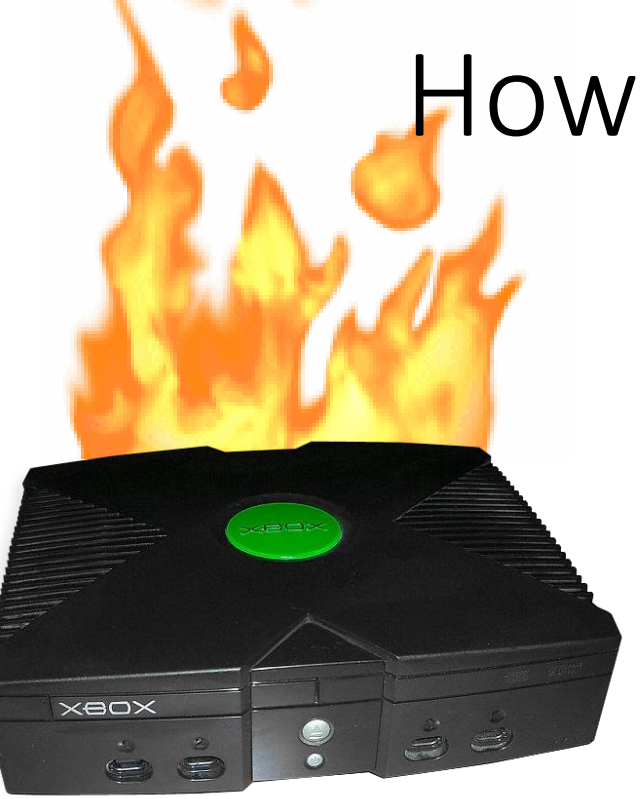
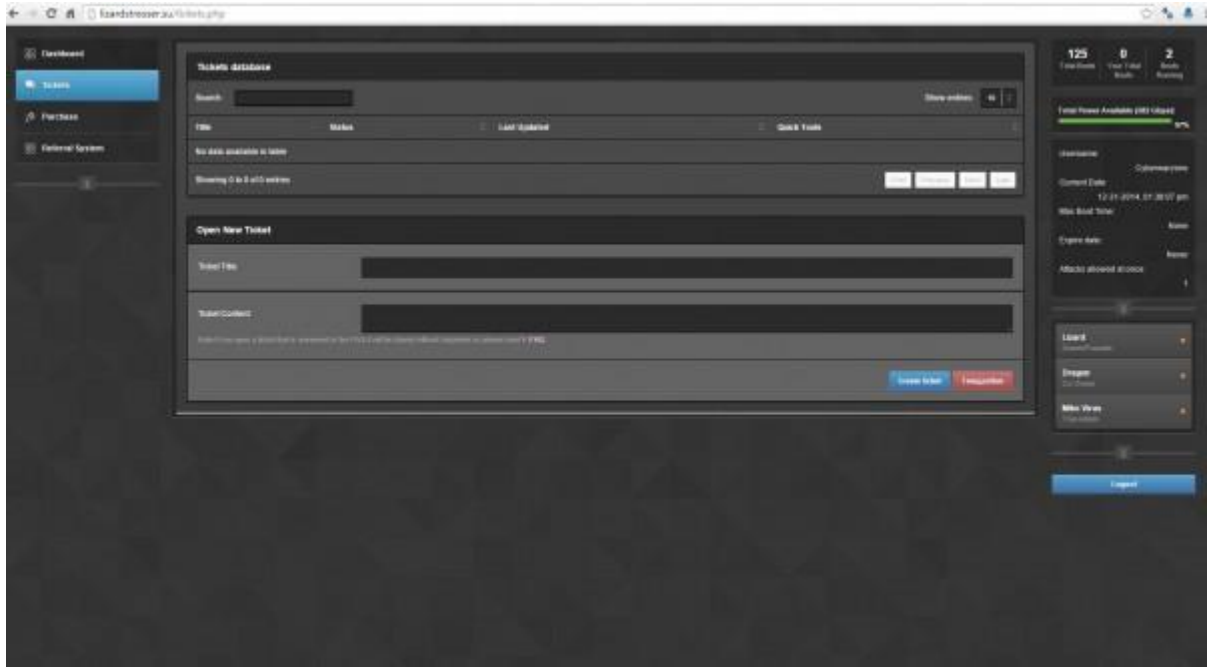
How Kim Dotcom saved Christmas

Wil Koch, Mike Marcin, Sophia Yakoubov



Lizard Squad (in the role of the grinch)

- Took down Xbox and PSN
- To advertise “stresser” service
  - allows customers to knock out web service of their choice



DDoS Background

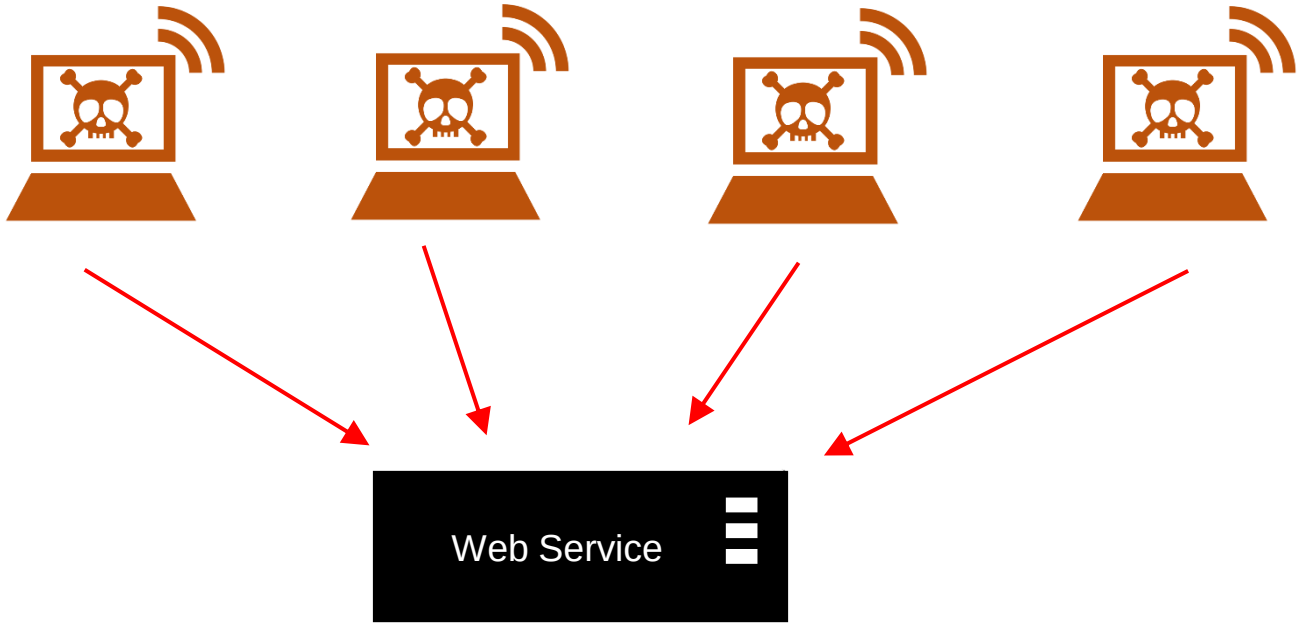
Q: How can Lizard Squad take any web service offline?

A: DDoS (Distributed Denial of Service) attack

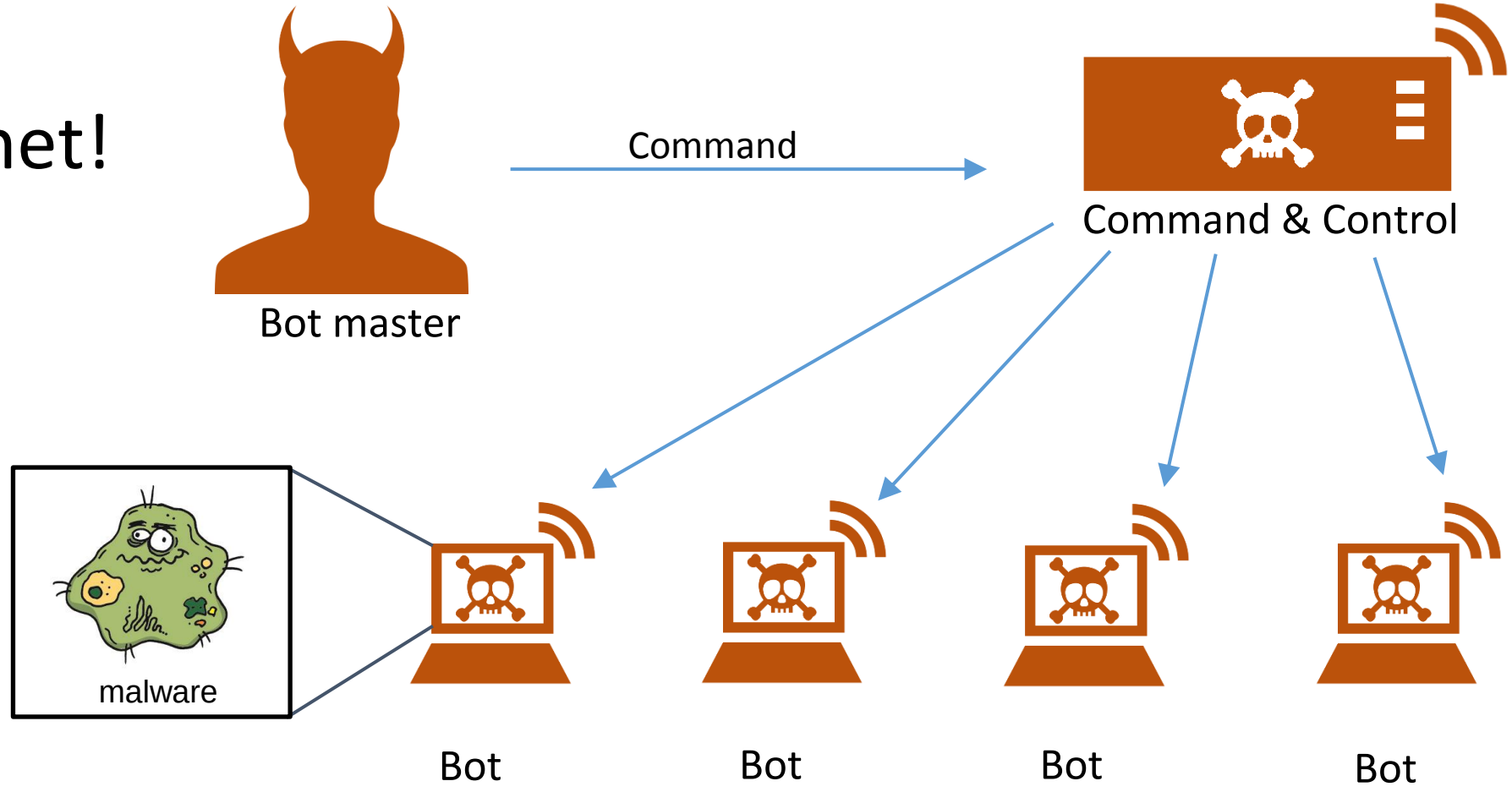
- Attacker controls multiple hosts
- Uses them to create traffic for the web service (identified by IP or hostname), overwhelming it
- Hard to defend against:
  - Cannot block by IP – too many sources!
  - Cannot distinguish malicious traffic from honest users

DDoS Background - Types of DDoS Attack

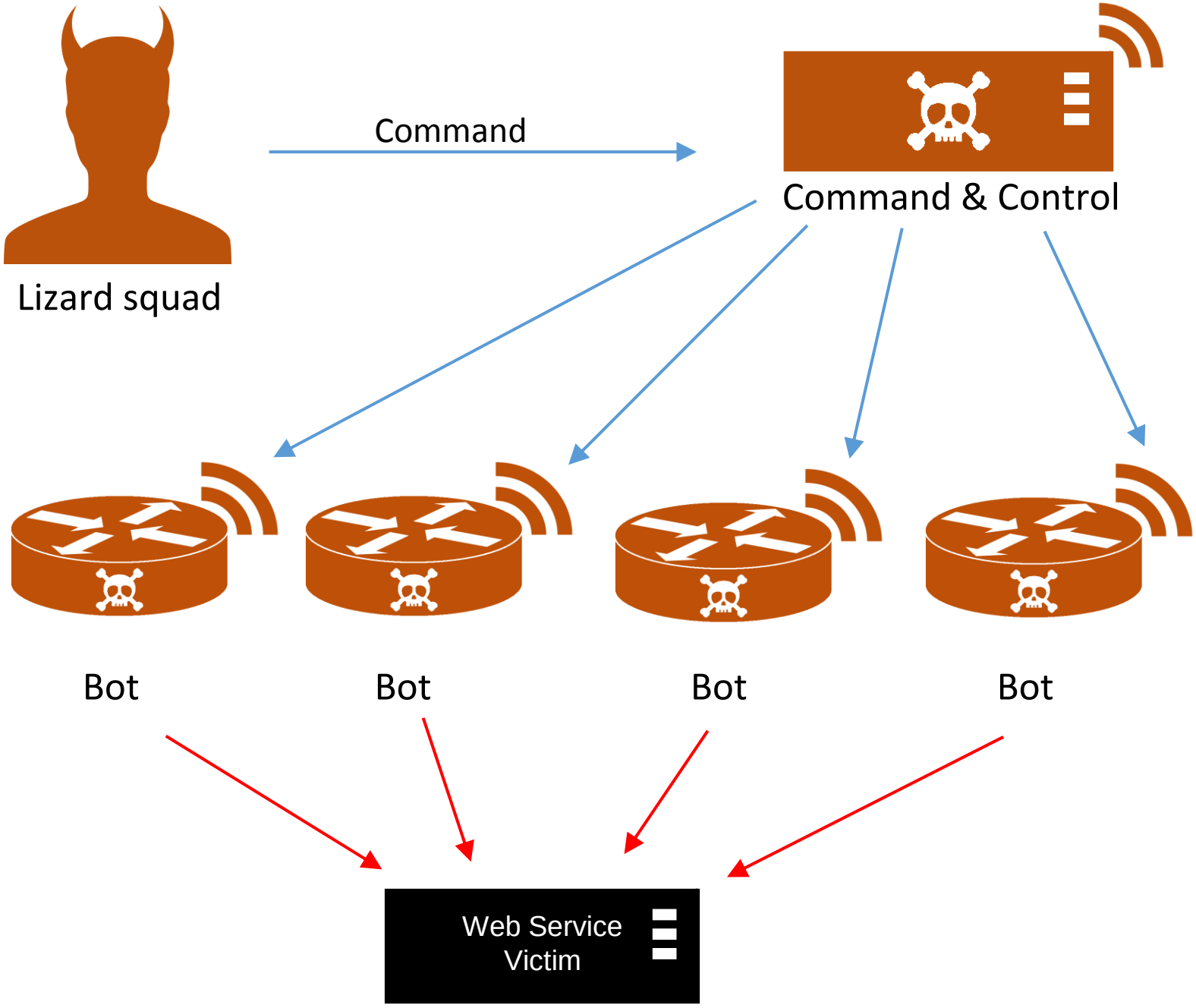
- **Computational:** uses up...
  - memory
  - disk space
  - processor time
- **Volume:** uses up bandwidth
- **Specifics of LizardStresser:**
  - Various DDoS techniques (UDP, TCP, JUNK, HOLD)
  - Uses Botnet for DDoS



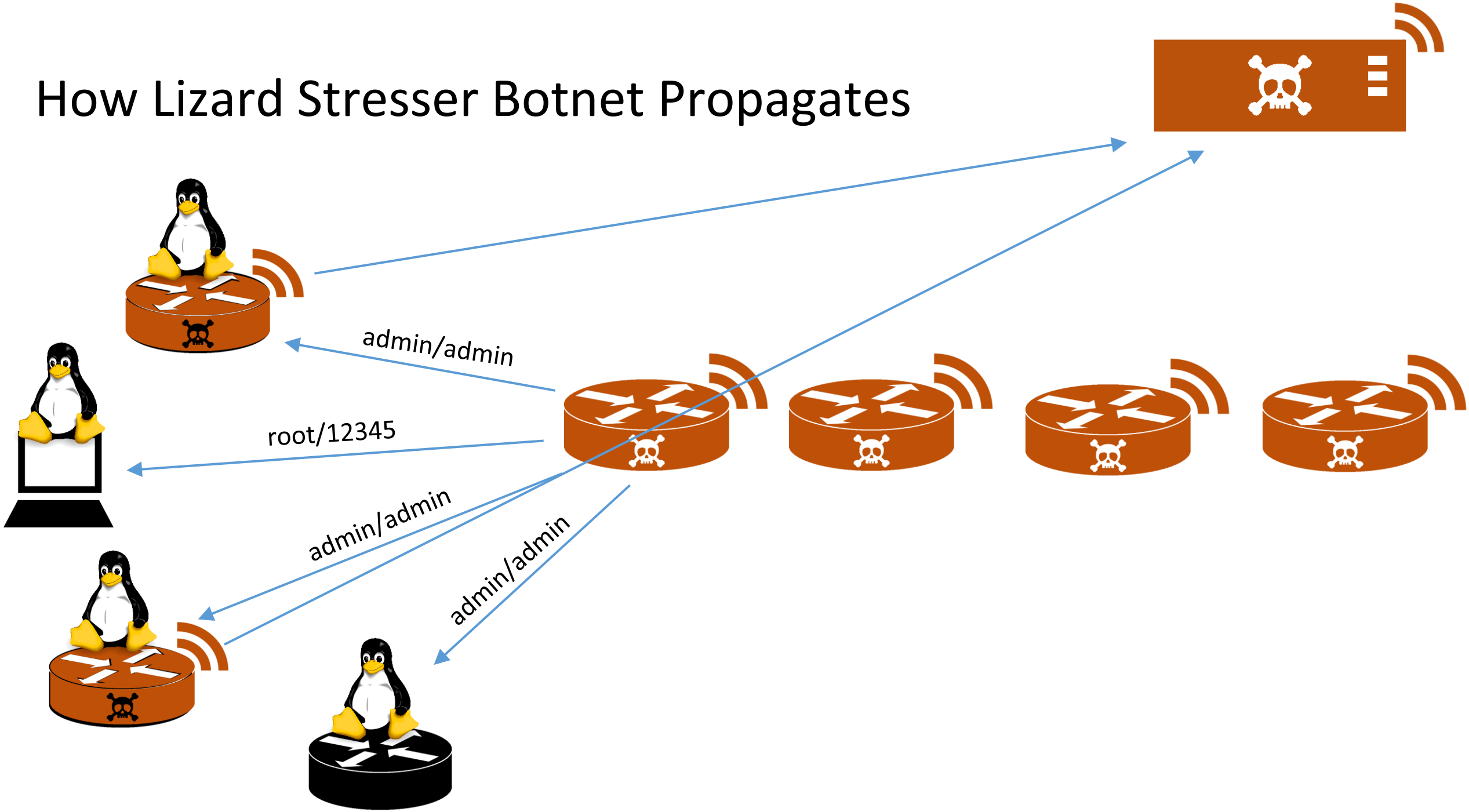
DDoS… By a botnet!



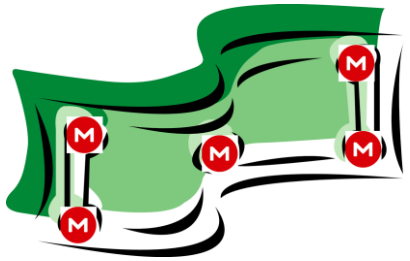
Lizard Stresser Botnet

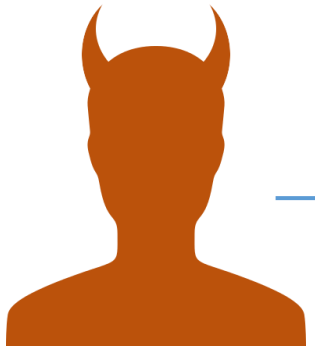


How Lizard Stresser Botnet Propagates

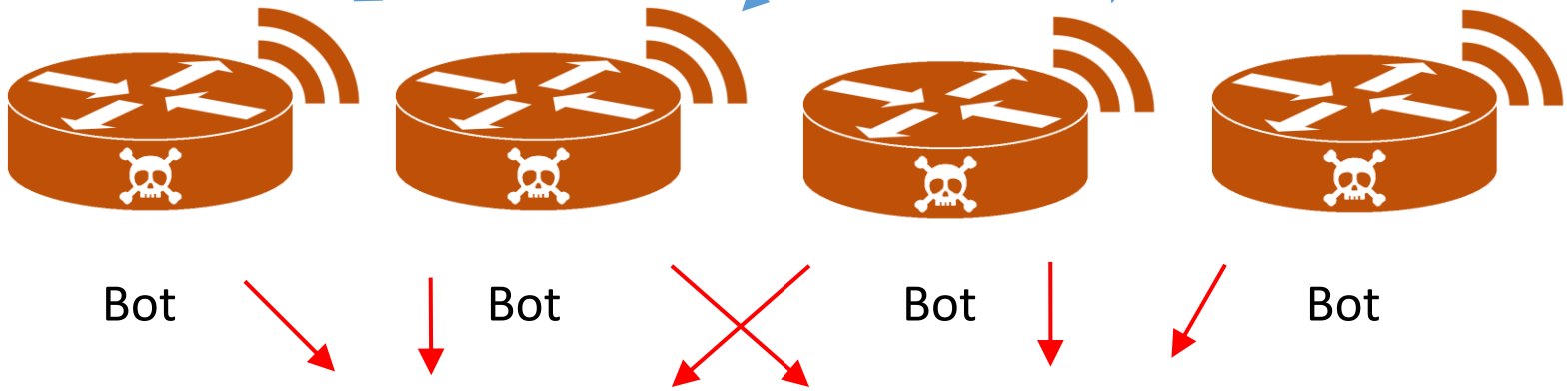


DDoS attack on Christmas





Command



Vincent Omari, 22

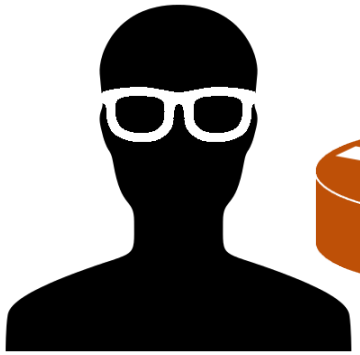
Julius Kivimaki, 1

rd Squad

Command

217.71.50.x

Command & Control



Bot

Bot

Bot

Bot

"*Ensuring* Authority for Courts to Shut Down Botnets"

Changes to 18 U.S.C . § 1345 to include Computer Fraud and Abuse Act (18 U.S.C. § 1030) allow for injunctive relief when criminal actions affect 100 or more computers.

Current laws:	Proposed law:
•Banking fraud •Wire fraud •Communication interception	•Denying access to or operation of the computers •Installing unwanted software •Using computers without authorization •Obtaining information without authorization

Create liability protection and allow for reimbursement of costs for companies.

Lessons Learned

- Avoid single point(s) of failure
  - centralized C&C
- Don’t hardcode values into bots
- Crime doesn’t pay!

- Avoid weak passwords
- Change defaults!
- Invest in DDoS mitigation (if you can afford it!)

References

- Wikipedia on Denial of Service
- Cowards Attack Sony Playstation Microsoft Xbox Networks
- Lizard Stresser Runs On Hacked Home Routers
- Who's in the Lizard Squad
- Teen Arrested in UK for Xbox Playstation Attacks
- Lizard Squad Releases Lizardstresser Ddos Service
- How Kim Dotcom (Almost) Saved Christmas From the Lizard Squad by Forbes
- What is Lizard Squad by Pcpro
- Lizard Squad's DDoS Service Hacked, Buyers Details Revealed by nakedsecurity
- Lizard Stresser Runs on Hacked Home Routers by Brian Krebs
- Lizard Stresser botnet source code via Chippy1337 and the packet prophet
- Translation of Linux backdoor discovered by Dr. Web

References continued

- Hackers That Took Down PSN and Xbox Live Now Selling Their DDoS Attack by gizmodo
- Xbox, Sony Hackers Hit by Hack Attack by BBC
- Net Closes Around Lizard Squad as DDos Site is Hacked, infosecurity
- Securing Cyberspace, whitehouse.gov
- White House Cybersecurity Bill: Botnets and "Creative Lawyering", justsecurity.org
- 18 U.S. Code § 1345 - Injunctions against fraud, law.cornell.edu
- Deputy Attorney General James M. Cole Addresses the Georgetown Cybersecurity Law Institute
- Updated Administration Proposal: Law Enforcement Provisions