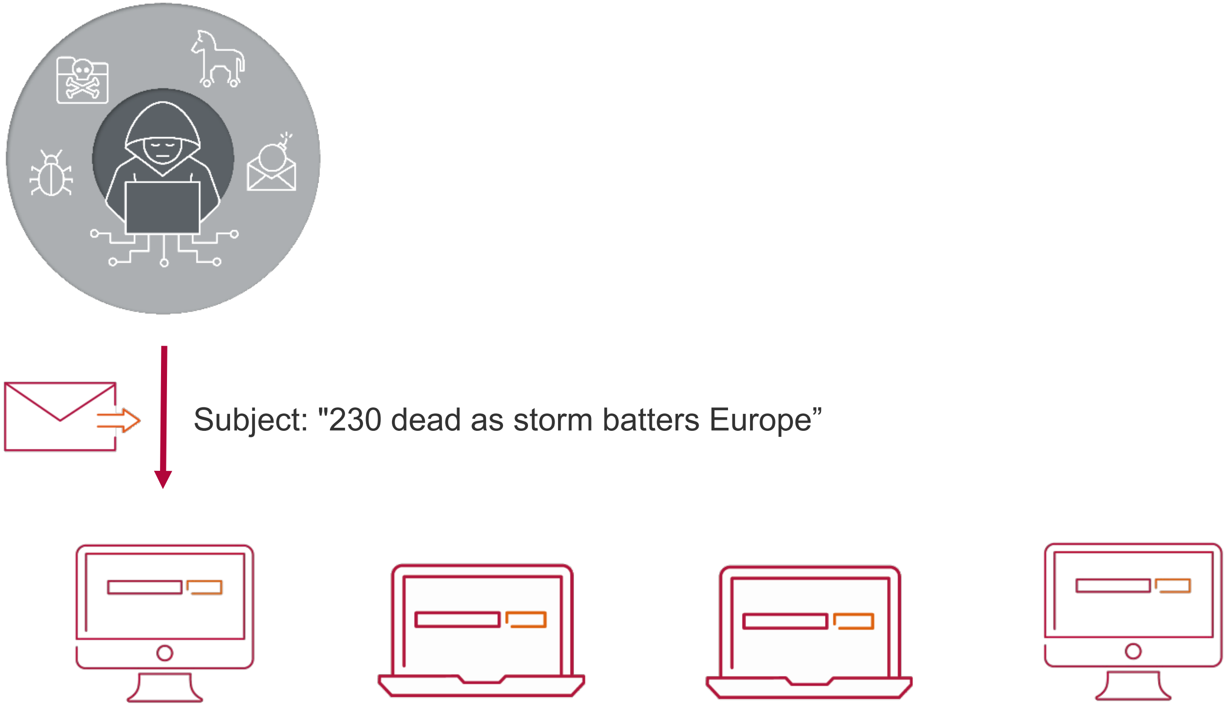
- Estimated size: 9.000.000 bots
- Discovered: 2011

Mirai

- Estimated size : 1.500.000 bots
- Discovered : 2016

Botnets – Known Examples
Storm (1/4)

- Distribution via spam emails and subsequent infection
- Estimated spread: 1-50 (!) million Windows PCs
- Undetected deactivation of anti-virus programms

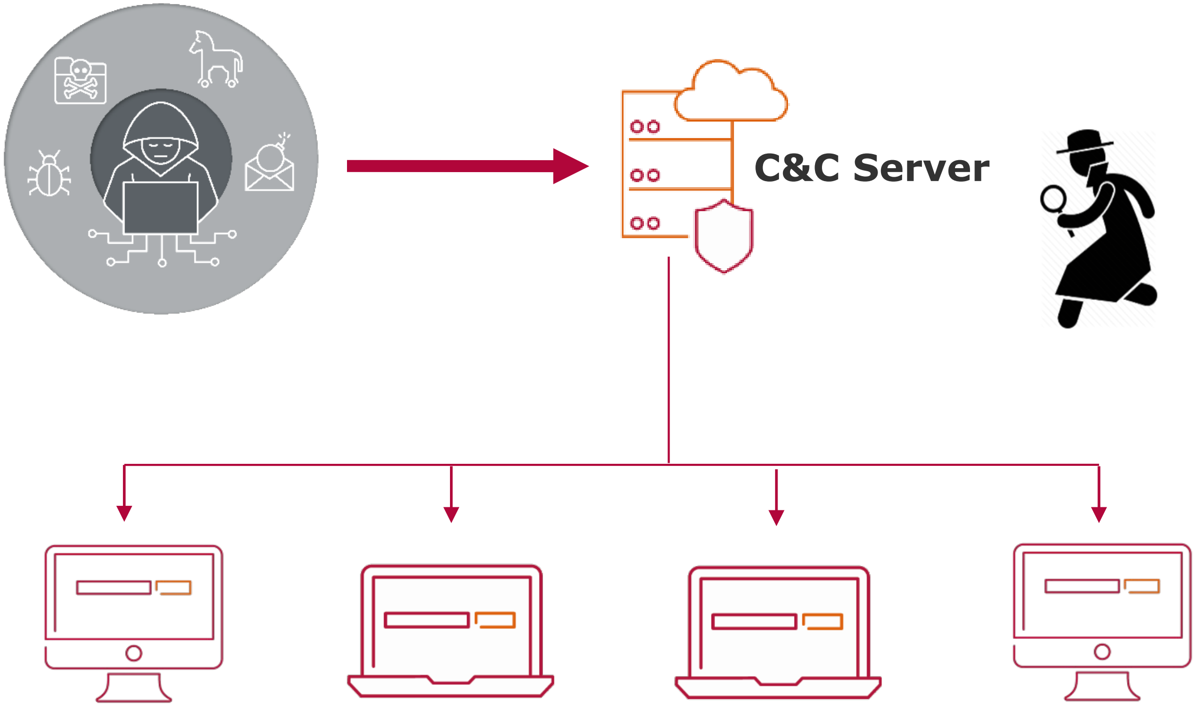


Subject: "230 dead as storm batters Europe”

Botnets – Known Examples
Storm (2/4)

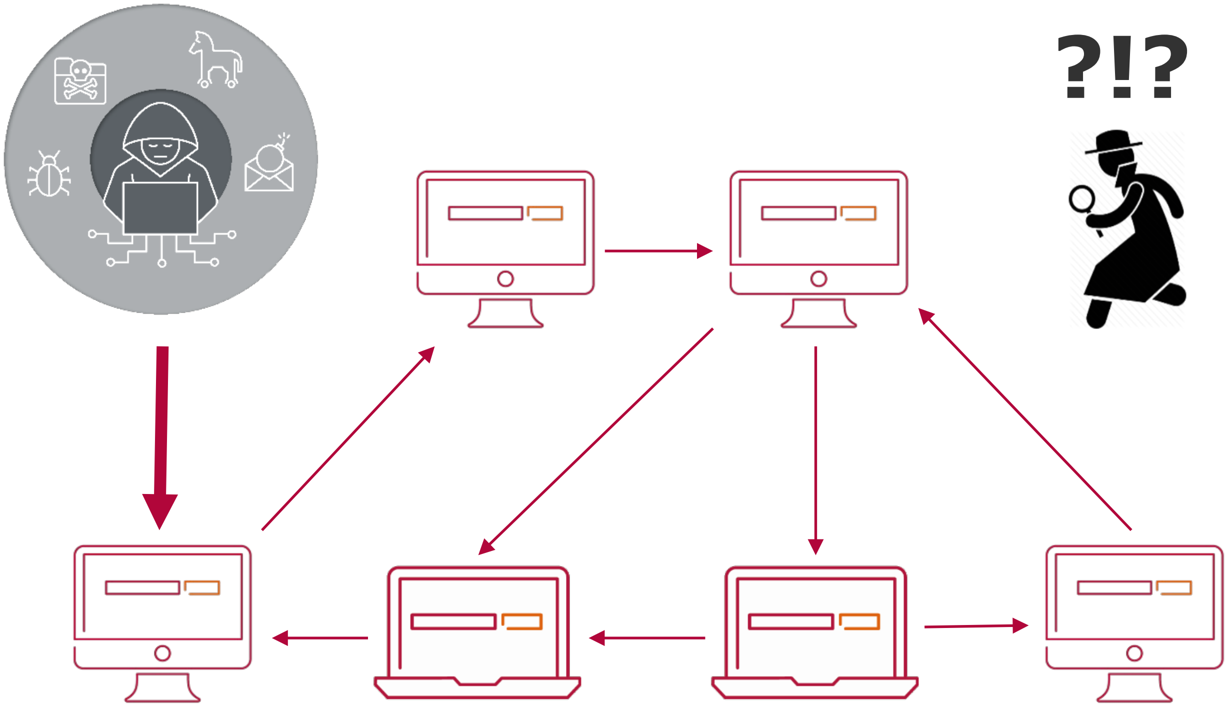
Command & control servers ...

- can be monitored and disabled by security experts, but **...**



Botnets – Known Examples
Storm (3/4)

Storm **does not** have a **central** command & control server, instead commands from the attacker are distributed using "peer-to-peer" connections



Botnets – Known Examples
Storm (4/4)

- 2007, the operators of the "Storm" botnet began to split up the organization, possibly to offer parts of the botnet for sale
- Communication with the botnet is encrypted
- Architecture became very complex with many different components:
  (1) Backdoor or downloader malware

  (2) SMTP relay server to send emails

  (3) Attack software to steal email addresses

  (4) Attack software for spreading the malware via emails

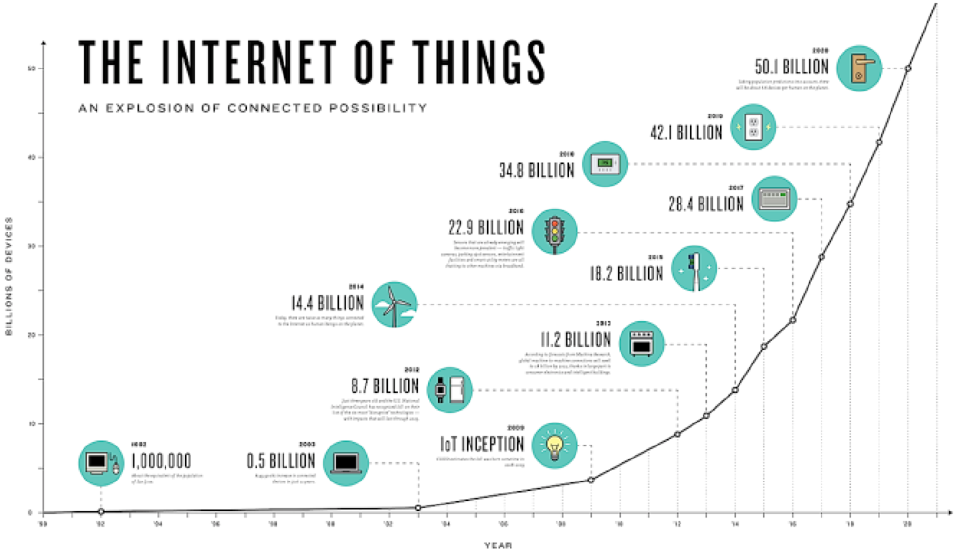
  (5) DDoS attack software for distributed attacks

  (6) Updated malware installers

Botnets – Known Examples
Mirai (1/2)

Smart devices like cameras, home routers, IoT devices, etc. can be abused as bots in a botnet

- In many areas IoT devices are used
- Often configured with poor security settings
  - □ standard passwords
  - □ open to the Internet
  - □ not updated with the latest security updates

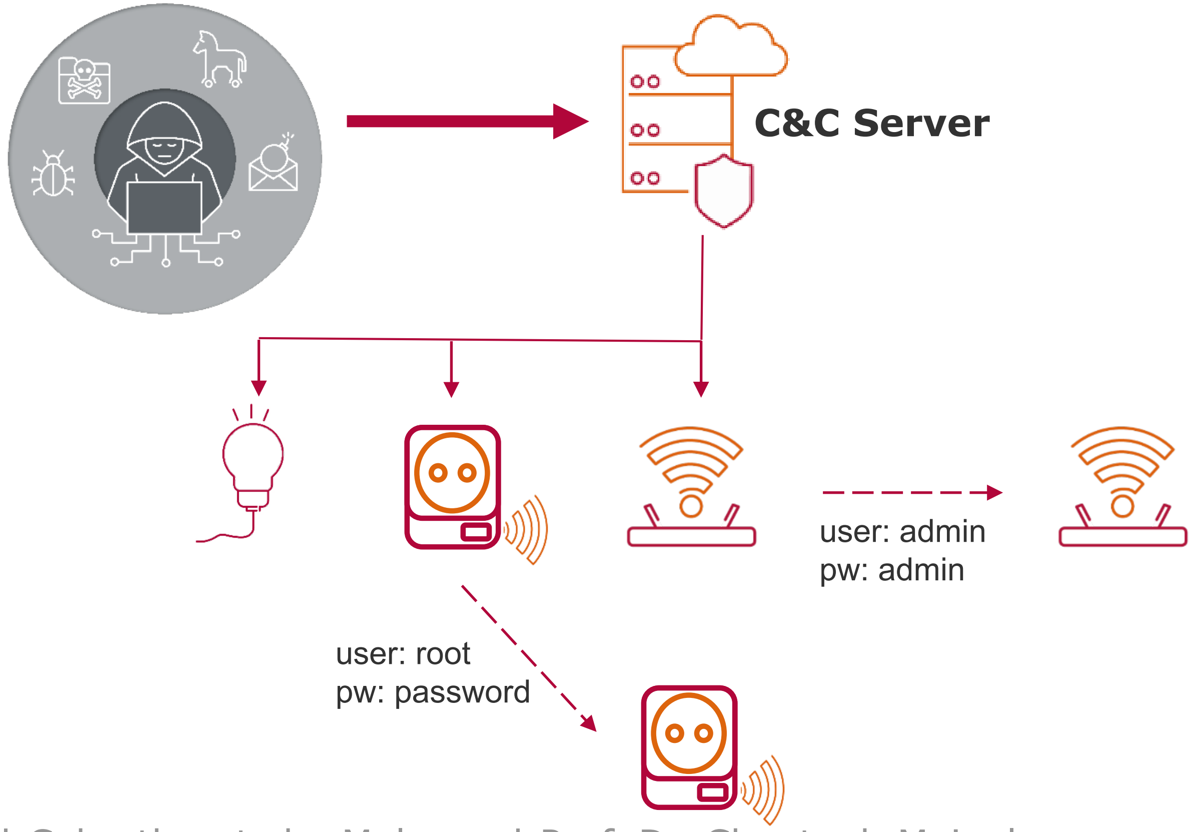


Source: Kaspersky Labs. The Future of Embedded and IoT Security, 2017

Botnets – Known Examples
Mirai (2/2)

Bots are used to find other vulnerable IoT devices

- Using standard user names/passwords to gain access to the devices


C&C Server
user: admin
pw: admin
user: root
pw: password