ISP and NSP Security Workshop

APRICOT 2013

Day 1

Core Security

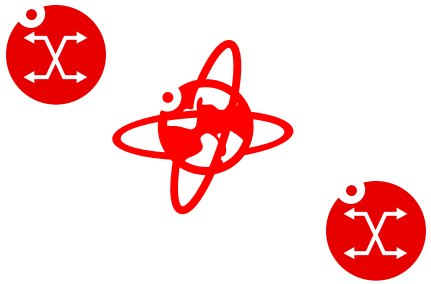
Expectations

- This tutorial is about the fundamentals
  - Today's best practice
  - Base layer for new solutions and technique to be built upon
- Everything cannot be covered today – or even this week
  - There is a lot of material
- We cannot go in-depth on *everything*
- **Ask questions!**

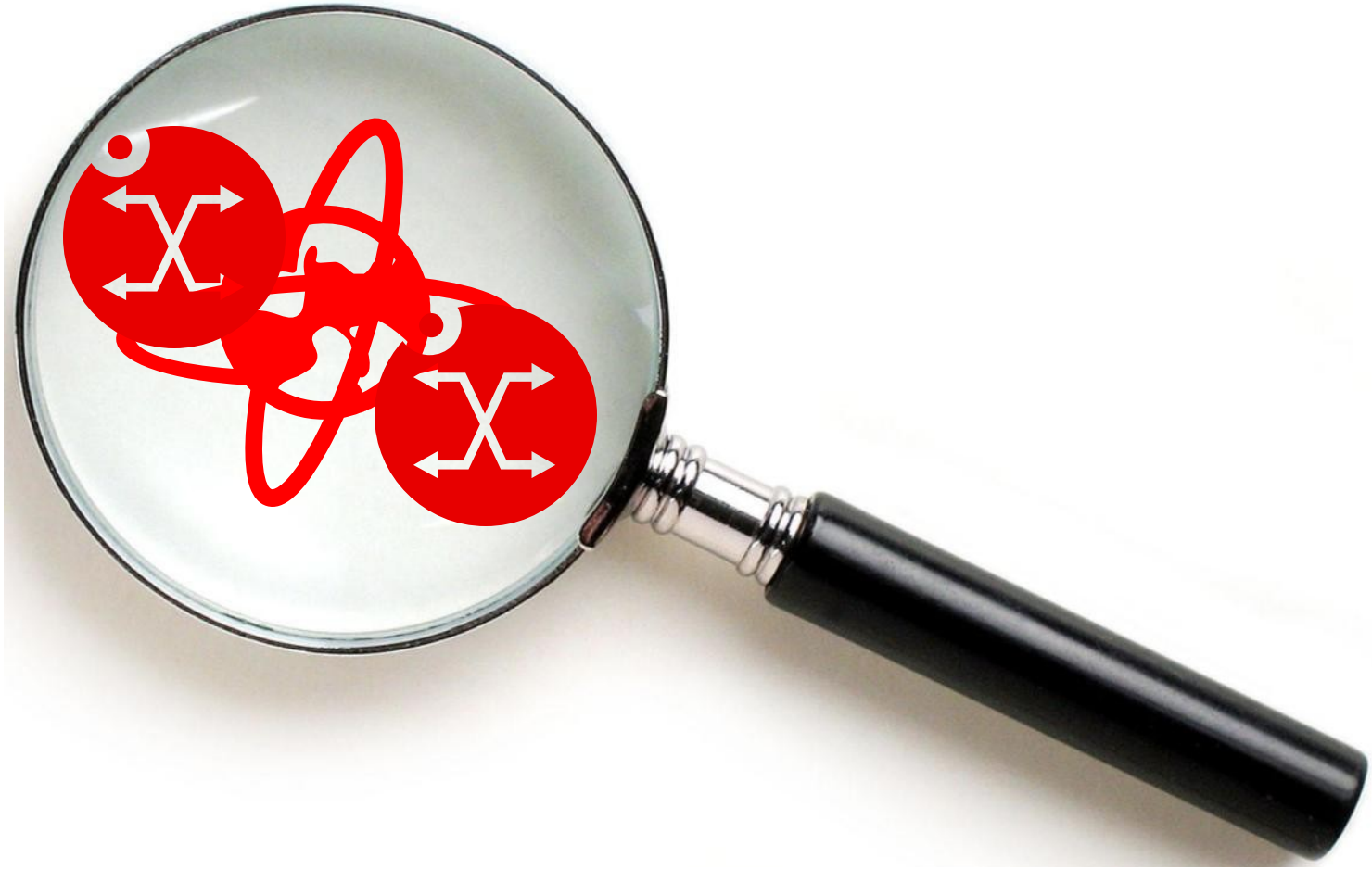
Agenda

1. Introduction
2. Awareness and understanding the threat
3. How did it all begin?
4. What is core security?
5. Denial of Service
6. Worms
7. Security response
8. Reaction and post-mortem

Awareness



Awareness



Awareness

- Being aware of what is going on around us is critical to our daily life
- The same is true for our networks!
- Understanding our network, threats and attack vectors, and life on the Internet is critical to protecting ourselves
- Think: *what should I be aware of,* ***right now?***

How did it all begin?

- Security events have been ongoing since the first networks were developed
  - Inadvertent
  - Malicious
  - Morris Worm, November 1988
- As Internet connectedness increased, as did the number of attacks and incidents
  - Amusement
  - To take someone offline
- As more commerce relies on the Internet, attacks became big business
  - "DDoS for hire"

February 2000

CNN.com

MAIN PAGE
WORLD
U.S.
LOCAL
POLITICS
WEATHER
BUSINESS
SPORTS
TECHNOLOGY
computing
personal technology
SPACE
HEALTH
ENTERTAINMENT
BOOKS
TRAVEL
FOOD
ARTS & STYLE
NATURE
IN-DEPTH
ANALYSIS
myCNN

Headline News brief
news quiz
daily almanac

MULTIMEDIA:
video
video archive
audio
multimedia showcase
more services

sci-tech > computing > story page

From...

'Immense' network assault takes down Yahoo

CNN.com technology > computing

MAINPAGE
WORLD
U.S.
WEATHER
BUSINESS
SPORTS
TECHNOLOGY
computing
personal technology
SPACE
HEALTH
ENTERTAINMENT
POLITICS
LAW
CAREER
TRAVEL
FOOD
ARTS & STYLE
BOOKS
NATURE
IN-DEPTH
ANALYSIS
LOCAL

EDITIONS:
CNN.com Europe
change default edition

MULTIMEDIA:
video
video archive

Editions | myCNN | Video | Audio | Headline News Brief | Feedback

Cyber-attacks batter Web heavyweights

Strikes on eBay, Amazon, CNN.com follow Monday Yahoo! attack

hacking

February 9, 2000
Web posted at: 9:56 a.m. EST (1456 GMT)

In this story:

FBI expected to investigate strikes

Tactic 'difficult to address'

RELATED STORIES, SITES

ATLANTA (CNN) -- A series of cyber-attacks Tuesday left some of the Web's most high-profile sites staggering under the weight of tens of thousands of bogus messages.

The targets included retail giant Amazon.com, electronic auction house eBay, discount retailer Buy.com and CNN Interactive.

VIDEO
Interview with CNN Technology Correspondent Ann Kellan about how the attacks hardly affect home computers.

CNN.com NewsNet
CNN Sites
Search
CNN.com
Find

TECHNOLOGY
TOP STORIES

Consumer group: Online privacy protections fall short

Guide to a wired Super Bowl

Debate opens on making e-commerce law consistent

(MORE)

CNN.com
TOP STORIES

More than 11,000 killed in India quake

Mideast negotiators want to continue talks after Israeli elections

(MORE)

CNNmoney BUSINESS

Playing for Iraq's jackpot

Waiting for www.cnn.com...

YAHOO!

CNN.com

amazon.com

eBay

PCH
Packet Clearing House

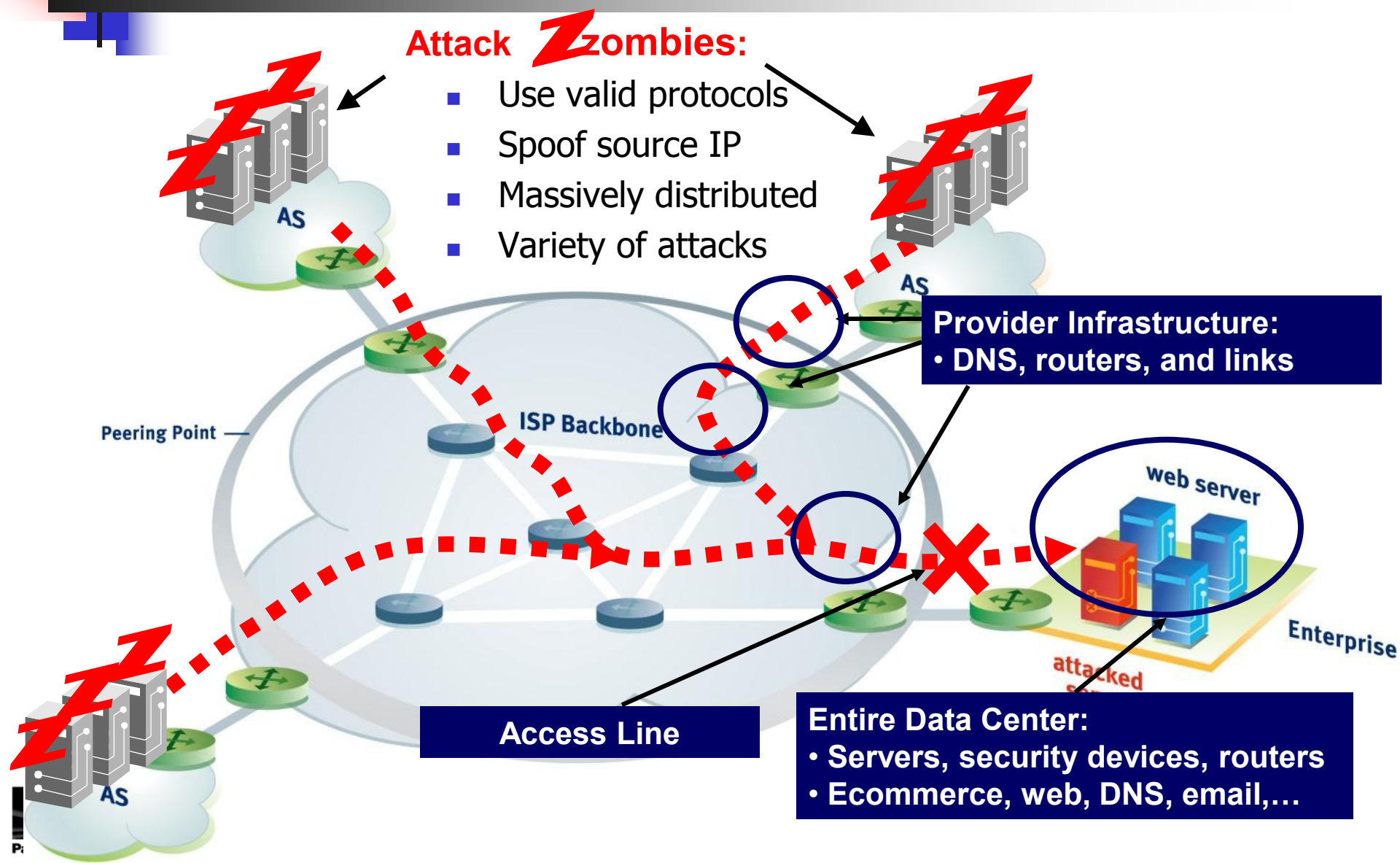
What Is Core Security?

- Often thought of as "SP Security"
  - What is an SP today?
- Internal networks are no longer truly internal
  - Tunneling
  - VPN
  - Worms, worms, worms
- The infrastructure is critical; if we can't protect it, nothing else matters
  - Edge security initiatives abound: NAC, 802.1X, personal firewalls, etc.

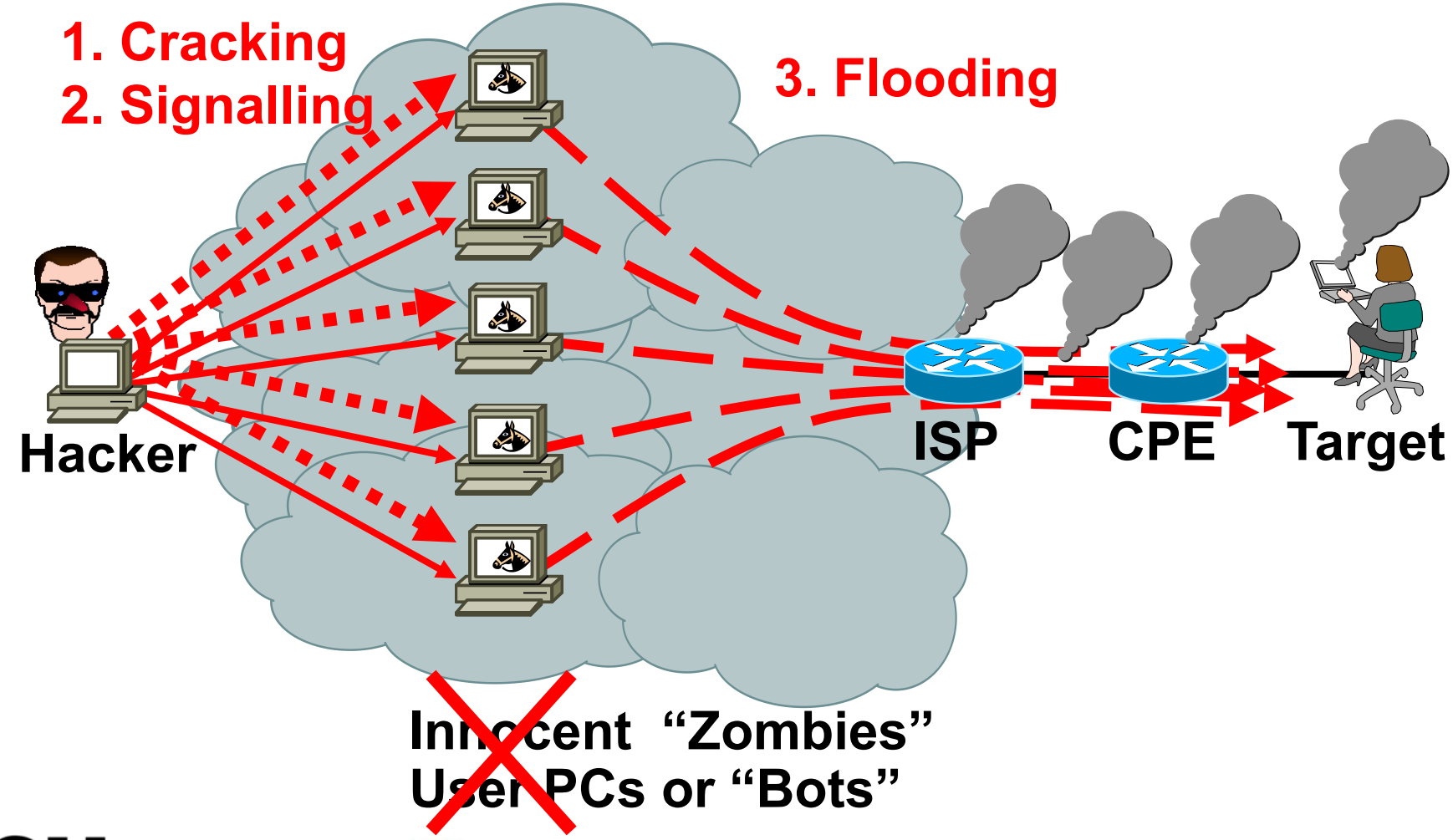
Denial of Service Attacks

- We understand intrusions (patch, patch, patch ;-))
- What about DoS? Do "the right things" and still suffer
- The vast majority of modern DoS attacks are distributed
  - DDos IS DoS
- DoS is often driven by financial motivation
  - DoS for hire :-(
  - Economically-driven miscreant community
- DoS cannot be ignored; your business depends on effective handling of attacks

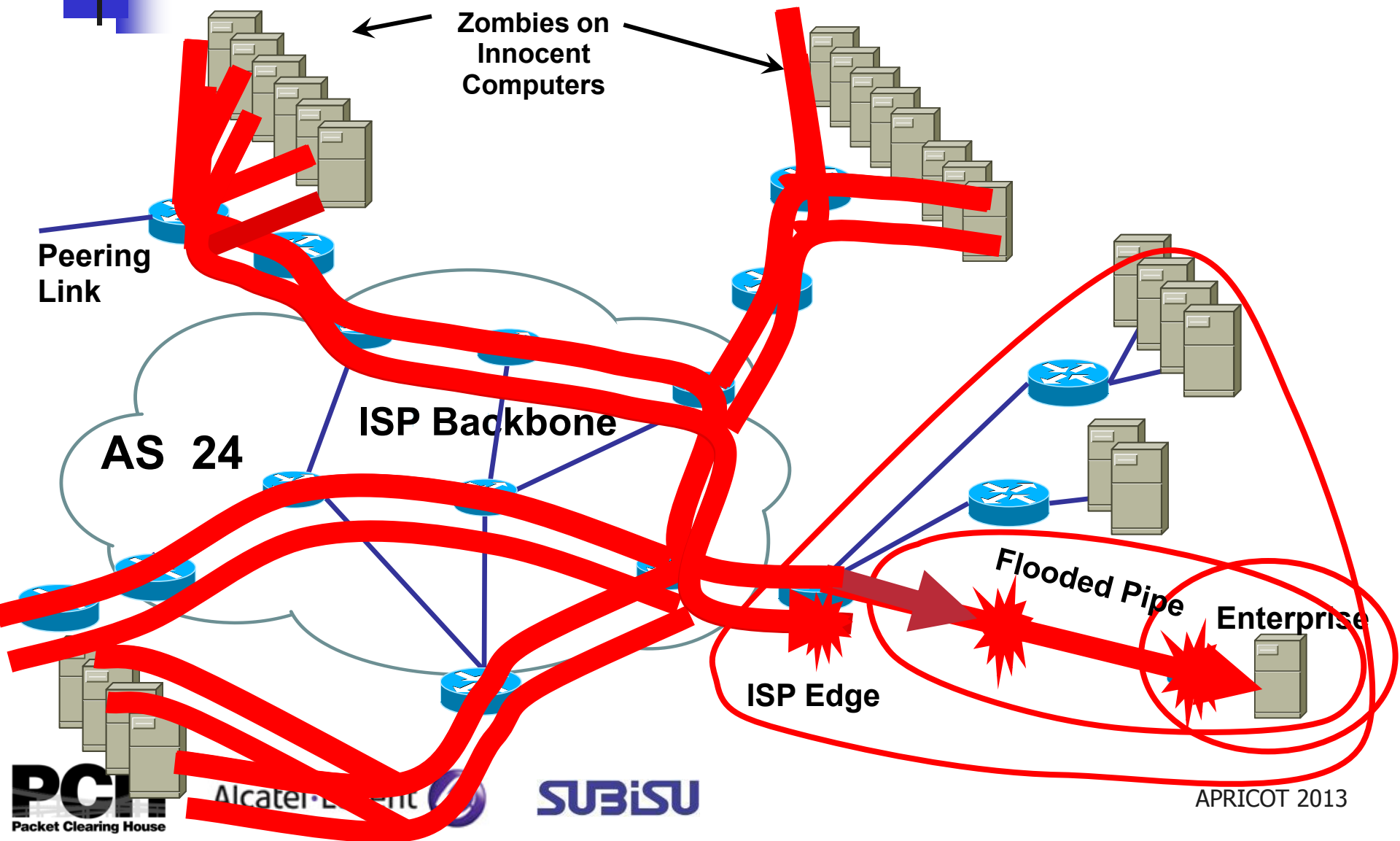
DDoS Vulnerabilities, Threats and Targets



DoS: The Procedure



An SP View: Denial of Service



Infrastructure Attacks

- Infrastructure attacks are increasing in both volume and sophistication
  - Marked increase in presentations about routers, routing and router vulnerabilities at conferences like Blackhat, Defcon and Hivercon
  - Router attack tools and training are being published
  - Compromising secure environments through network access
- Why mount high-traffic DDOS attacks when you can take out your target's gateway routers?
- Hijacked routers are valuable in the spam world, which has a profit driver
- Router compromise (0wn3d) due to weak password

From Bad to Worms

- Worms have emerged as the new security reality
- Old worms never die!
  - Millions of UPnP and Slammer packets still captured daily
- Most worms are intended to compromise hosts
- Worm propagation is dependant on network availability
- Worms and DoS are closely related
  - Secondary worm effects can lead to denial of service
  - Worms enable DoS by compromising hosts → BOTnets
- Perimeters are crumbling under the worm onslaught (VPN/mobile workers, partners, etc.)

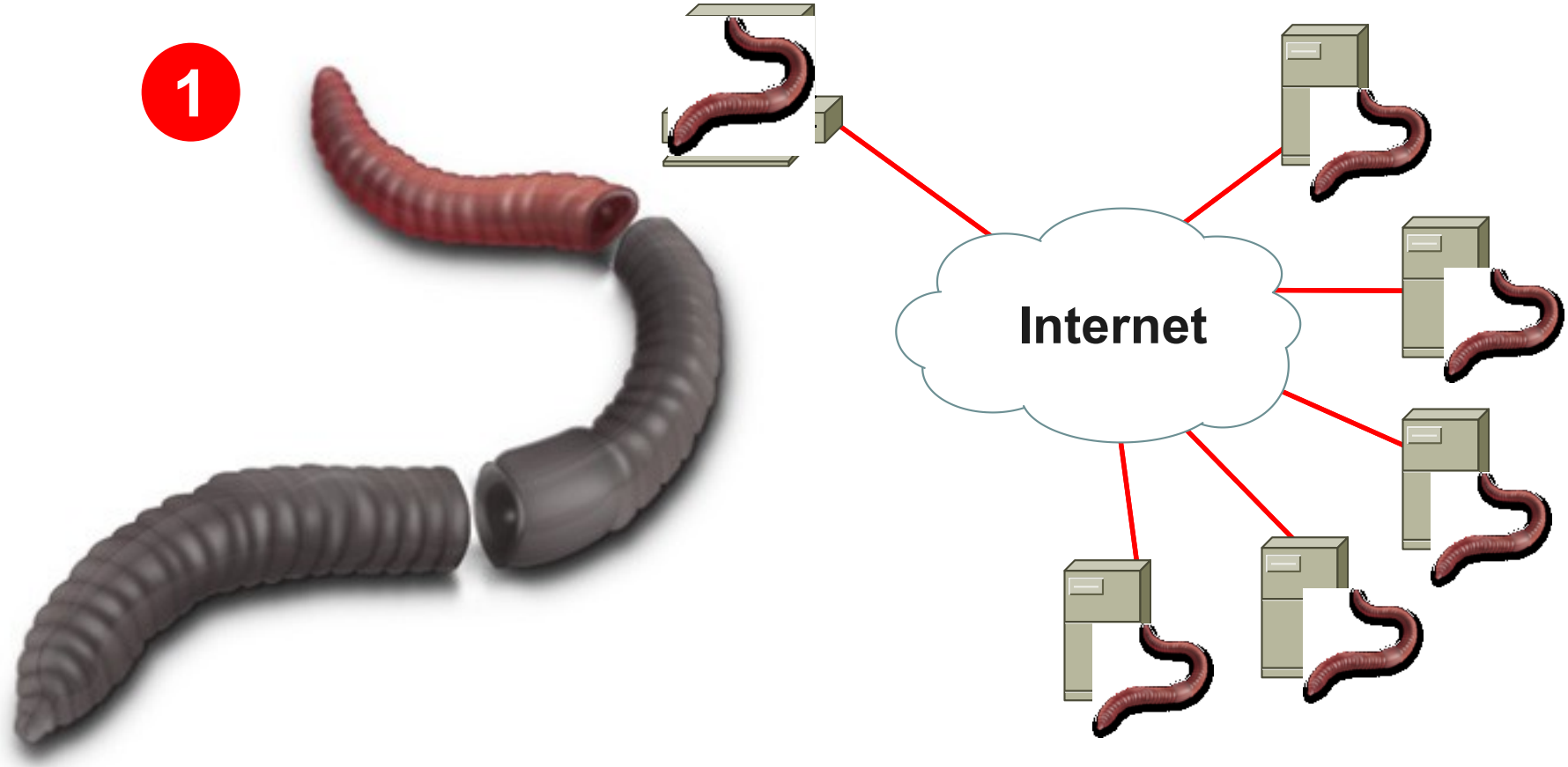
Anatomy of a Worm

1—The Enabling Vulnerability

2—Propagation Mechanism

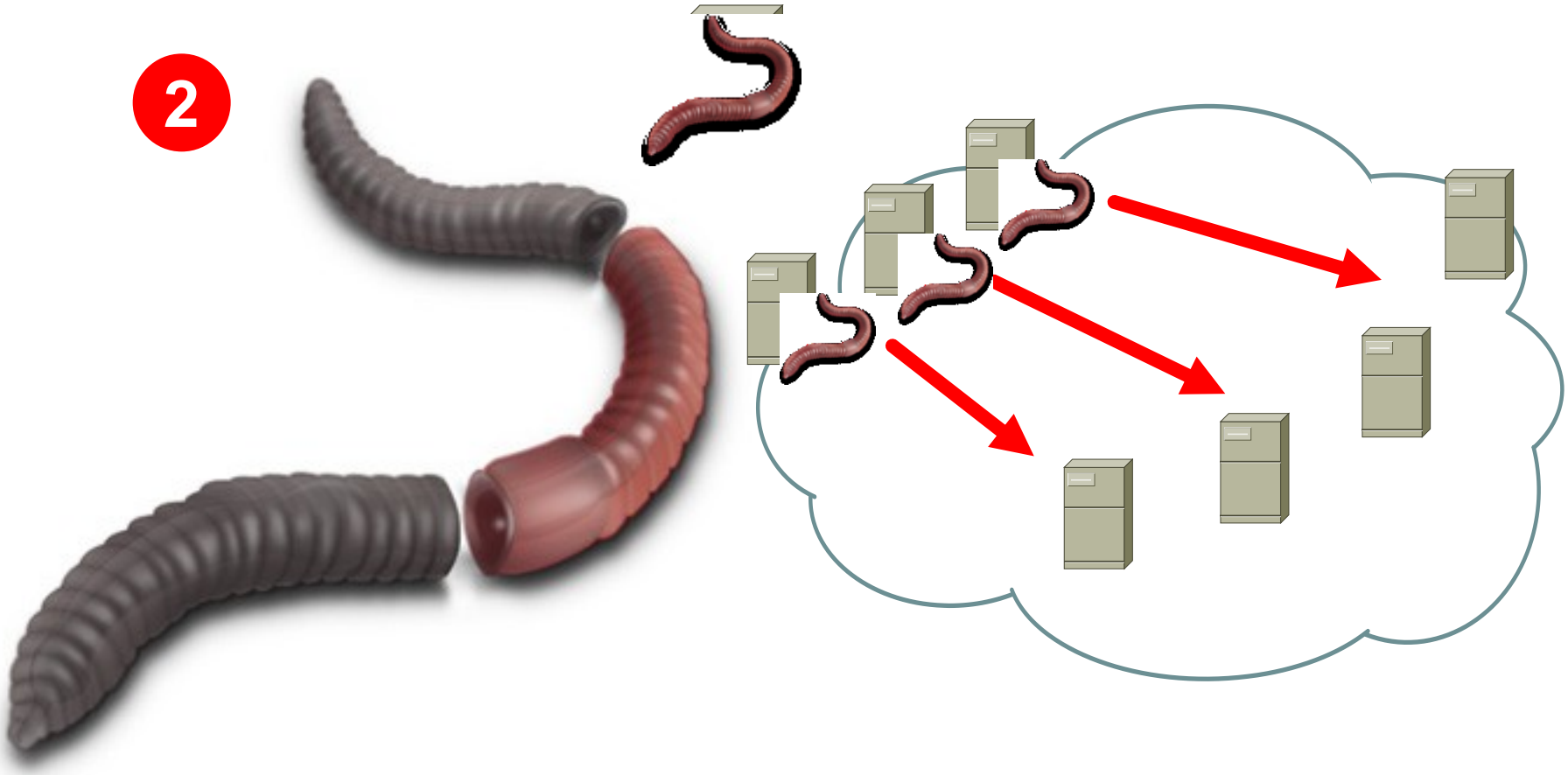
3—Payload

The Enabling Vulnerability



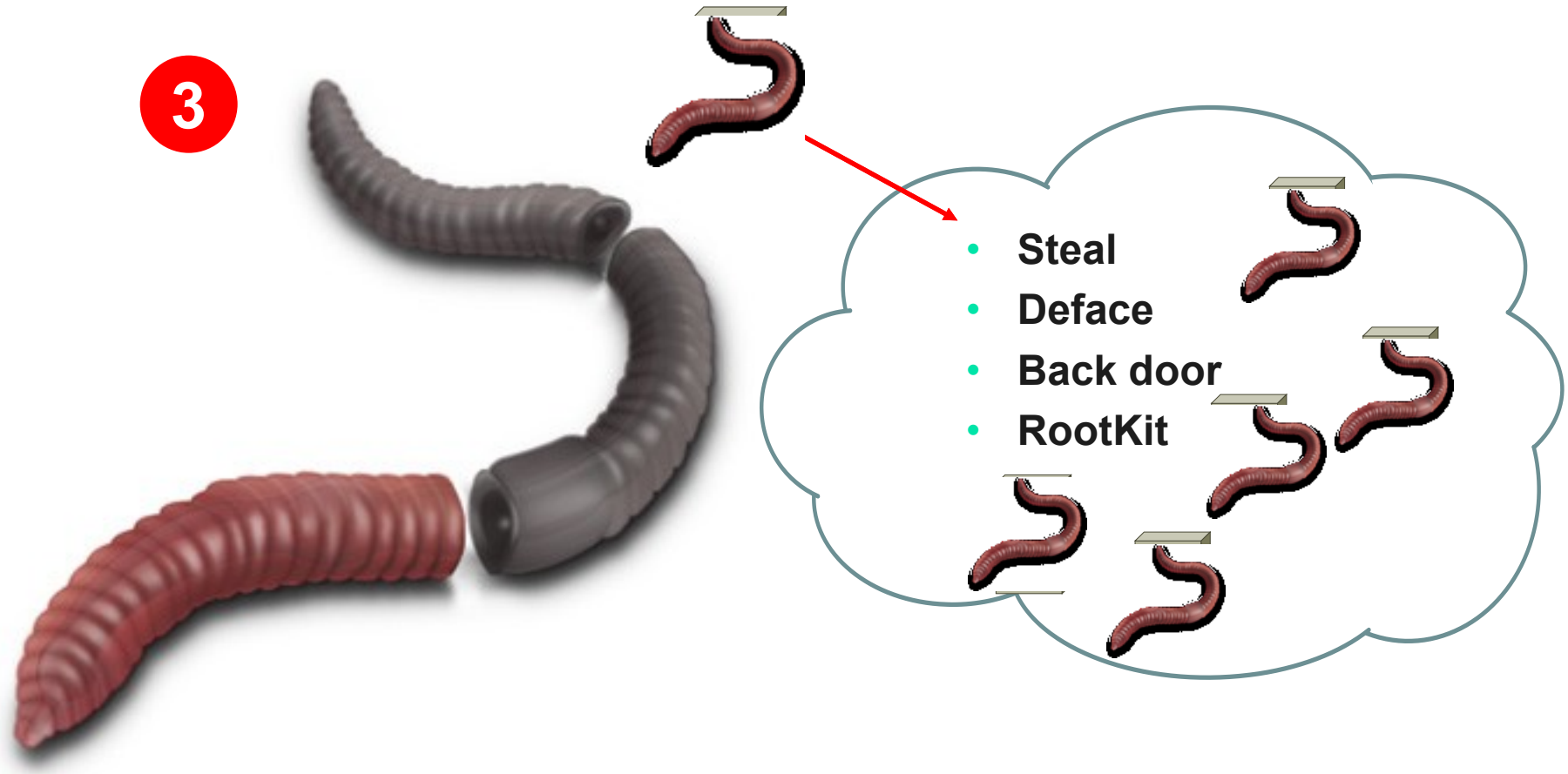
A Worm Installs Itself Using an Exploit Vector on a Vulnerable System

Propagation



After Gaining Access to Devices,
Worm Replicates and Selects New Targets

Payload



Worms and the Infrastructure

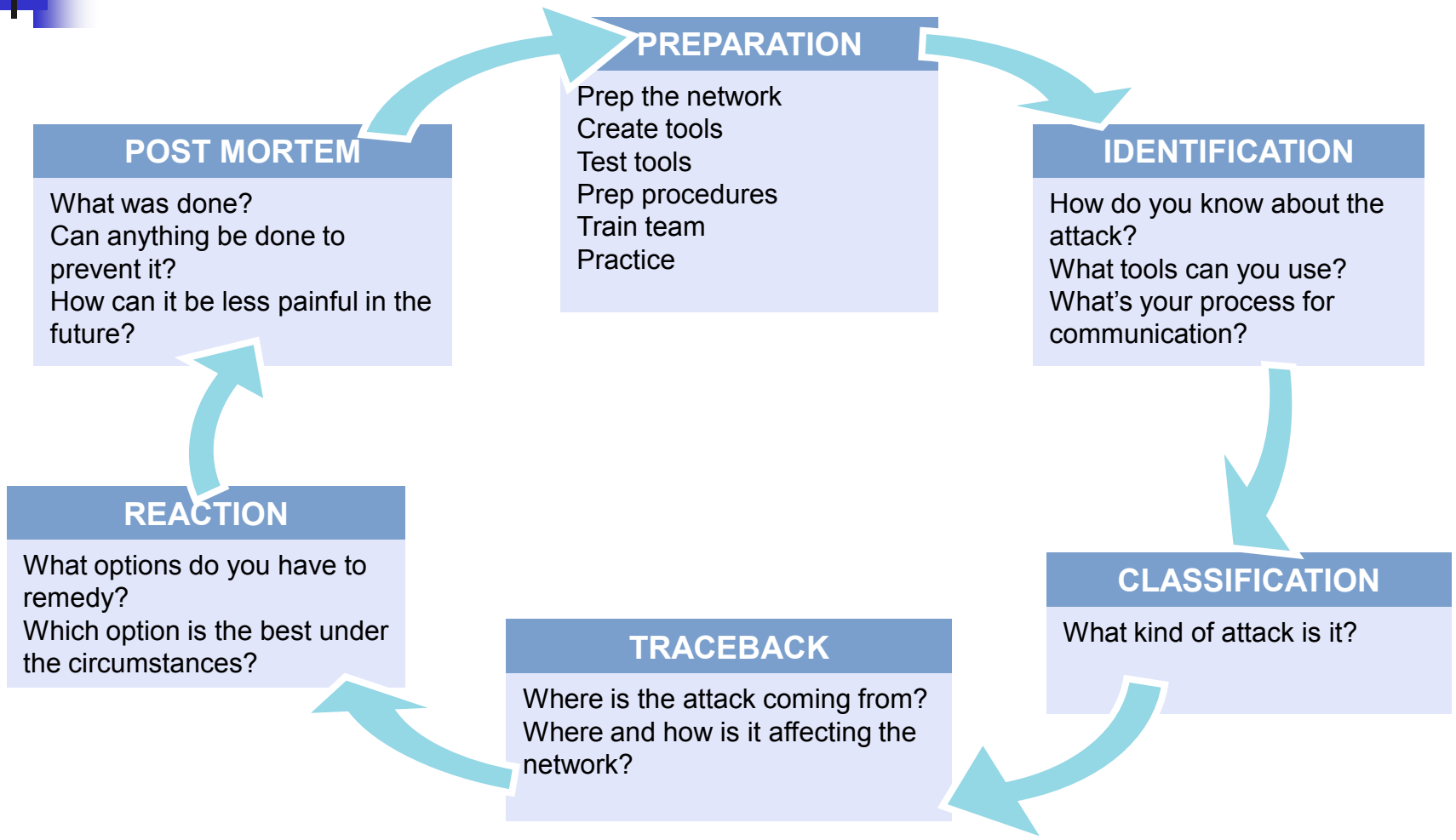
- Worms typically infect end-stations
- Worms have targeted infrastructure as well as direct targets, secondary effects have wreaked havoc
  - Increased traffic
  - Random scanning for destination
  - Destination address is multicast
  - TTL and other header variances
- At the core SP level, the aggregate affects of a worm can be substantial
- Worm severity is escalating and evolving

How Do You Respond?

With Money Being the Key Driver of Miscreant Activity, Large Network Operators Will Need to Respond

- BCP deployment
- Execution of a broad and deep security toolkit
- Rethink some network/service architectures
- Create, staff, and train an operational security (OPSEC) team
- Practice! Practice! Practice!

Six Phases of Incident Response



Preparation

Preparation—Develop and Deploy a Solid Security Foundation

- Includes technical and non-technical components
- Encompasses best practices
- The hardest, yet most important phase
- Without adequate preparation, you are destined to fail
- The midst of a large attack is not the time to be implementing foundational best practices and processes

Preparation

- Know the enemy
  - Understand what drives the miscreants
  - Understand their techniques
- Create the security team and plan
  - Who handles security during an event? Is it the security folks? The networking folks?
- Harden the devices
- Prepare the tools
  - Network telemetry
  - Reaction tools
  - Understand performance characteristics

Identification

Identification—How Do You Know You or Your Customer Is Under Attack?

- It is more than just waiting for your customers to scream or your network to crash
- What tools are available?
- What can you do today on a tight budget?

Ways to Detect

- Customer call
  - "The Internet is down"
- Unexplained changes in network baseline
  - SNMP: line/CPU overload, drops
  - Bandwidth
  - NetFlow
- ACLs with logging
- Backscatter
- Packet capture
- Network IDS
- Anomaly detection

Network Baselines

- NMS baselines
- Unexplained changes in link utilization
  - Worms can generate a lot of traffic, sudden changes in link utilization can indicate a worm
- Unexplained changes in CPU utilization
  - Worm scans can affect routers/switches resulting in increased CPU both process and interrupt switched
- Unexplained syslog entries
- These are examples
  - Changes don't always indicate a security event!
  - Need to know what's normal in order to identify abnormal behavior

Classification

- Classification—understand the details and scope
  of the attack
  - Identification is not sufficient; once an attack is identified, details matter
  - Guides subsequent actions
- Identification and classification are often simultaneous

Classification

- Qualify and quantify the attack without jeopardizing services availability (e.g., crashing a router):
  - What type of attack has been identified?
  - What's the effect of the attack on the victim(s)?
  - What next steps are required (if any)?
- At the very least:
  - Source and destination address
  - Protocol information
  - Port information

Traceback

- Traceback—what are the sources of the attack?
  - How to trace to network ingress points
  - Your Internet connection is NOT the only vector
  - Understand your topology!
- Traceback to network perimeter
  - NetFlow
  - Backscatter
  - Packet accounting
- Retain attack data
  - Use to correlate interdomain traceback
  - Required for prosecution
  - Deters future attacks
  - Clarify billing and other disputes
  - Post mortem analysis

Reaction

Reaction—Do Something to Counter the Attack

- Should you mitigate the attack?
  - Where? How?
- No reaction is a valid form of reaction in certain circumstances
- Reaction often entails more than just throwing an ACL onto a router

Post Mortem

Post Mortem—Analyze the Event

- The step everyone forgets!
- What worked? What didn't? How can we improve?
- What can be done to build build defense against repeat occurrences
- Was the DOS attack you just handled the real threat? Or was it a smoke screen for something else that just happened?
- What can you do to make it faster, easier, less painful in the future?
- Metrics are important!
  - Resources, headcount, etc.