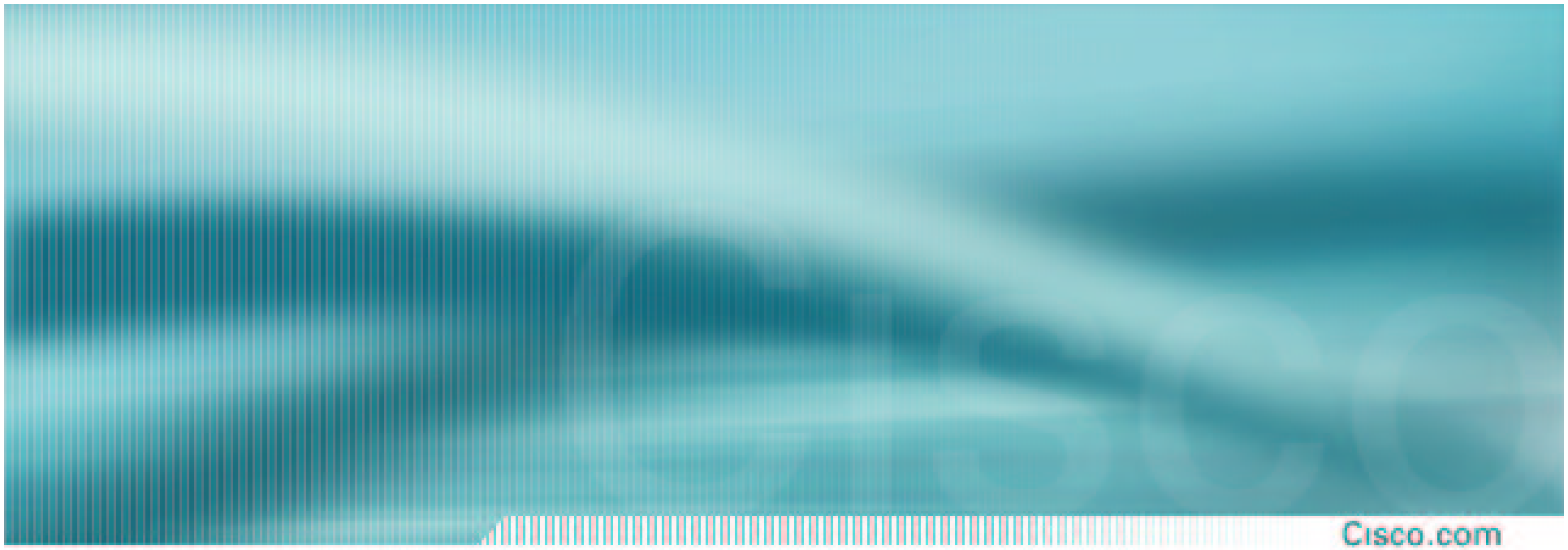


Responding to Security Incidents

Agenda

Cisco.com

- Introduction
- The Nature of Attacks
- Phases of Incident Response
- Tools and Techniques
- Putting It All Together - Case Studies

Goal

- **To empower you with the knowledge of procedures, tools, and techniques you can use to respond to Internet security issues.**

What Incidents?

Do You Care Who's Behind the Incident?

Determined Attackers

Nation States

Script Kiddies

The SQL Slammer Worm: What Happened??

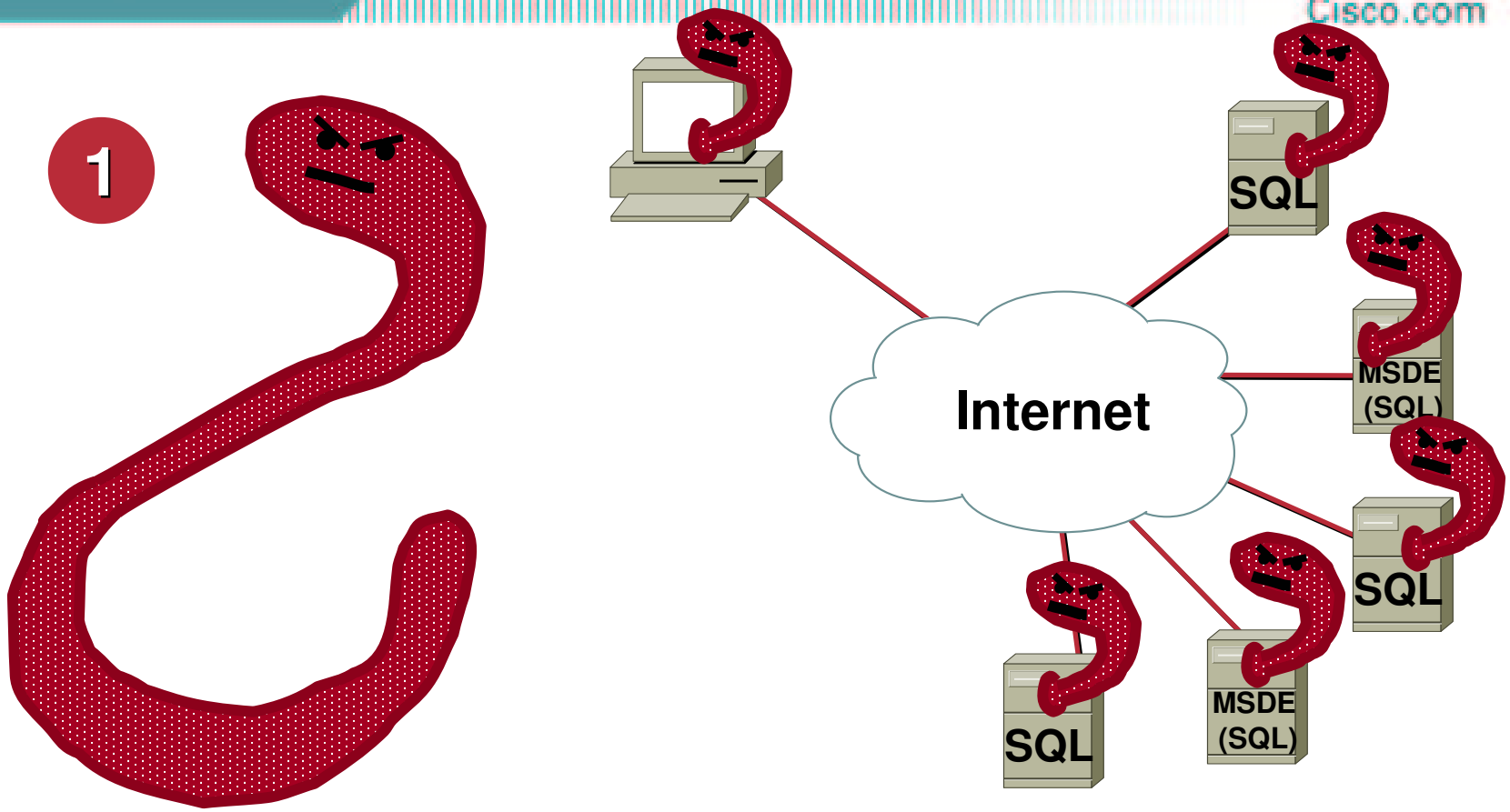
- January 25 2003
- Doubled in size every 8.5 seconds
- Infected 90% of vulnerable hosts within 10 minutes!!
- Saturation point reached within 2 hours of start of infection
- 250,000 – 300,000 hosts infected overall
- Internet Connectivity affected worldwide including bank ATM networks.

source: http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

The SQL Slammer Worm: How It Works

- Exploits vulnerability in Microsoft SQL Resolution Service via buffer overflow attack
- Affected systems include Microsoft SQL Server 2000 hosts as well as hosts with Microsoft Desktop Engine (MSDE) installed
- Vulnerability published in July 2002. Patch was made available from Microsoft at that time.
- Worm executes arbitrary code and installs a copy of itself into the infected computer's memory – which infects other hosts.

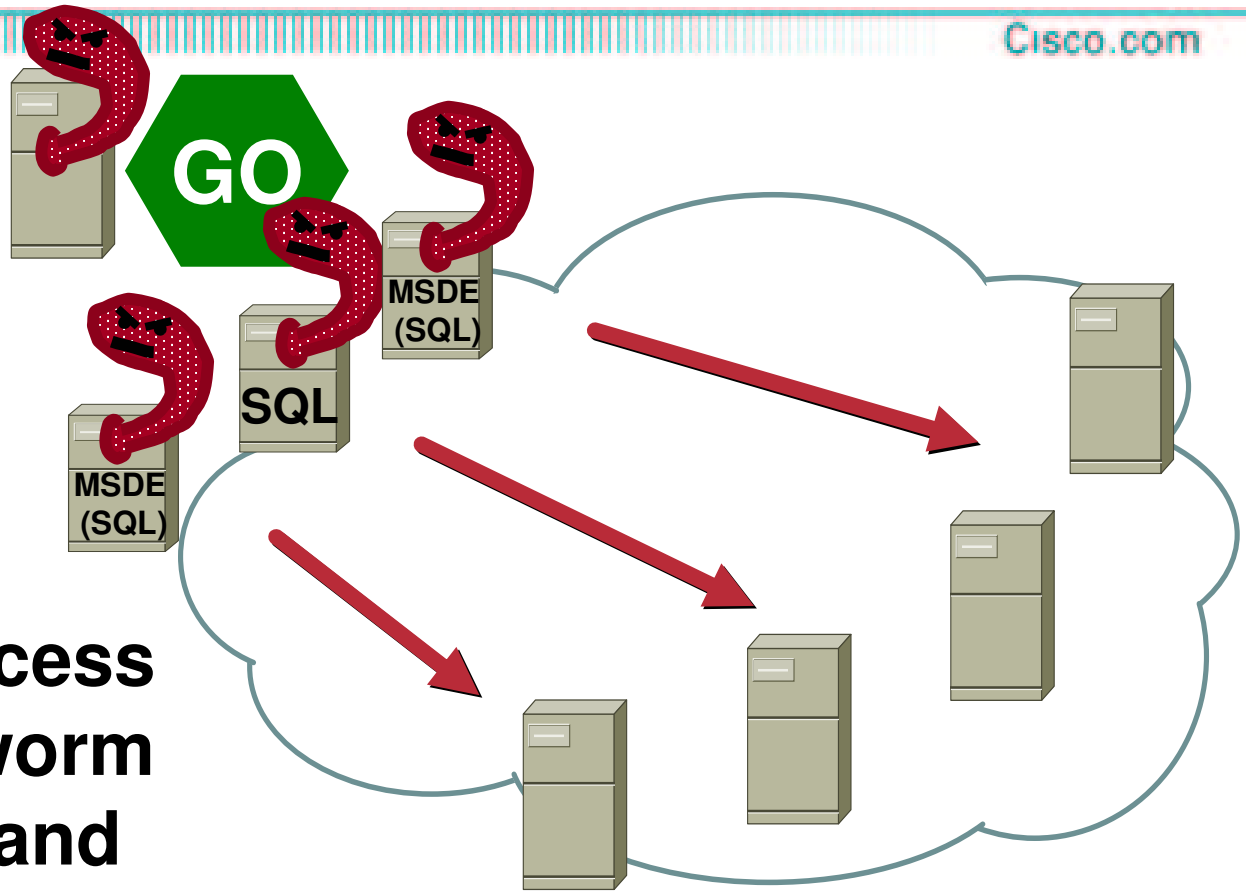
The Enabling Vulnerability



Using the SQL Monitor Service buffer overflow attack, worm installs itself on SQL servers.

Propagation

2

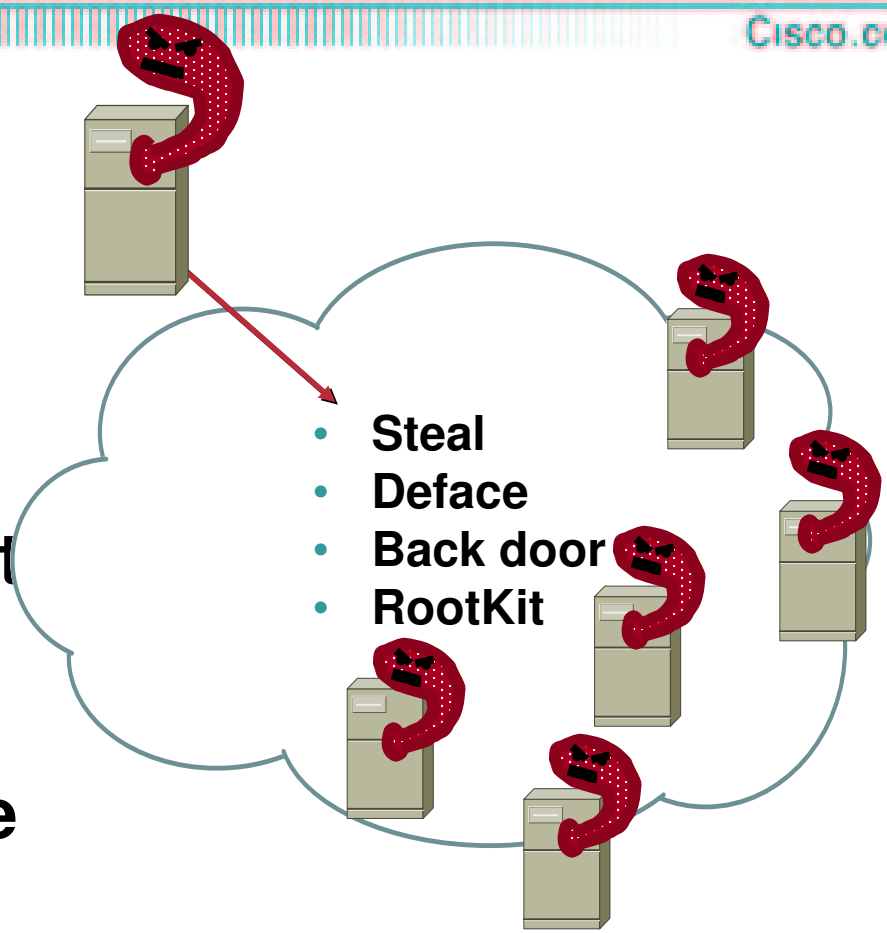


After gaining access to servers, the worm replicates itself and selects new targets.

Payload

3

- When the server is infected with the worm, the attacker has access to the host as the SYSTEM user
- Attacker could use a local exploit to elevate his privilege level to Administrator



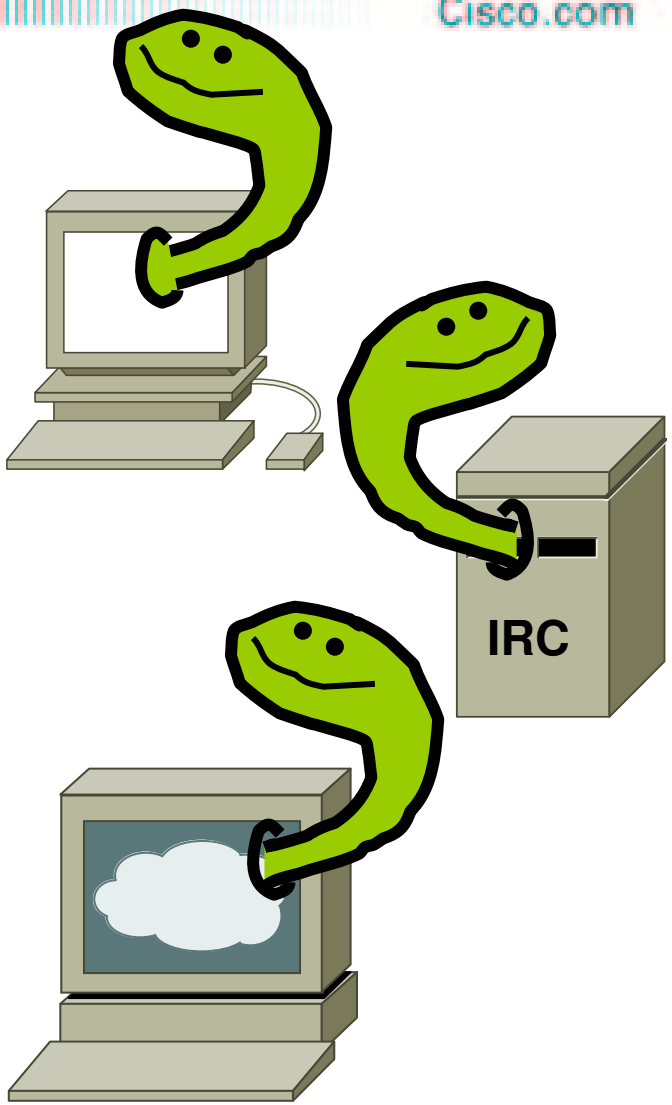
Network Effects Of The SQL Slammer Worm

Cisco.com

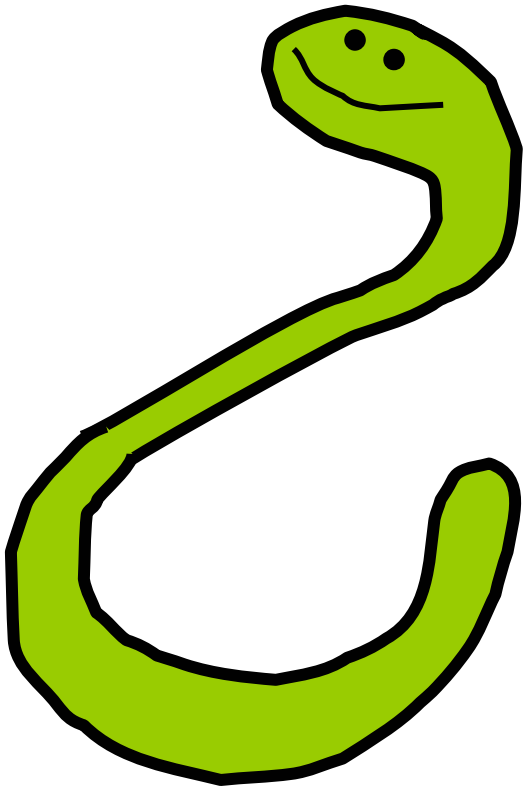
- Several service providers noted significant bandwidth consumption at peering points
- Average packet loss at the height of infections was 20%
- Country of South Korea lost almost all Internet service for period of time
- Financial ATMs were affected
- SQL Slammer overwhelmed some airline ticketing systems

Fizzer Worm Details

- First appeared around May 8, 2003
- Transmitted two ways:
  - as e-mail with various subject lines and message body texts
  - infecting shared files folder used by the Kazaa peer to peer file sharing program and spreads over the Kazaa network
- If a user opens the attached file or otherwise activates the worm via P2P file sharing, three files are added to the Windows directory:
  - initbak.dat, which is a copy of the worm
  - iservc.exe, which is a copy of the worm
  - progop.exe
  - iservc.dll, which contains the keystroke logging Trojan
- Modifications to the registry are made
- Signs of infection include unexpected traffic on ports 6667 (IRC) and 5190 (AIM)

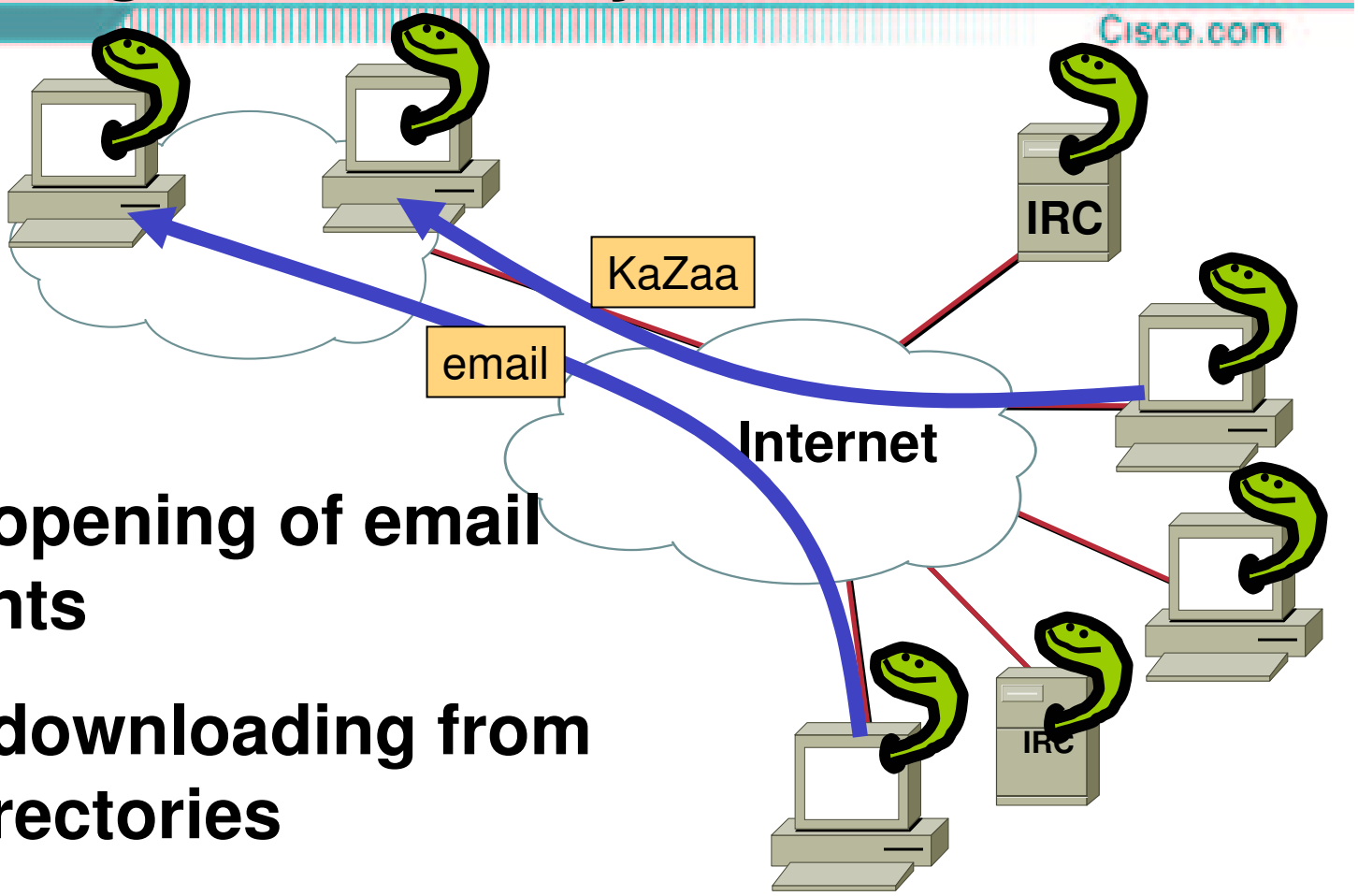


The Fizzer Worm: How It Works



- **Mass-email type worm**
- **Affects systems running Windows**
- **Worm executes arbitrary code and installs a copy of itself into the infected computer's memory – which infects other hosts.**

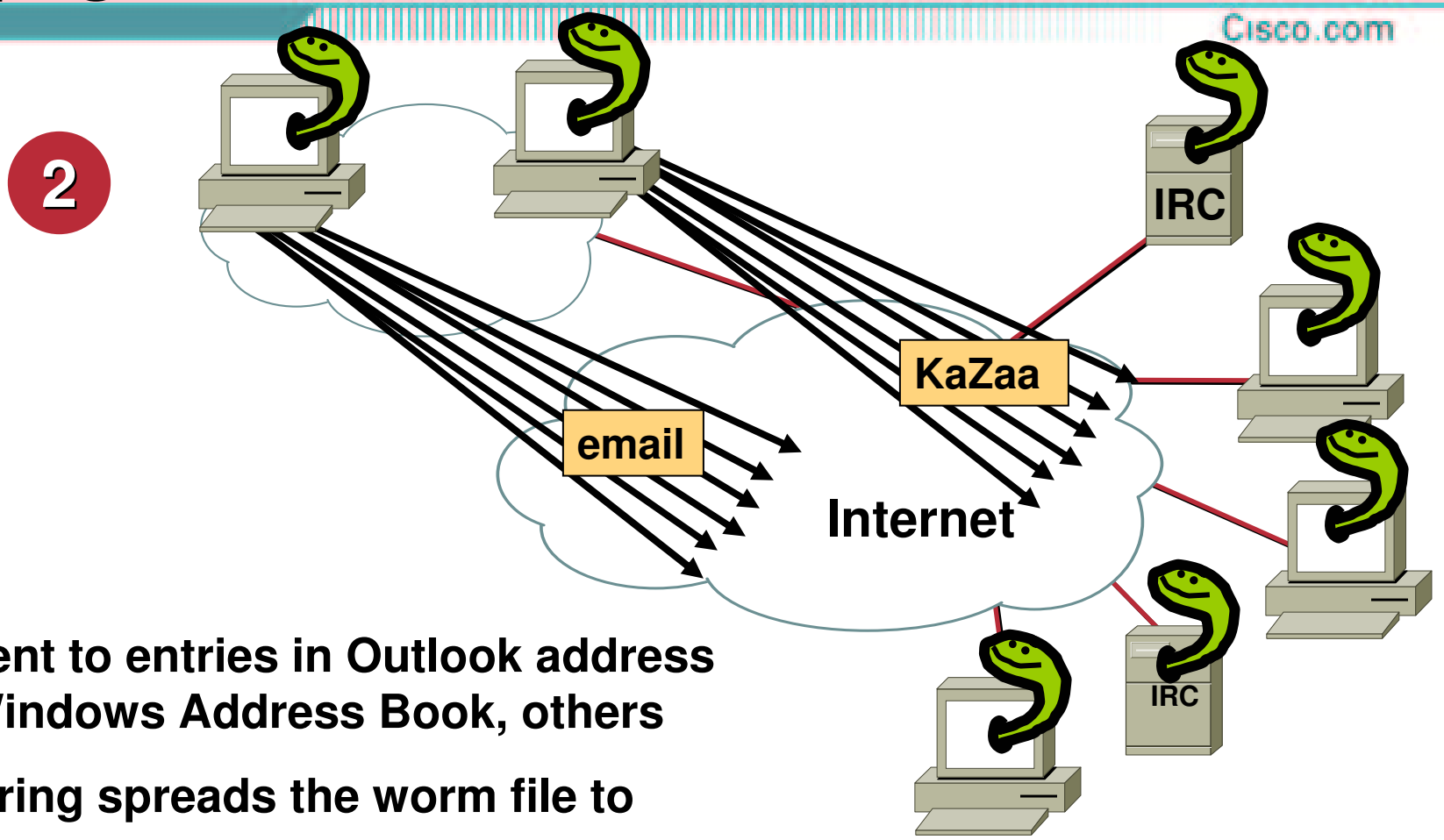
The Enabling Vulnerability



Careless opening of email attachments

Careless downloading from shared directories

Propagation

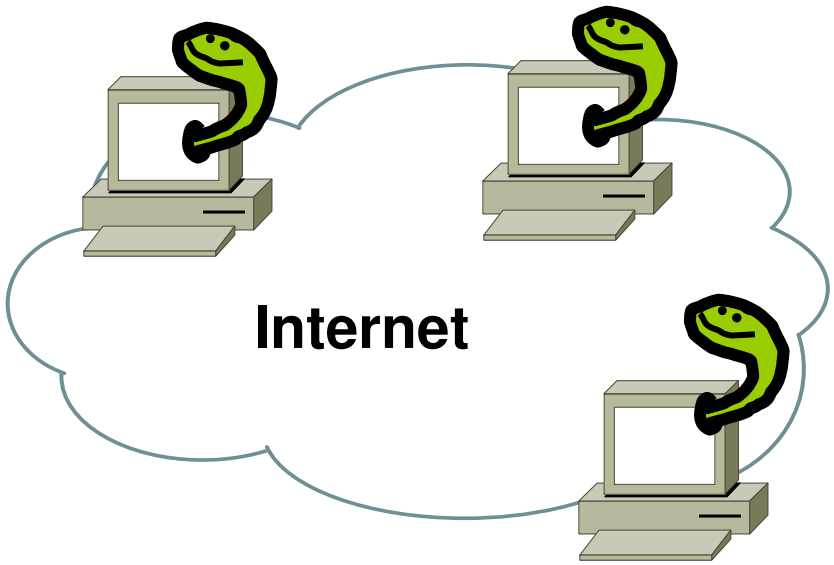


Email sent to entries in Outlook address book, Windows Address Book, others

File sharing spreads the worm file to other peers

Payload

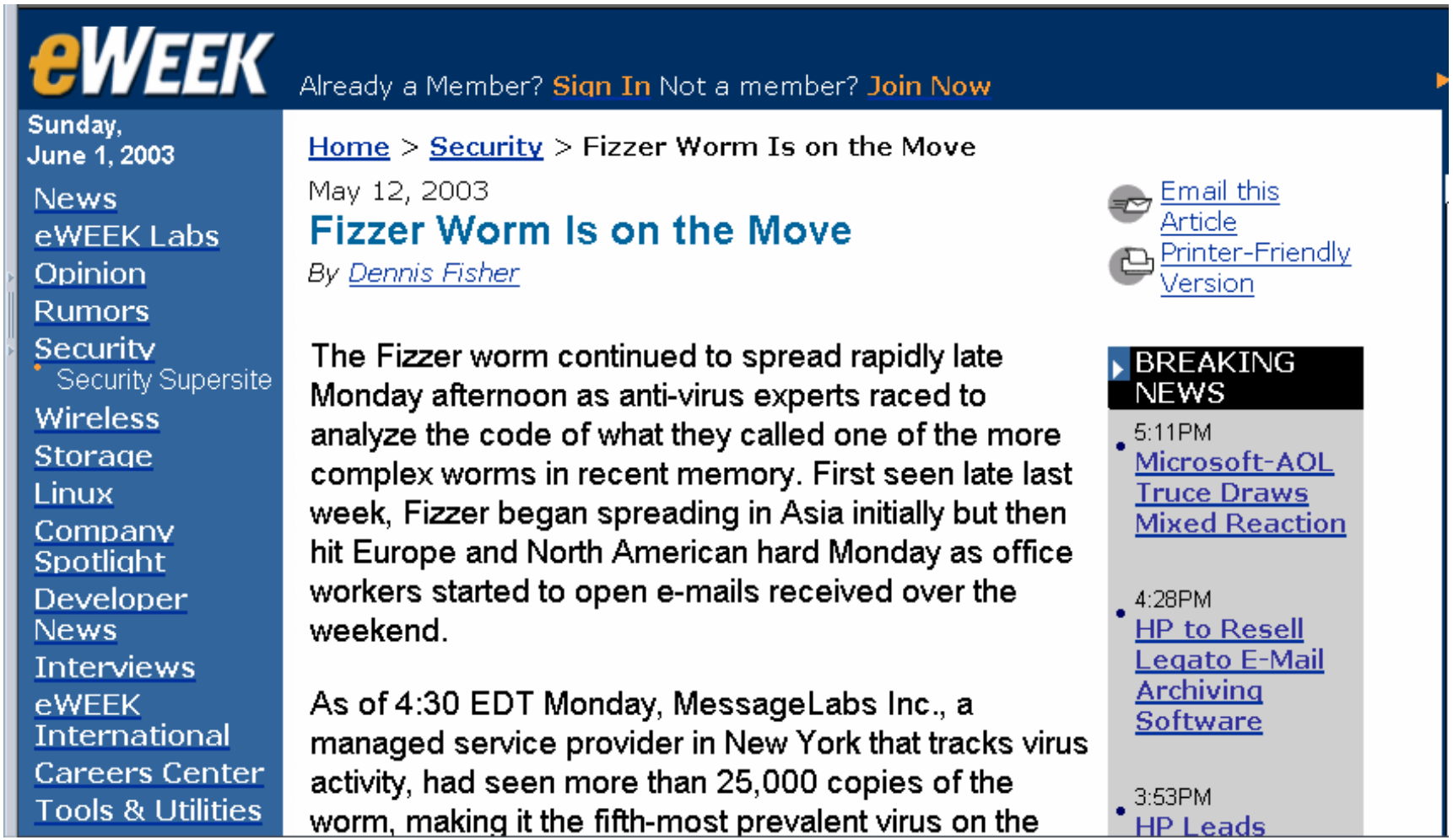
3



Keystroke logger:
The worm captures typed keystrokes and stores them in a encrypted file named iservc.klg in the Windows directory.

HTTP server:
The worm runs an HTTP server on port 81. The web server acts as a console from which information can be gathered, or instructions given

Fizzer Worm



eWEEK

Already a Member? Sign In Not a member? Join Now

Sunday,
June 1, 2003

News
eWEEK Labs
Opinion
Rumors
Security
Security Supersite
Wireless
Storage
Linux
Company Spotlight
Developer News
Interviews
eWEEK International
Careers Center
Tools & Utilities

Home > Security > Fizzer Worm Is on the Move

May 12, 2003

Fizzer Worm Is on the Move

By Dennis Fisher

Email this Article
Printer-Friendly Version

The Fizzer worm continued to spread rapidly late Monday afternoon as anti-virus experts raced to analyze the code of what they called one of the more complex worms in recent memory. First seen late last week, Fizzer began spreading in Asia initially but then hit Europe and North American hard Monday as office workers started to open e-mails received over the weekend.

As of 4:30 EDT Monday, MessageLabs Inc., a managed service provider in New York that tracks virus activity, had seen more than 25,000 copies of the worm, making it the fifth-most prevalent virus on the

BREAKING NEWS

- 5:11PM Microsoft-AOL Truce Draws Mixed Reaction
- 4:28PM HP to Resell Legato E-Mail Archiving Software
- 3:53PM HP Leads

More Recently: Fizzer Worm

2 - 3 Weeks Later

Cisco.com

30 May 2003
Updated: 16:53 GMT

The Register

Biting the hand that feeds IT

Fizzer blasts Klez-H off top spot in viral charts

By John Leyden
Posted: 30/05/2003 at 15:27 GMT

The newly emerged Fizzer worm has displaced Klez as the most common viral menace on the Internet over the last month.

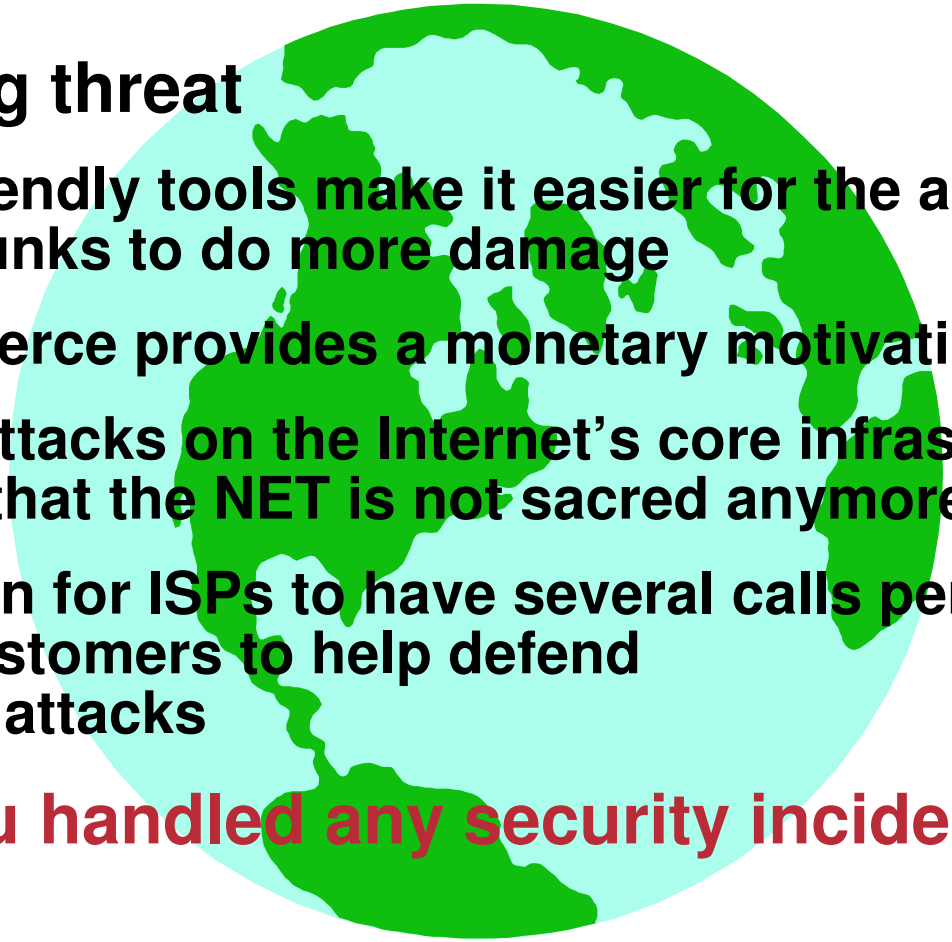
Managed services firm Messagelabs blocked Fizzer 497,846 times in May, relegating Klez-H (293,028 interceptions) to fourth place in the firm's monthly viral charts.

MessageLabs reports that one in 145 emails it processed this month contained a virus.

The company also operates an anti-spam service. In May, for the first time, spam exceeded legitimate email in percentage terms. The global ratio of spam in email scanned by MessageLabs Anti-Spam service was 1 in 1.8 (55.1 per cent) emails.

Over at anti-virus firm Sophos the Palyh (Microsoft support) worm was the most common subject of support calls with Fizzer coming in as the second most commonly reported irritant. In MessageLabs

The Internet World Today



- **Changing threat**
  - **User friendly tools make it easier for the amateur cyberpunks to do more damage**
  - **eCommerce provides a monetary motivation**
  - **Direct attacks on the Internet's core infrastructure means that the NET is not sacred anymore**
  - **Common for ISPs to have several calls per day from their customers to help defend against attacks**
- **Have you handled any security incidents lately?**

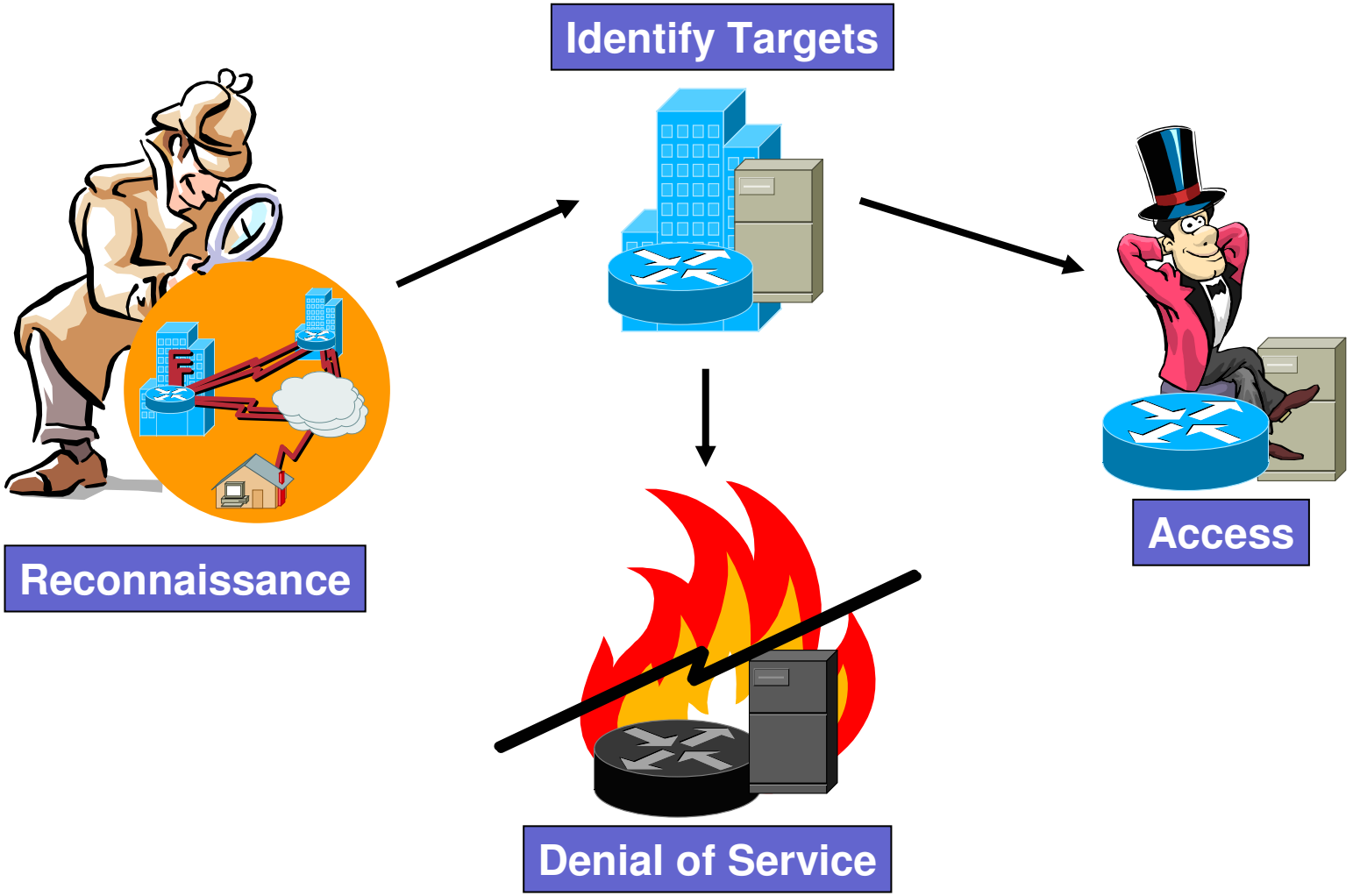
Agenda

Cisco.com

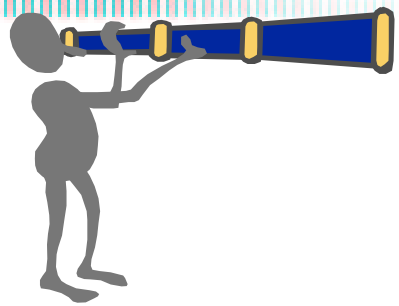
- Introduction
- The Nature of Attacks
- Phases of Incident Response
- Tools and Techniques
- Putting It All Together - Case Studies

Steps In A Typical Attack

Cisco.com



Reconnaissance



- **Obtaining information**

  Unauthorized discovery and mapping of systems, services, or vulnerabilities

- **Common Commands and Administrative Utilities**

  nslookup, ping, netcat, telnet, finger, rpcinfo, file explorer, dumpacl

- **Public Tools**

  Sniffers, NMAP, xprobe, Whisker, SATAN, SAINT, custom scripts

Access

- **Access**

  Unauthorized data manipulation, system access, or privilege escalation

- **Access Methods**

  Exploiting passwords: brute force, cracking tools

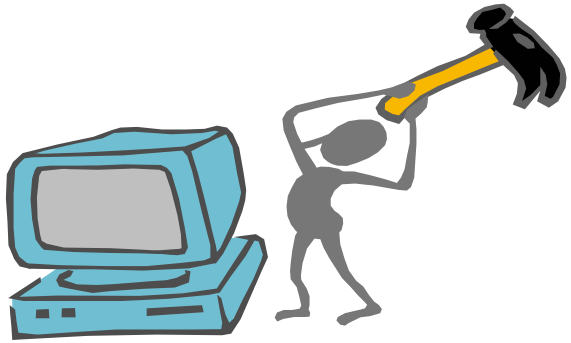
  Exploit poorly configured or managed services

  Exploiting protocol weaknesses: Fragmentation, TCP session hijacking

  Exploiting application holes

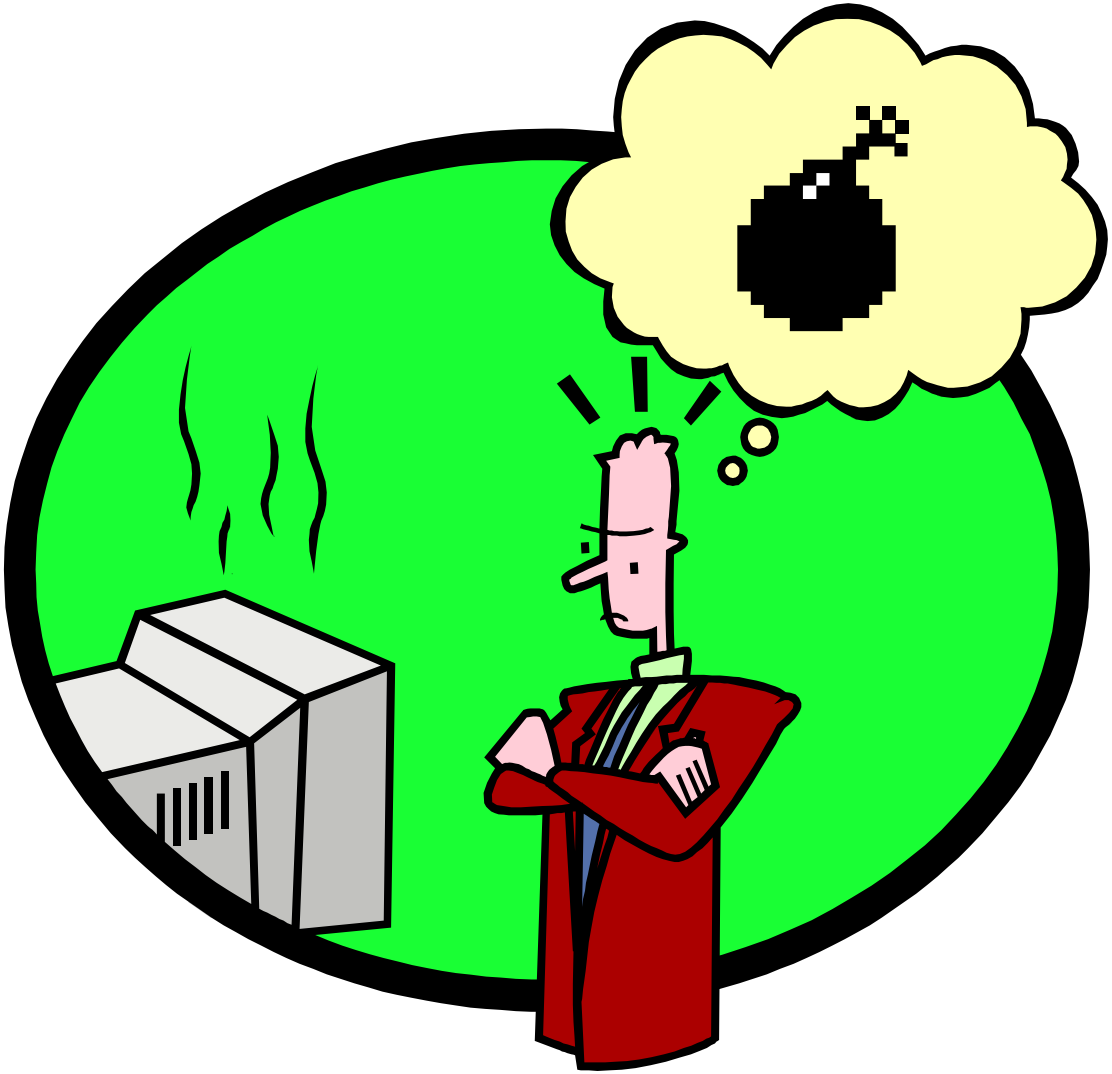
  Trojan horses: Programs that plant a backdoor into a host

Denial of Service (DoS)



- **Denial of Service**
  - **Disable or disrupt networks, systems or services**
- **Denial of Service Methods**
  - **Overloading resources**
  - **Exploiting software bugs**
- **Attacks can be distributed for amplification**

Now What????



Symptoms and Artifacts of Attacks

- **Reconnaissance**
  - **Log entries**
  - **Suspicious probes such as numerous unsuccessful login attempts**
  - **Unusual packets on the network: unexpected ARP, strange ICMPs, TCP packets with unusual flags**
  - **Increase in traffic**
  - **Intrusion detection alarms and notifications**
  - **None: passive sniffers being used**

Symptoms and Artifacts of Attacks (Cont.)

Cisco.com

- **Access**

  Machine has open ports that were not open before

  Strange traffic: UDP to some new open port, encrypted packets. May be inbound or outbound.

  Added/deleted/modified accounts (Inability of a user or administrator to log in due to account modifications could be a sign of this)

  High activity on a previously low usage account

  Log entries

  Intrusion detection alarms and notifications

  Accounting discrepancies (e.g., if the operating system accounting files shrink in size)

Symptoms and Artifacts of Attacks (Cont.)

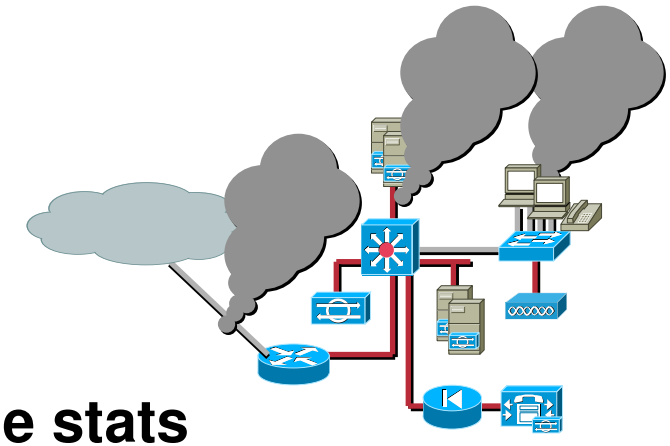
- **Access (cont.)**

  - **Device reboots**
  - **Excessive device resource utilization: memory, cpu, disk, …**
  - **Unexplained increased device activity**

  - **Added/deleted/modified software**
  - **Added/deleted/modified data files: including changes to configuration files, changes in file lengths or dates**
  - **Anomalies: odd messages displayed, unusual beeps, anything out of the ordinary**

Symptoms and Artifacts of Attacks (Cont.)

- **Denial of Service (DoS)**
  - **Sluggish or clogged network: poor network performance**
  - **Excessive device/network link resource utilization: memory, cpu, or disk exhaustion**
  - **Unexplained poor device/system performance**
  - **Unresponsive device**
  - **Device reboots**
  - **Device crashes**
  - **Log entries**
  - **System resource/service usage stats**



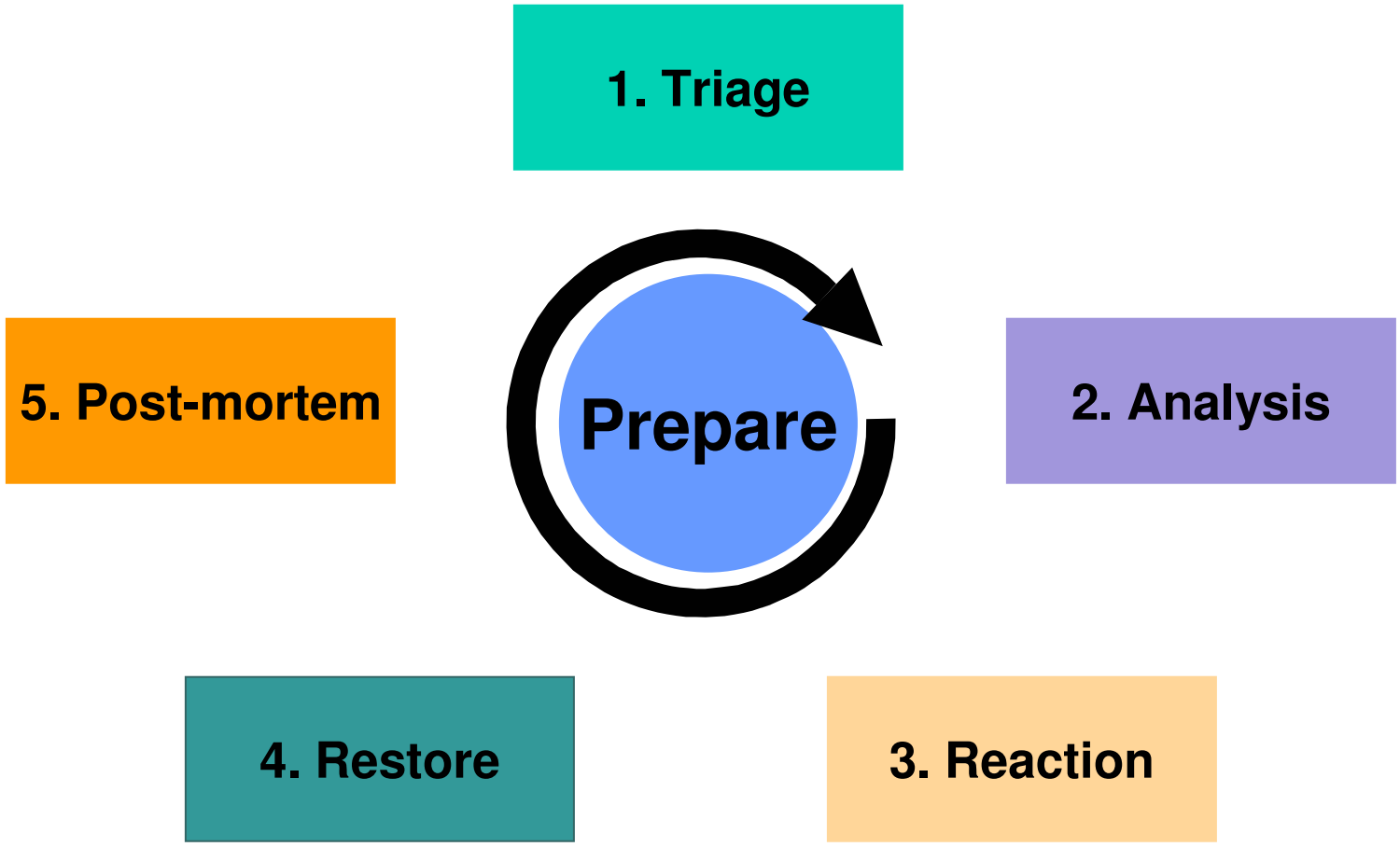
You Must Have A Plan

- **So that you can quickly respond to the incident**
  - **To minimize the damage to systems, services, data, and the network**
  - **To contain the scope of the incident**
  - **To avoid possibly costly media exposure and legal liabilities**

Agenda

- Introduction
- The Nature of Attacks
- Phases of Incident Response
- Tools and Techniques
- Putting It All Together - Case Studies

Phases of Security Incident Response



Be Prepared

- Be aware of current attack methods that can affect the devices and services in your network
  - e.g., may DoS attacks use forged source addresses
- Establish a secure archive of original media, configuration files, and security-related patches for all network device images, operating systems, and application software versions
  - Establish effective, reliable backup tools and procedures and test them
  - Ghost is your friend
- Develop an accurate set of contact information
  - Examples: internal infosec, management, ISP security contact, public relations and legal, incident response teams, law enforcement

Be Prepared (Cont.)

- **Setup secure communications mechanism**

  Don't use the compromised host when sending email; the telephone is actually ok!

- **Assemble a toolkit (crash kit) to be used when responding to incidents and make sure you know how to use them before an incident occurs**
- **Test your response procedures**
- **Maintain an isolated test network**
- **Keep response plans, procedures and tools up to date**

Classes of Incidents

Cisco.com

- **Destruction of Assets: destruction or unauthorized modification of corporate information, data, or systems**
- **Unauthorized Disclosure of sensitive information, including intellectual property**
- **Unauthorized Access: escalation of privileges or intentionally bypassing controls**
- **Denial of Service**
- **Reconnaissance**
- **Others**

Classes of Incidents

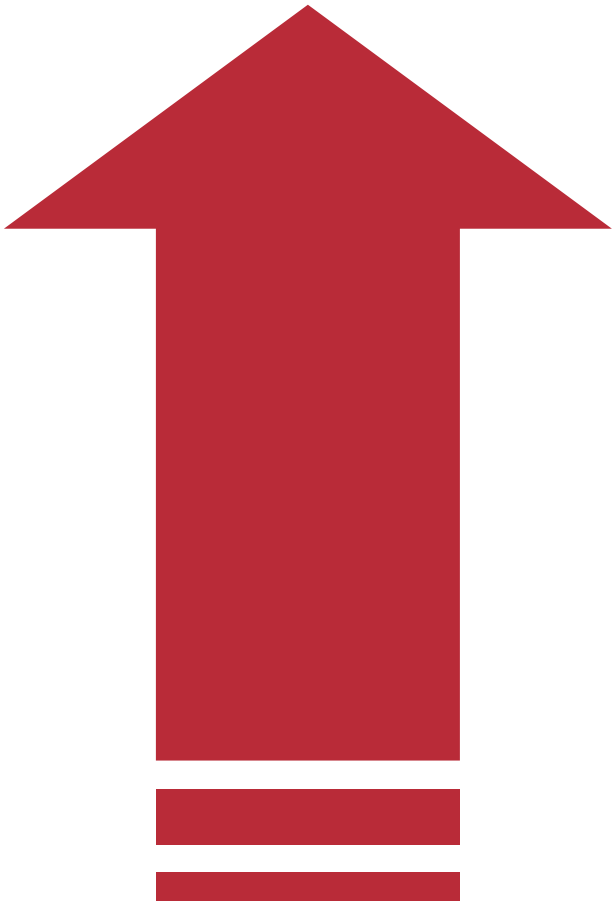
Cisco.com

- Not all incidents are created equal
- You must prioritize in order to optimize the use of resources
- Decide what's important to you

If you don't care about it, don't look for it!

One Way to Prioritize Resources

1. Exploitation, target vulnerable, confirmed compromise
2. Exploitation, target vulnerable, unknown compromise
3. Exploitation, target not vulnerable
4. Exploitation



Risk = Vulnerability * Value * Threat

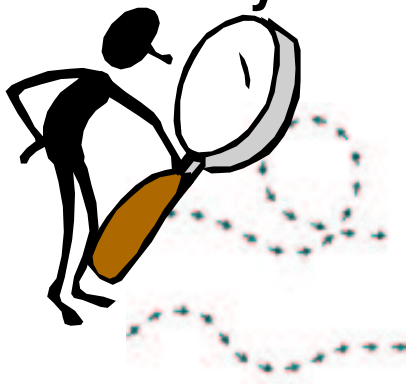
Triage - Initial Analysis and Response

Cisco.com

- **Verify that the event is an actual incident**
  - **How do you know you are under attack?**
  - **Do you know when maintenance activities are scheduled?**
  - **Do you have a way to identify attacks directed at your devices and services?**
- **Stop the bleeding**
  - **Turn off device**
  - **Remove device from network**
- **Communicate**

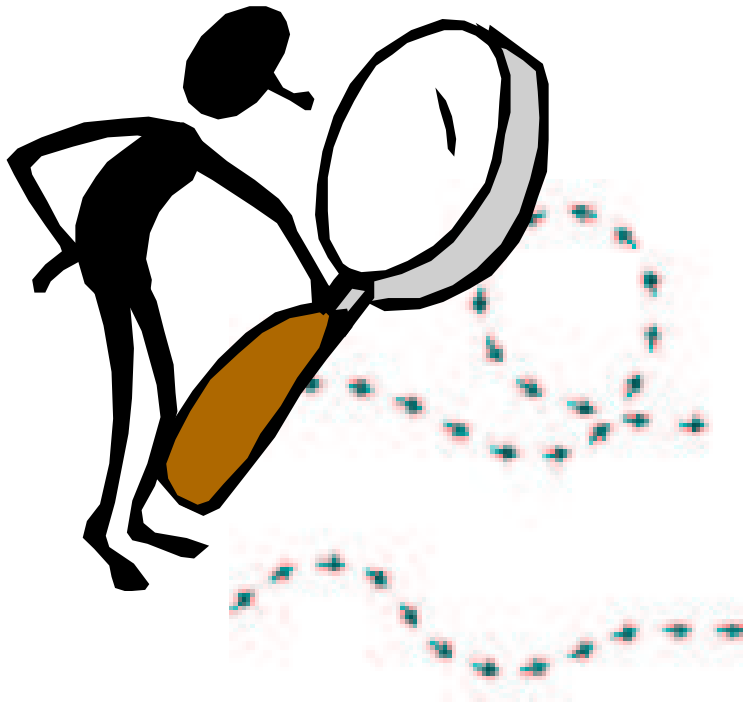
Analysis

- **Classification: understanding the type of attack and what damage is it causing**
  - **You need to know what you are getting hit with**
  - **How can you do this without crashing your router or your e-commerce servers?**
- **Traceback: from where is the attack originating?**
  - **Know your ISP, they can continue the trace beyond your network**
  - **Sometimes this is NOT important**



Analysis (Cont.)

- Scope the incident: the number of devices, data, and other resources affected - Look beyond the initially identified target
- Measure the impact: what are the resulting effects of the incident on the organization
  - Loss of online e-commerce service
  - Employees unable to access corporate network from remote branches, etc.
- Results of analysis guide you in your selection of reaction to the incident

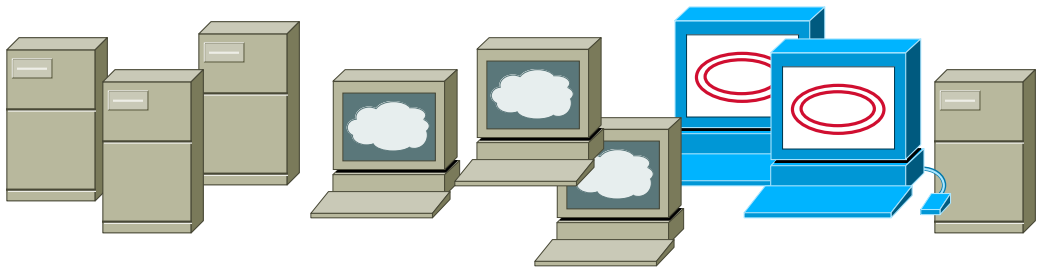


Reaction

- **Doing something to counter the attack – even if you choose to do nothing.**
  - **Should you mitigate the attack?**
  - **It is often more then just throwing an ACL onto a router.**
- **Generally, the highest priority is to regain full function of all devices and services**
- **It is often less important to find the perpetrator of the attack**

Restoring Operational Functionality

- **Servers:**
  - **Reload system software from secure backup or from distribution media; do NOT trust backups**
  - **Apply corrective actions: patches, new configuration, …**
  - **Change static passwords where appropriate**



Restoring Operational Functionality (Cont.)

- **Network devices like routers, switches:**
  - **Ensure correct image is loaded, if patch exists ensure you load the patched image**
  - **Update configuration to address problem**
  - **Change static passwords where appropriate**

Buffer Overflow in Instant Messenger

CNET tech sites: Price comparisons | Product reviews | Tech news
Downloads | Site ma

c|net NEWS.COM TECH NEWS FIRST

Front Page | Enterprise | E-Business | Communications | Media | Personal Technology | Investor

Yahoo issues IM, chat security patches

By Evan Hansen
Staff Writer, CNET News.com
May 30, 2003, 6:09 PM PT

Yahoo issued on Friday security patches for its Yahoo Instant Messenger and Yahoo Chat clients in an effort to fix a buffer overflow vulnerability discovered in the software.

When users of the software log on to the IM network or enter a chat room, Yahoo is prompting them to install the patches. In addition, the company posted the patches on its Web site.

A buffer overflow is a common security vulnerability in computer programs written in C and C++ that allows more information to be added to a chunk of memory than it was designed to hold.

Buffer overflow attacks in Yahoo IM and Yahoo Chat could lead to a

advertisement
The Perfect Combination of Features.

Search News.com
Go!
Advanced search

Latest Headlines
display on desktop
Nextel to up U.S. 'push to talk' range
Macromedia updates e-learning tools
Altnet to pay Kazaa users for swapping
HP, Opsware to join forces on data center
Electrolux charges forward with IBM
Microsoft to abandon standalone IE

Post Mortem

- **Fully analyzing, in depth, what just happened. Determining what can be done to build resistance to the attack happening again**

  Was the attack you just handled, the real threat? Or was it a smoke screen for something else that just happened?

- **Learning from experience: what can you do to make handling this type of incident faster, easier, and less painful in the future?**

Do it! This is the step everyone forgets or chooses to ignore!

And Sometimes It's Not This Easy

Cisco.com

- You may need to restore servers and network devices to operational state before you have completed analysis
- If you don't eliminate all known vulnerability, it's likely the attacker will repeat using an unpatched vulnerability
- You may have to restore multiple times!

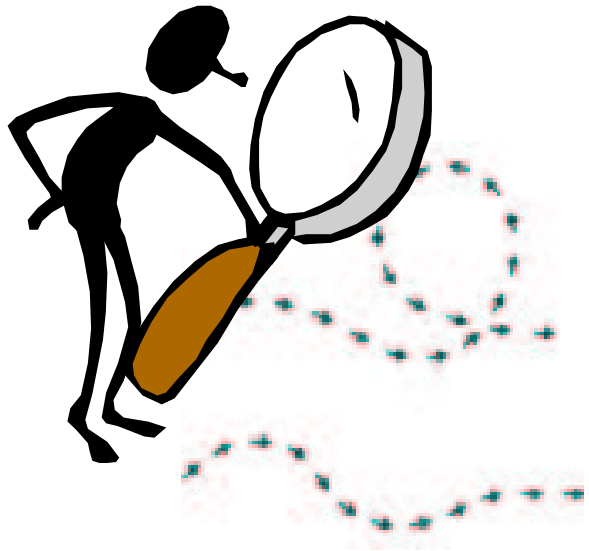
Agenda

Cisco.com

- Introduction
- The Nature of Attacks
- Phases of Incident Response
- Tools and Techniques
- Putting It All Together - Case Studies

Analysis and Identification

- **What's Available**
  - **Intrusion Detection Systems**
  - **Operating system utilities: netstat**
  - **Logging**
  - **ACLs**
  - **Netflow**
  - **Sniffers**



Intrusion Detection Systems

Cisco.com

- IDS sensors provides real-time monitoring and misuse detection
- They can detect a wide range of attacks
- Most sensors are designed not to impact network performance and are completely transparent to the end user.
- Commercial and public tools
- Network and host-based IDS available

netstat

Cisco.com

NETSTAT(8) Linux Programmer's Manual NETSTAT(8)

NAME

netstat - Print network connections, routing tables, interface statistics, masquerade connections, and multi-cast memberships

- Lots and lots of options:

  To get help use netstat -h

  netstat -a, --all Shows both listening and non-listening sockets. With the --interfaces option, show interfaces that are not marked

netstat output

Cisco.com

```
[testhost]$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:32768                 *:*                     LISTEN
tcp        0      0 localhost:32769         *:*                     LISTEN
tcp        0      0 *:sunrpc                *:*                     LISTEN
tcp        0      0 *:http                  *:*                     LISTEN
tcp        0      0 *:10000                 *:*                     LISTEN
tcp        0      0 *:tacacs                *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
tcp        0      0 wwwin-cons:domain       *:*                     LISTEN
tcp        0      0 localhost:domain        *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 *:smtp                  *:*                     LISTEN
tcp        0      0 localhost:rndc          *:*                     LISTEN
tcp        0      0 testhost:ssh            sj-host1.cisco:1656 ESTABLISHED
tcp        0      0 testhost:ssh            sj-host2.cisco:32805 ESTABLISHED
tcp        0      0 testhost:ssh            sj-host3.cisco:4835 ESTABLISHED
```

Logging

- **Syslog: standard logging facility available on most operating systems and network devices**
  - **routers**
  - **firewalls**
  - **servers**
  - **whatever you have!**

Configuring Syslog on a Router

- **To log messages to a syslog server host, use the logging global configuration command**

```
logging host
logging trap level
```

- **To log to internal buffer use:**

```
logging buffered size
```

Typical Syslog Configurations

Cisco.com

```
logging on
logging standby
logging console warnings
logging trap informational
logging host dmz 10.30.1.2
```

Pix

```
logging on
logging 10.30.1.2
logging trap informational
```

IOS Router

Syslog Output Examples

IOS Router

```
02-15-2003 11:58:20 Local7.Info 10.30.1.1 30: 00:24:17: %SEC-6-
IPACCESSLOGP: list 100 permitted tcp 192.168.1.14(0) -> 10.30.1.1(0), 1 packet

02-15-2003 11:58:06 Local7.Info 10.30.1.1 29: 00:24:03: %SEC-6-
IPACCESSLOGP: list 100 permitted tcp 192.168.1.14(0) -> 172.16.1.1(0), 16
packets
```

Pix

```
2003-02-08 03:30:02 Local4.Warning 172.16.1.1 %PIX-4-106023:
Deny tcp src outside: 12.36.111.161/42247 dst inside:10.30.1.2/80 by
access-group "dirty_list"
2003-02-08 03:30:05 Local4.Warning 172.16.1.1 %PIX-4-106023: Deny
tcp src outside: 12.36.111.161 /42247 dst inside:1-.3-.1.2/80 by access-
group "dirty_list"
```

Using Access Control Lists - ACLs

- **Access control lists can be helpful in both analyzing and responding**

  You can use the `show access-list xxx` command to see how many packets have hit it

  You can use the `log/log-input` keyword to send information to syslog

  Once you understand the traffic that is giving you problems, you can create an ACL to block it

Classifying DoS with ACLs

- **Requires ACLs to be in place (for classifying)**

```
Extended IP access list 169
        permit icmp any any echo (2 matches)
        permit icmp any any echo-reply (21374 matches)
        permit udp any any eq echo
        permit udp any eq echo any
        permit tcp any any established (150 matches)
        permit tcp any any (15 matches)
        permit ip any any (45 matches)
```

Found:
- attack type
- interface

-> Watch performance impact
-> Normally only on demand, not pro-active
-> More used for checking than for detection

Tracing DoS and Other Attacks

Cisco.com

- **If source prefix is not spoofed:**
  - **Routing table**
  - **Internet Routing Registry (IRR)**
  - **Direct site contact**
- **If source prefix is spoofed:**
  - **Trace packet flow through the network**
  - **Find upstream ISP**
  - **Upstream needs to continue tracing**

The Internet Routing Registry (IRR): Network Info


```
madrid% whois -h whois.arin.net 64.103.0.0
Cisco Systems, Inc. (NETBLK-CISCO-GEN-6)
   170 West Tasman Drive
   San Jose, CA 95134
   US
   Netname: CISCO-GEN-6
   Netblock: 64.100.0.0 - 64.104.255.255

   Coordinator:
      Huegen, Craig  (CAH5-ARIN)  chuegen@cisco.com
      +1-408-526-8104 (FAX) +1 408 525 2597

   Domain System inverse mapping provided by:

   NS1.CISCO.COM             192.31.7.92
   NS2.CISCO.COM             192.135.250.69
   DNS-SJ6.CISCO.COM           192.31.7.93
   DNS-RTP4.CISCO.COM           192.135.250.70
   Record last updated on 11-Jan-2001.
   Database last updated on 2-Aug-2001 23:12:13 EDT.
```

- **Europe: whois.ripe.net**
- **Asia-Pac: whois.apnic.net**
- **USA and rest: whois.arin.net**

The Internet Routing Registry (IRR): AS Information

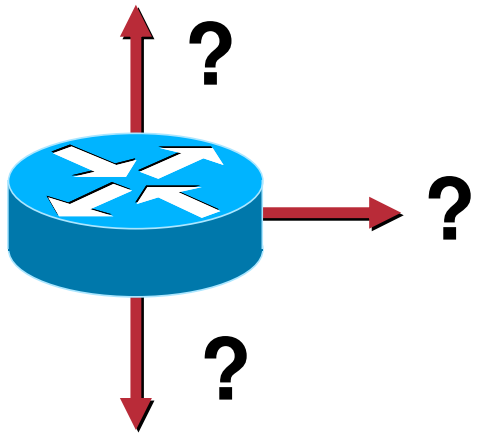

```
madrid% whois -h whois.arin.net "as 109"
Cisco Systems, Inc. (ASN-CISCO)
   170 W. Tasman Drive
   San Jose, CA 95134
   US

   Autonomous System Name: CISCOSYSTEMS
   Autonomous System Number: 109

   Coordinator:
      Koblas, Michelle  (MRK4-ARIN)  mkoblas@CISCO.COM
      (408) 526-5269 (FAX) (408) 526-4575

   Record last updated on 20-May-1997.
   Database last updated on 2-Aug-2001 23:12:13 EDT.
```

Also, if Domain Known: abuse@domain

NetFlow

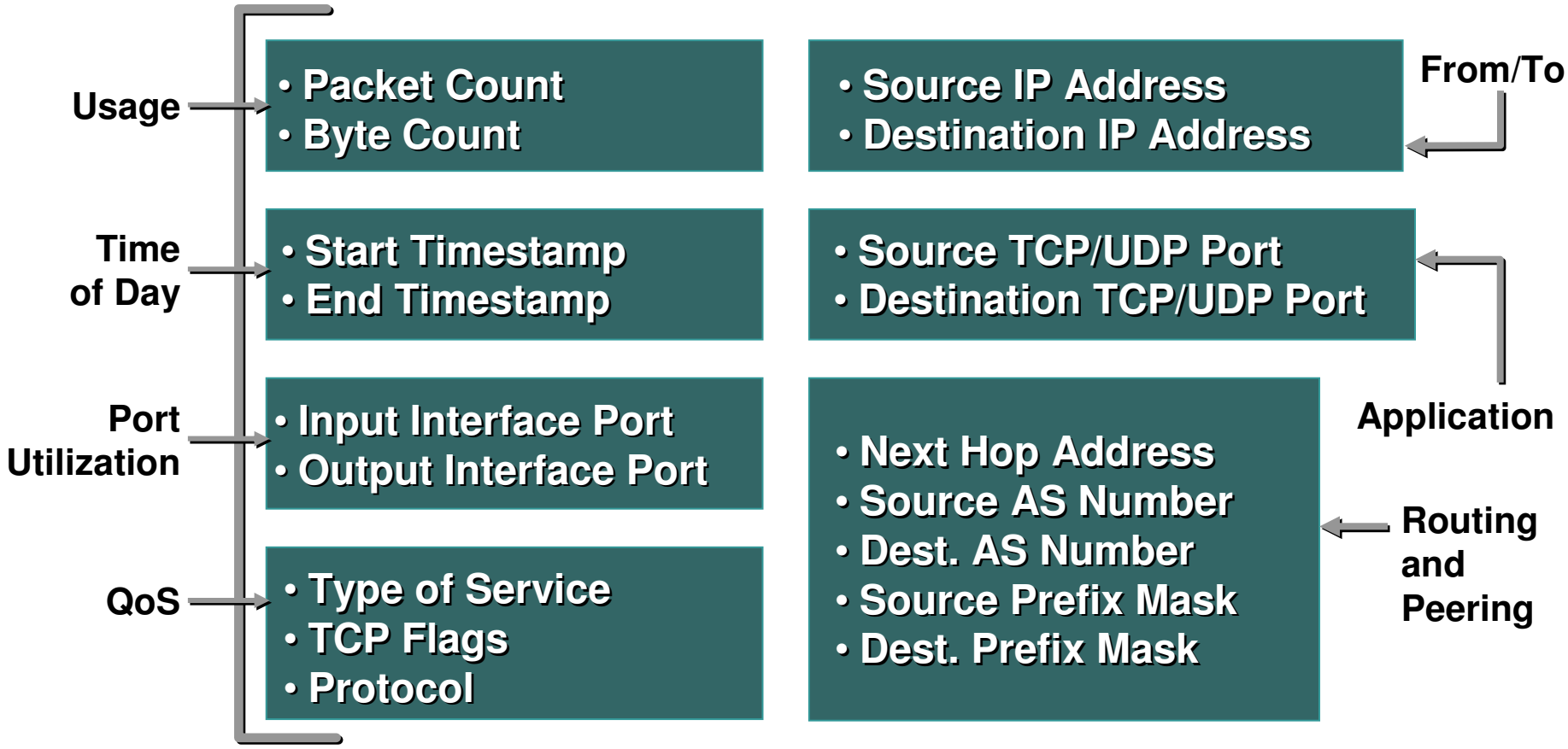
- **NetFlow statistics empowers users with the ability to characterize their IP data flows**
- **For incident response, it can help you traceback the attack path**

Where did it come from?



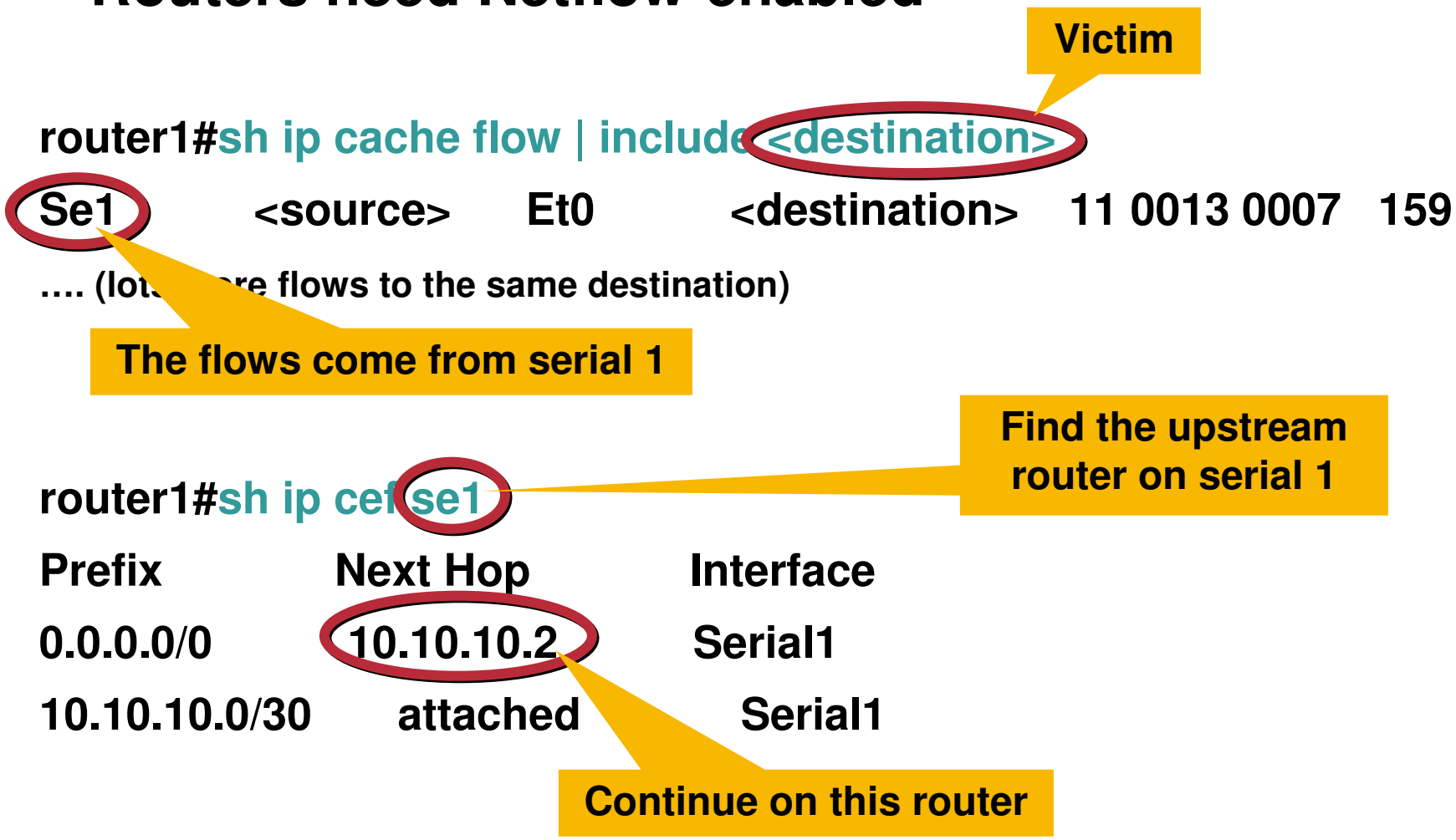
NetFlow Data Record

Cisco.com



Tracing Back with Netflow

- **Routers need Netflow-enabled**



Network Sniffers

- **Allows you to view actual network traffic**
- **Commercial and publicly available**
  - **tcpdump**
  - **ethereal**
  - **Sniffer**

TCPDump Example

Cisco.com

```
07:58:36.613296 ada.48837 > 10.51.2.4.telnet: S
1982589974:1982589974(0) win 8760 <mss 1460> (DF)
```

Timestamp: `07:58:36.613296`

Source IP and Port: `ada.48837`

Destination IP and Port: `10.51.2.4.telnet`

Flags: `S` **(SYN)**

Initial Synchronization Number and Bytes of Data in Payload: `1982589974:1982589974(0)`

Window Size in Bytes: `win 8760`

Maximum Segment Size in Bytes: `mss 1460`

No Option Byte Pads: `none`

Selective Acknowledgment Allowed?: `not specified`

Don't Fragment Bit Present?: `(DF)`

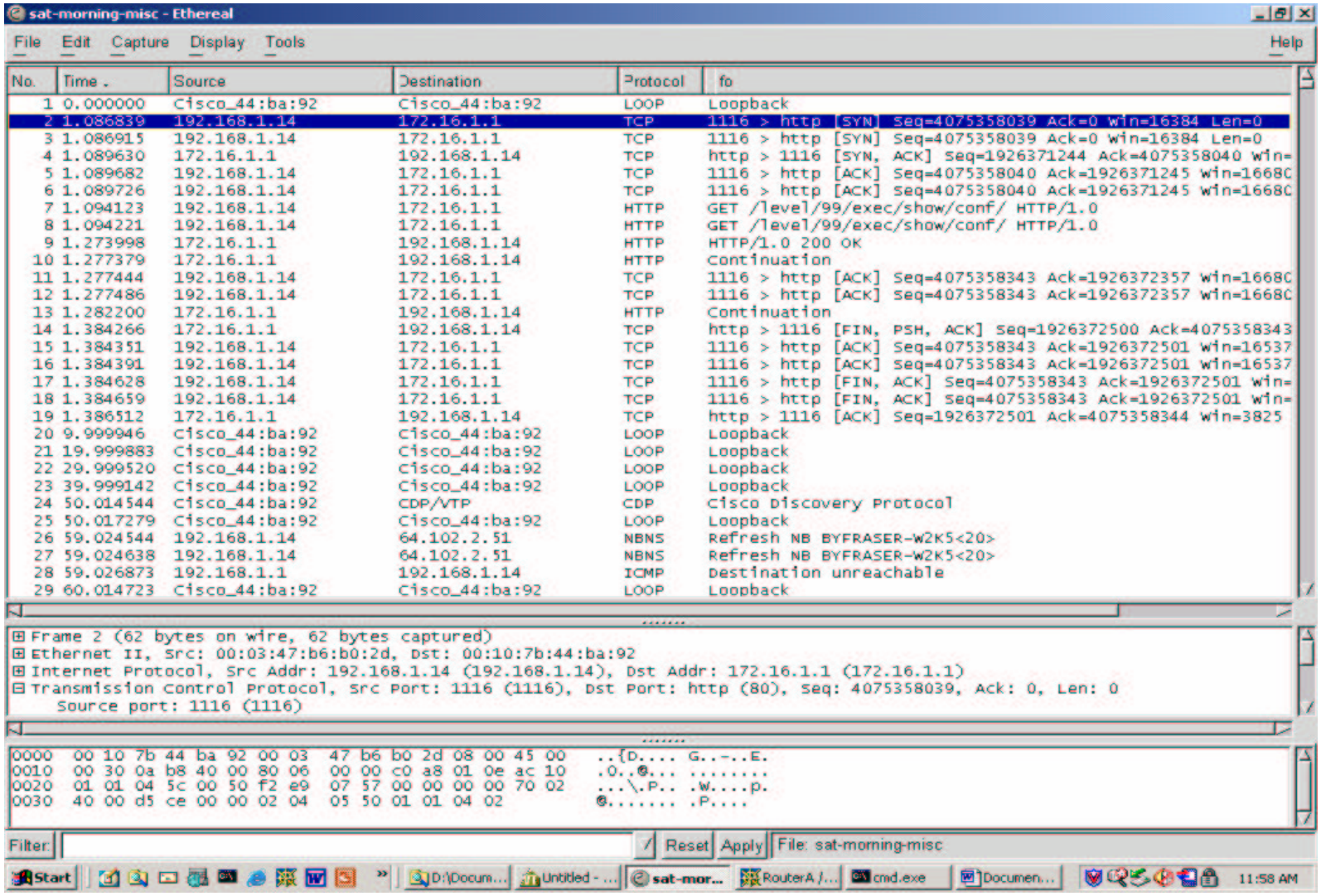
Syn Flood

Cisco.com

```
07:58:36.245995 ada.48664 > 10.51.2.4.1376: S
1970808309:1970808309(0) win 8760 <mss 1460> (DF)

07:58:36.246249 ada.48665 > 10.51.2.4.1652: S
1970938341:1970938341(0) win 8760 <mss 1460> (DF)

07:58:36.246499 ada.48666 > 10.51.2.4.295: S
1971031403:1971031403(0) win 8760 <mss 1460> (DF)

07:58:36.246749 ada.48667 > 10.51.2.4.849: S
1971096604:1971096604(0) win 8760 <mss 1460> (DF)
```

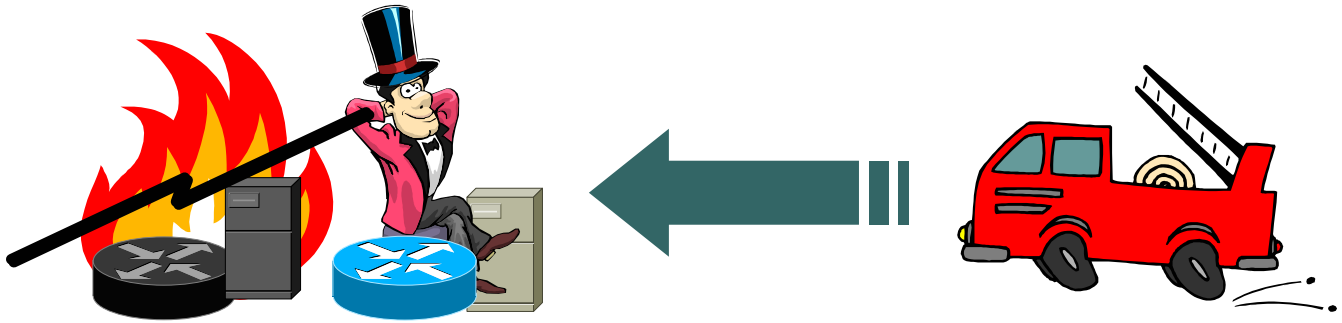
- **Notes:**
  - **Sequential source port numbers**
  - **Randomized destination port numbers**

Ethereal Output



Reaction

- **What's Available**
  - **IDS response mechanisms**
  - **Sink hole router**
  - **ACLs**
  - **Committed Access Rate (CAR)**
  - **Unicast Reverse Path Forwarding (uRPF)**
  - **Network Based Application Recognition (NBAR)**
  - **uRPF and BGP**

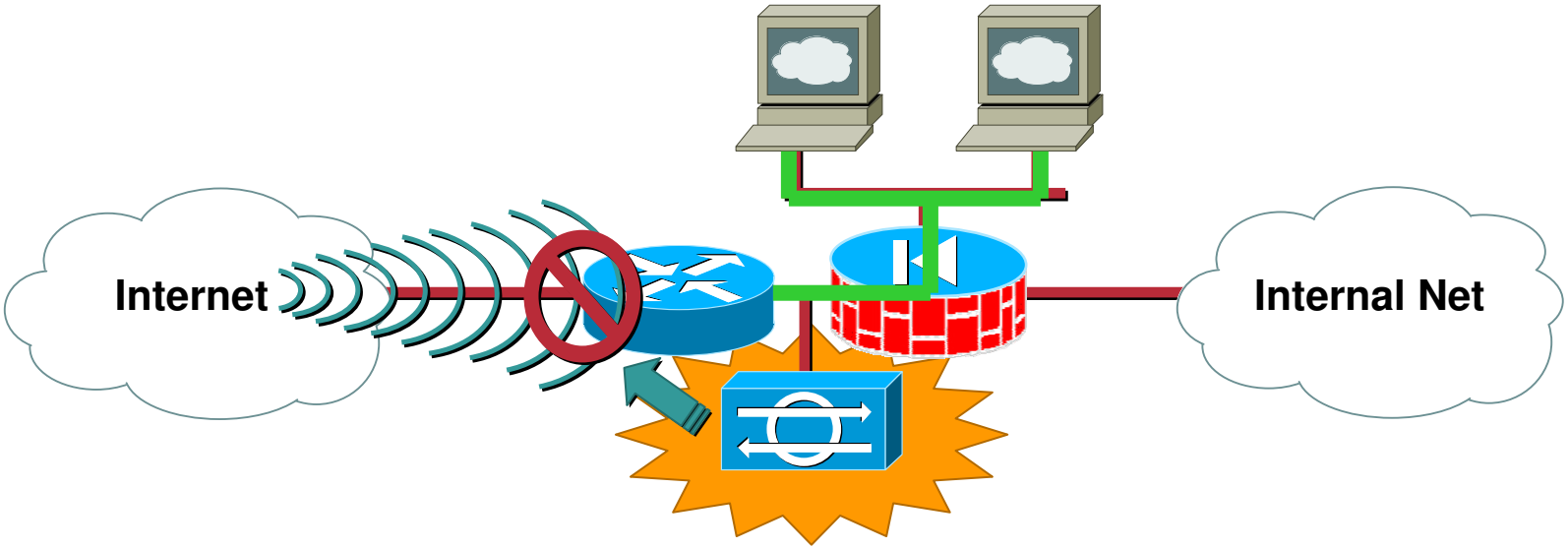


IDS Response Mechanisms

Cisco.com

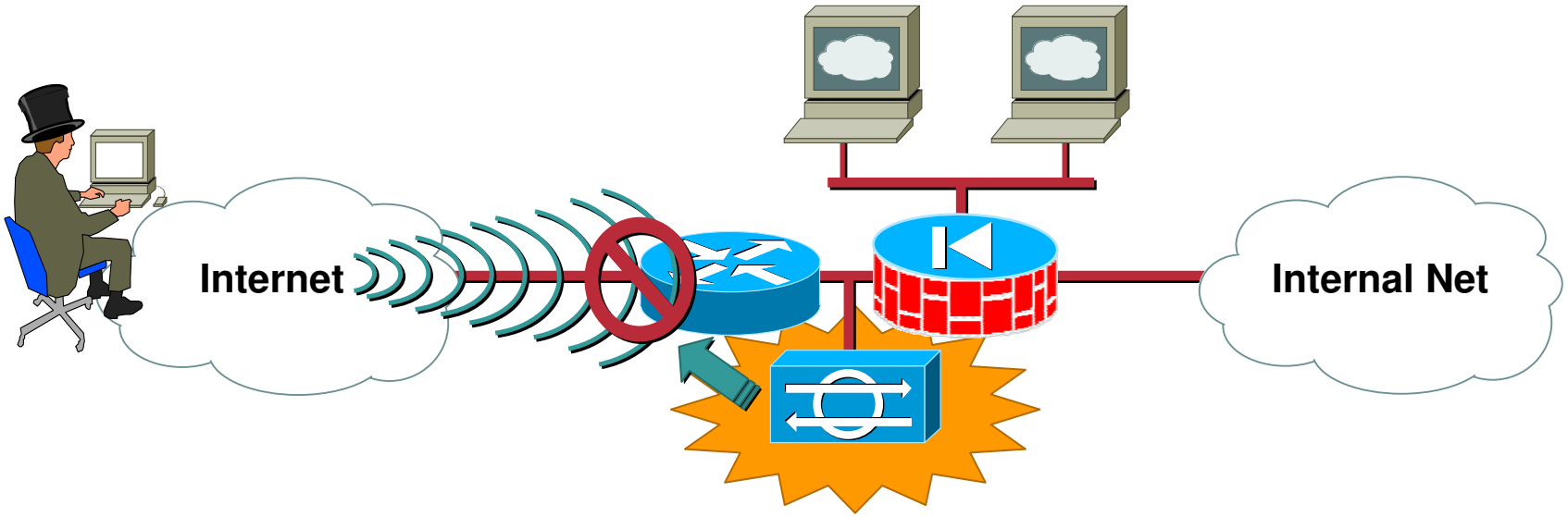
- **IP session logging**
  - **Useful for analyzing events**
  - **Usually only the trigger packet and subsequent packets are logged**
- **TCP resets**
  - **Resets sent from “sniffing” interface**
  - **Trigger packet still goes through**
  - **Must guess correct TCP sequence number**
- **Shunning/blocking**

Shunning Goal



- Identified problematic traffic can be shunned
- Good traffic can pass through

But … The Challenge



- **Placement of IDS device may make it vulnerable to shunning legitimate traffic**
- **Attacks that spoof the source IP address shouldn't be shunned**

IDS Response Actions Caveats

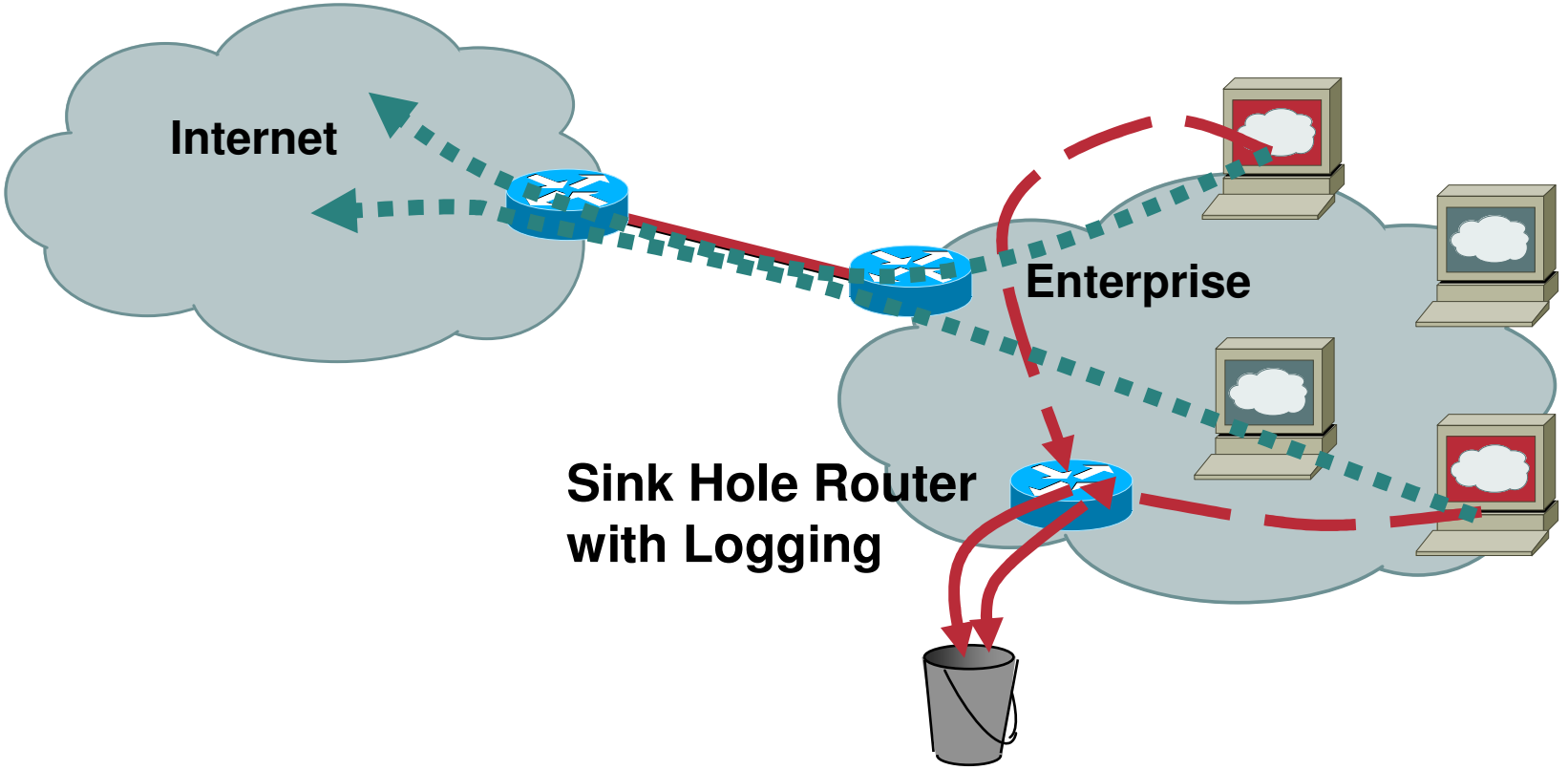
Cisco.com

- **Shunning/blocking**
  - **Use carefully and for limited periods of time to minimize possibility of blocking legitimate traffic**
  - **Use “Addresses to Never Block/Shun” where possible**
    - **routers, DNS servers, DHCP servers, …**

Sink Hole Router

- A designated router is set up to advertise addresses not yet allocated by the Internet Assigned Numbers Authority (IANA)
- This “sink-hole” router advertises these networks locally (only), and any attempts at reaching them are then routed to the router.
- When a worm or other malicious code gets into your network and begins to generate traffic to random addresses, some will be addresses within the unallocated ranges.
- When received, they can be logged and discarded. The results of the logs will provide a list of infected hosts.

Sink Hole Router



Using ACLs To Block Traffic

- **Ingress**

  Proper ACLs will prevent hostile traffic from reaching your network devices and hosts

  Be smart

    deny all tcp port 53 traffic except from your secondary!!

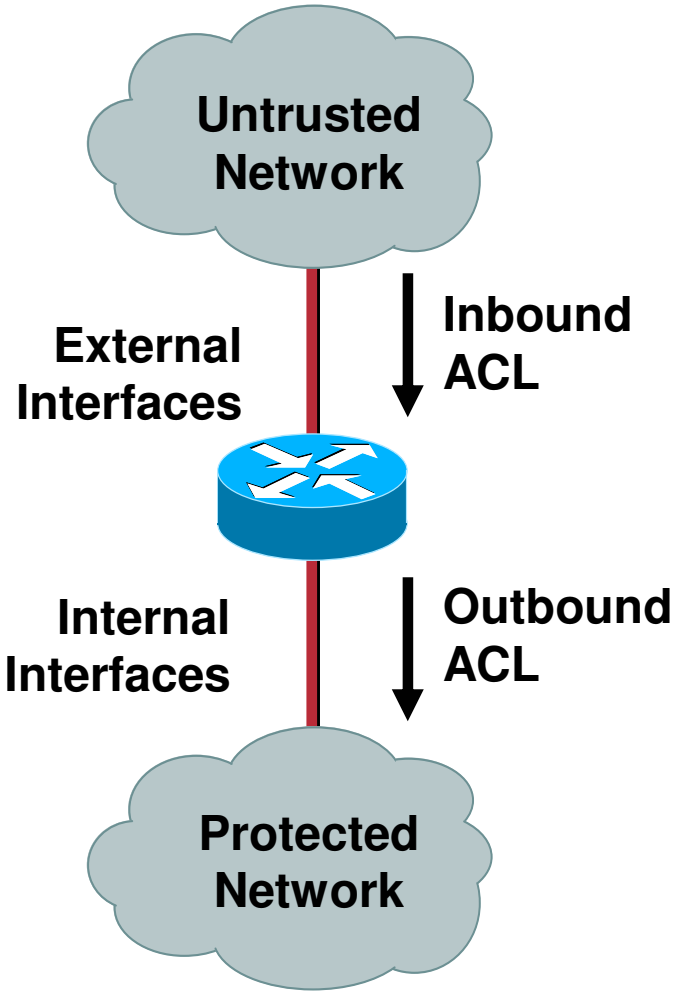
- **Egress**

  Ensure that compromised hosts aren't able to spew hostile traffic back into the Internet

Routers: Where to Apply ACLs

Cisco.com

- You configure interface and direction to apply ACL
- External interface—Apply on inbound direction
  - Denies traffic before it enters the router
- Internal interface—Apply on outbound direction
  - Doesn't protect the router



Tracing Back with ACLs

- **Create ACL:**

```
access-list 101 permit ip any <target> log
```

- **Apply to interface for a few seconds:**

```
interface xxx
ip access-group 101 in
    (wait a few seconds)
no ip access-group 101
```

- **Look at results:**

```
show access-list 101
```

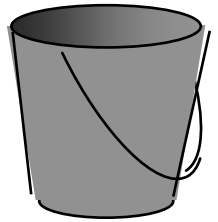
- **If lots of hits: Attack is coming from this i/f**

Using CAR to Rate Limit Attack Traffic

Cisco.com

```
interface Serial 0
   rate-limit output access-group 102 64000 2000 2000
      conform-action transmit exceed-action drop
!
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

- Other ACLs for other attacks: UDP based attacks,…
- Watch your CPU!!!



Deployment Considerations With CAR

Cisco.com

- **Need to understand normal traffic characteristics**
- **May be more effective if deployed by your Internet Service Provider**

Network Based Application Recognition - NBAR

- **Network-Based Application Recognition (NBAR)**
  - **Classify traffic by application protocols**
  - **Allows for custom protocol definition**
  - **Once classified, use QoS to prioritize traffic**
  - **NBAR can be configured to recognize particular strings in the data portion of the packet**
  - **Once recognized, inbound and outbound packets can be dropped before reaching their target**

www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e2/nbar2e.htm

Code Red Example

- The initial infection attempt sends a large HTTP GET request to the target IIS server

  2001-08-04 16:32:23 24.101.17.216 - 10.1.1.75 80 GET /default.ida NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801 %u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403

- Classify inbound "Code Red" hacks with the class-based marking feature

```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*default.ida*"
```

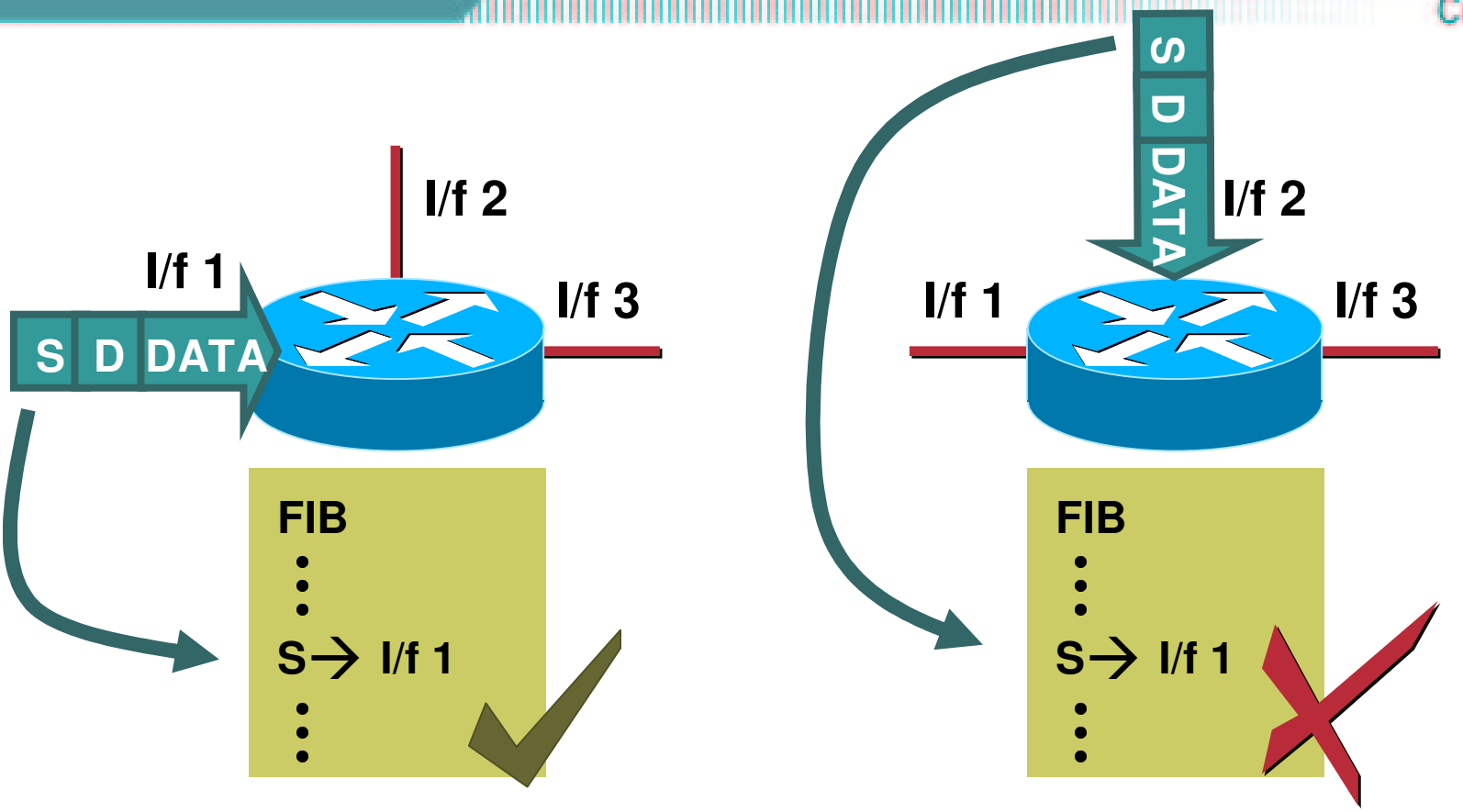
- Once marked, you can use ACLs, Policy Based Routing (PBR), or Class Based Policing to discard the packets

Unicast Reverse Path Forwarding - uRPF

- **Use to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router.**
- **Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.**

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tsr/fothercr/sftrpf.htm#1023632

Strict uRPF



2 CLI commands
router(config-if)# ip verify unicast reverse-path
router(config-if)# ip verify unicast source reachable-via rx allow-default

Unicast RPF Configuration

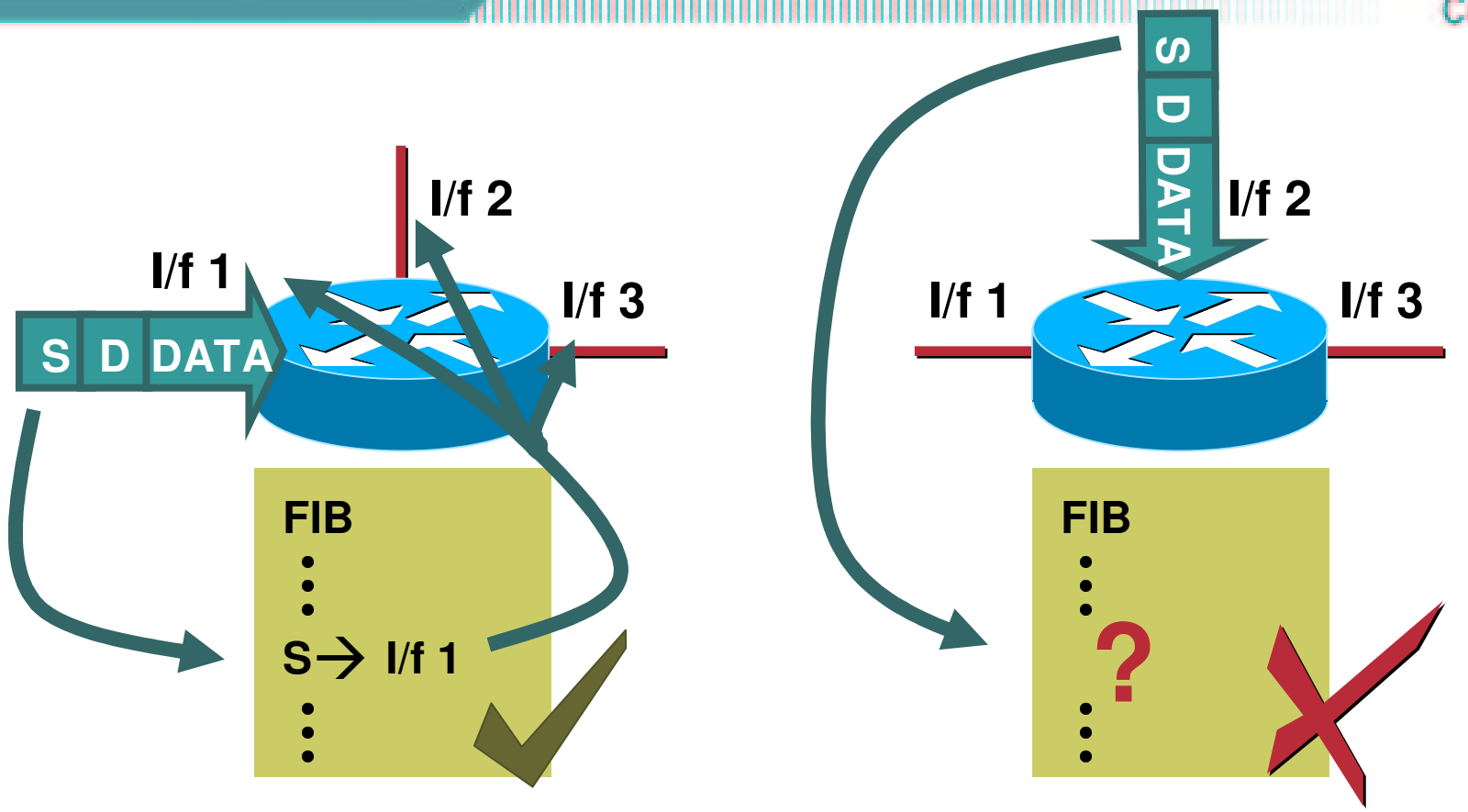
Must Have CEF Enabled

u-RFP config Line

Ingress and Egress Source Address Filters

```
ip cef switch
!
interface Serial 5/0/0
 description Connection to Upstream ISP
 ip address 64.100.2.32 255.255.255.252
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reverse-path
 ip access-group 111 in
 ip access-group 110 out
!
access-list 110 permit ip 64.100.1.0 0.0.0.127  any
access-list 110 deny ip any any log
access-list 111 deny ip host 0.0.0.0 any log
access-list 111 deny ip 127.0.0.0 0.255.255.255 any log
access-list 111 deny ip 10.0.0.0 0.255.255.255 any log
access-list 111 deny ip 172.16.0.0 0.15.255.255 any log
access-list 111 deny ip 192.168.0.0 0.0.255.255 any log
access-list 111 deny ip 64.100.1.0 0.0.0.127 any log
access-list 111 permit ip any any
!
```

Loose uRPF



router(config-if)# ip verify unicast source reachable-via any

Agenda

Cisco.com

- Introduction
- The Nature of Attacks
- Phases of Incident Response
- Tools and Techniques
- Putting It All Together - Case Studies

Case Study - Slammer Worm

Detecting SQL Slammer Infection

- Can't tell on individual hosts
- Inspect network traffic
  - Traffic to UDP port 1434 on random IP addresses indicates infection
- Use IP access-lists or NetFlow
  - Access list:

    access-list 110 permit any any udp eq 1434 log
  - NetFlow:

    sh ip cache flow | include 059A

Detection: Slammer Worm Log

Cisco.com

Jan 25 00:18:11 RouterA-int 71529: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 162.33.125.131(63952) -> 66.92.161.14(137), 1 packet

Jan 25 00:18:20 RouterA-int 71530: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 162.33.125.131(63973) -> 66.92.161.76(137), 1 packet

Jan 25 00:19:26 RouterA-int 71531: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 211.252.55.67(1978) -> 66.92.161.76(1978), 1 packet

Jan 25 00:20:01 RouterA-int 71532: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 61.163.246.150(1978) -> 66.92.161.76(1978), 1 packet

Jan 25 00:21:57 RouterA-int 71533: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 217.167.149.246(1978) -> 66.92.161.76(1978), 1 packet

Jan 25 00:24:52 RouterA-int 71534: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 203.194.148.150(1978) -> 66.92.161.76(1978), 1 packet

Jan 25 00:25:13 RouterA-int 71535: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 202.105.113.190(1978) -> 66.92.161.76(1978), 1 packet

Jan 25 00:26:39 RouterA-int 71536: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 62.85.48.114(4156) -> 66.92.161.76(4156), 1 packet

Detection: Slammer Worm Log (Cont.)

Cisco.com

Jan 25 00:29:36 RouterA-int 71537: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 66.92.160.18(1026) -> 66.92.161.14(137), 1 packet

Jan 25 00:29:46 RouterA-int 71538: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 66.92.160.18(1026) -> 66.92.161.76(137), 1 packet

Jan 25 00:29:56 RouterA-int 71539: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 66.92.160.18(1026) -> 66.92.161.139(137), 1 packet

Jan 25 00:30:58 RouterA-int 71540: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 209.161.7.118(1051) -> 66.92.161.14(1434), 1 packet

Jan 25 00:31:02 RouterA-int 71541: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 216.200.119.92(2848) -> 66.92.161.76(1434), 1 packet

Jan 25 00:31:24 RouterA-int 71542: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 204.68.170.62(3558) -> 66.92.161.139(1434), 1 packet

---hundreds of these entries---

Jan 25 02:45:54 RouterA-int 71923: 4w5d: %SEC-6-IPACCESSLOGP: list 101 denied udp 157.182.151.215(1428) -> 66.92.161.14(1434), 1 packet

ACL 101

Cisco.com

```
access-list 101 deny   ip host 66.92.161.14 any log
access-list 101 deny   ip host 66.92.161.76 any log
access-list 101 deny   ip host 66.92.161.139 any log
access-list 101 deny   ip host 66.92.161.142 any log
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny   ip 192.0.2.0 0.0.0.255 any log
access-list 101 permit tcp any host 66.92.161.14 established
access-list 101 permit tcp any host 66.92.161.76 established
access-list 101 permit tcp any host 66.92.161.139 established
access-list 101 permit tcp any host 66.92.161.142 established
access-list 101 permit icmp any host 66.92.161.14 echo-reply
access-list 101 permit icmp any host 66.92.161.76 echo-reply
access-list 101 permit icmp any host 66.92.161.139 echo-reply
access-list 101 permit icmp any host 66.92.161.142 echo-reply
```

ACL 101 (Cont.)

Cisco.com

```
access-list 101 permit icmp any host 66.92.161.14 ttl-exceeded
access-list 101 permit icmp any host 66.92.161.76 ttl-exceeded
access-list 101 permit icmp any host 66.92.161.139 ttl-exceeded
access-list 101 permit icmp any host 66.92.161.142 ttl-exceeded
access-list 101 permit udp host 64.102.252.11 eq isakmp host 66.92.161.139
access-list 101 permit udp host 64.102.252.11 eq 10000 host 66.92.161.139
access-list 101 permit udp host 171.70.192.81 eq isakmp host 66.92.161.139
                        dp host 171.70.192.81 eq 10000 host 66.92.161.139
                        cp any host 66.92.161.139 eq 22
                        cp any host 66.92.161.139 eq smtp
access-list 1           it udp any host 66.92.161.14 eq domain
access-list 101         it udp any eq domain 66.92.161.0 0.0.0.255
access-list 101 per     it udp any eq ntp 66.92.161.0 0.0.0.255
access-list 101 deny    ip any any log
```

The traffic to port 1434 was denied and logged by this line

Reaction: Access Control

Cisco.com

- Ingress Filtering
  - -Block access to host/services that should not be publicly available
  - -Allow access to public servers – but **patch** them!
  - -Proper ingress filtering will block SQL Slammer attempts at user systems

```
access-list out deny ip any 192.168.254.0 255.255.255.0
access-list out deny ip any 192.168.253.0 255.255.255.0
access-list out permit icmp any any echo-reply
access-list out permit tcp any host 172.16.225.52 eq www
access-list out permit tcp any host 172.16.225.52 eq ftp
access-list out permit tcp any host 172.16.225.50 eq smtp
access-list out permit udp any host 172.16.225.51 eq domains
```

Reaction: Access Control

- **Egress Filtering**
  - **Block outbound access of devices designed for internal use only (ex. Network devices or certain web servers)**
  - **Such devices, if compromised, will be unable to launch DDOS attacks**

```
access-list in deny ip any 192.168.254.0 255.255.255.0
access-list in deny ip any 192.168.253.0 255.255.255.0
access-list in permit icmp any any echo
access-list in permit udp host 10.1.11.50 host 172.16.225.51 eq domain
access-list in permit tcp 10.0.0.0 255.0.0.0 host 172.16.225.52 eq www
access-list in permit tcp host 10.1.11.51 host 172.16.225.50 eq smtp
access-list in permit tcp host 10.1.11.51 host 172.16.225.50 eq 389
access-list in permit tcp 10.0.0.0 255.0.0.0 host 172.16.225.52 eq ftp
access-list in deny ip any 172.16.225.0 255.255.255.0
access-list in permit ip 10.0.0.0 255.0.0.0 any
access-list in permit esp host 10.1.20.57 host 172.16.224.23
access-list in permit esp host 10.1.20.57 host 172.16.224.24
access-list in permit udp host 10.1.20.57 host 172.16.224.23 eq isakmp
access-list in permit udp host 10.1.20.57 host 172.16.224.24 eq isakmp
```

Reaction: Intrusion Detection On The Host

- Use network security scanner to identify systems running SQL Server or that have MSDE installed
- Patch all vulnerable systems
- Install End-Point Intrusion Prevention System (EPIPS)
  - Analyzes SQL server to detect abnormal operations
  - Protects OS against buffer overflow and binary modifications
  - Sends alarm when exploitation is intercepted

* Rebranded as Cisco Secure Agent (CSA)

Reaction: Tune Network Intrusion Detection

- **Network Based Intrusion Detection (NIDS)**

  - Attack detection triggers NIDS to send alarm

  - Shunning not recommended for SQL Slammer since attack is contained in single packet and it was UDP that is simple to spoof

Reaction: Tune Firewalling

- **Filtering to allow only inbound connections to SQL server**
  - **Limit number of inbound connections to server**
  - **Disallow outbound connections from SQL server**
  - **Limits self-propagation of the worm**

Reaction: Network Based Application Recognition

- **Network-Based Application Recognition (NBAR)**
  - **NBAR can be configured to recognize the SQL Slammer worm**
  - **Once recognized, inbound and outbound packets can be dropped before reaching their target**

www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e2/nbar2e.htm

Reaction: Sink-Hole Router

- Set up Sink-Hole Router in addition to NIDS
- Use unallocated addresses which SQL Slammer will exploit
- Sinkhole Router locally advertises these addresses
- SQL Slammer infected servers will seek to contact them
- Log will provide list of locally infected hosts

Incident Example

- Sun PCI cards running windows were biting the dust
- Initial investigation:

  There were extra processes being spawned that were chewing up the CPU on the card

  Looking at traffic dumps, the rogue process (looked like a worm) was scanning the network for other Windows boxes and attempting to logon

  It was using TCP port 445 to do this, and was so active that it was killing the SunPC processes running on Solaris

  Not affecting user workstations or laptops

Incident Example (Cont.)

- **Immediate response:**

  remove affected Sun boxes from the network

- **More analysis**

  Ran some tools, and identified the netspree worm

  Determined what made the Suns different from the laptops: no administrative password YOW!!

  Worm was using default fileshares and trying null and simple passwords. Pretty dumb worm.

  Worm logs into IRC server master.leet-gamer.net on port 6667

- **What to do? AV company wasn't going to have a new DAT file for 24 hours**

Incident Example (Cont.)

- **Problem 1: stop contaminated machines from being remotely controlled**

  Contacted IT admin groups, explained problem, and they re-imaged hosts and made sure they had robust passwords

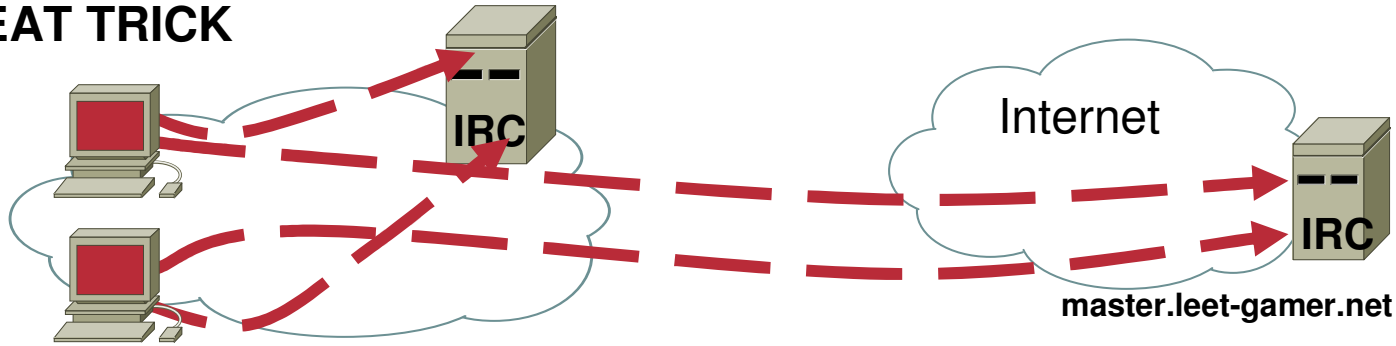
- **Problem 2: find other infected hosts**

  Set up an internal IRC server

  Alter the DNS server so that master.leet-gamer.net pointed to the internal server

  The fake IRC server now has a record of all infected machines

  VERY NEAT TRICK



Summary: Using Technology

- Detect attacks: IDS, Logging, Netflow, ACL, netstat
- Trace back random packet floods: Netflow, ACLs
- Shun a source: IDS, uRPF, ACL, NBAR
- Shun a destination: IDS, ACL
- Limit attacking traffic: CAR
- Update all routers via iBPG - Service Provider

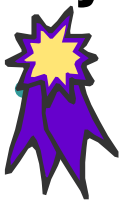
And Remember: You're Not Finished Until …

- A root cause analysis is performed
- A long term fix is implemented
- Completion of fix is confirmed

Summary - Be Prepared!!

Cisco.com

- Know the current attack methods
- Prepare procedures and tools to help you with each phase of response when the attack affects your network



- Learn from experience

1. Triage
2. Analysis
3. Reaction
4. Restore
5. Post-mortem

The Cisco PSIRT Can Help

Cisco.com

- **Product Security Incident Response Team**
- **Handling of *Cisco* product vulnerabilities and customer security incidents**
- **Customers report *security* problems with Cisco products to PSIRT**

  psirt@cisco.com

  www.cisco.com/go/psirt
- **The PSIRT:**

  … assists in finding immediate workarounds
  … works with engineering to fix vulnerabilities
  … escalates within Cisco if necessary
  … helps customer in fixing the problem

Additional Information

Cisco.com

- **Cisco SAFE and "Slammer" Whitepapers:** www. cisco.com/go/safe
- **Cisco Product Security Incident Response Team (PSIRT):** www.cisco.com/go/psirt
- **Cisco Security Information:** www.cisco.com/go/security
- **Cisco NIDS signature database:** www.cisco.com/go/csec
- **Cisco VLAN information:** http://www.cisco.com/warp/public/473/90.shtml
- **Cisco Network Based Application Recognition:** http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e2/nbar2e.htm
- **Microsoft Security:** http://www.microsoft.com/technet/security

Additional Information (Cont.)

- **Honeypots: Tracking Hackers**

  http://www.tracking-hackers.com/

- **"Tracing Spoofed IP Addresses": Rob Thomas, Feb 2001; (good technical description of using netflow to trace back a flow)**

  http://www.enteract.com/~robt/Docs/Articles/tracking-spoofed.html

- **"How to 0wn the Internet in Your Spare Time", Stuart Staniford (Silicon Defense), Vern Paxson (AT&T Center for Internet Research at the International Computer Science Institute), & Nicholas Weaver (UC Berkeley)**

  http://www.nanog.org/mtg-0210/vern.html

Additional Information (Cont.)

- RFC 2827 "Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing" ftp://ftp.isi.edu/in-notes/rfc2827.txt
- Forum of Incident Response and Security Teams (FIRST)

  Federation of over 100 international security incident response teams http://www.first.org
- RFC 2350 "Expectations for Computer Security Incident Response"
- *Handbook for Computer Security Incident Response Teams (CSIRTs)*, Software Engineering Institute, Carnegie Mellon University
  http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf

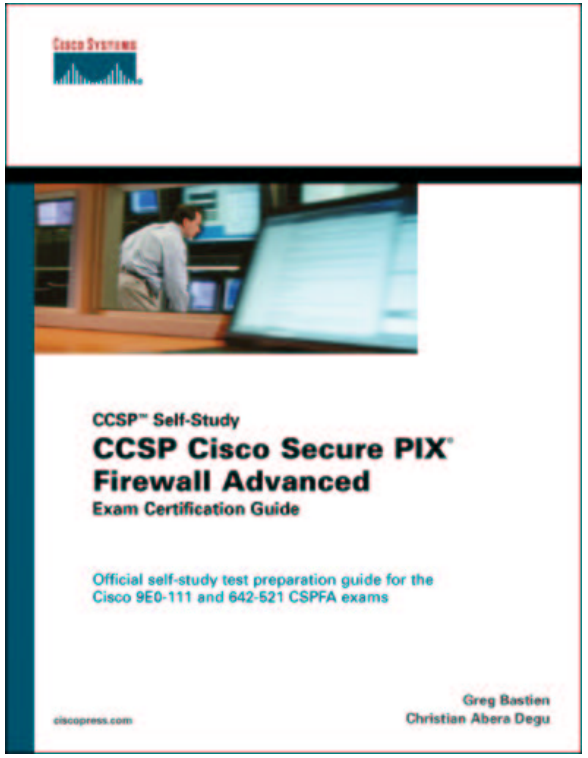
Recommended Reading

Cisco.com

Network Security Principles and Practices
ISBN: 1587050250

CCIE Security Exam Certification Guide
ISBN: 1587200651

CCIE Practical Studies: Security
ISBN: 1587051109



Available on-site at the Cisco Company Store

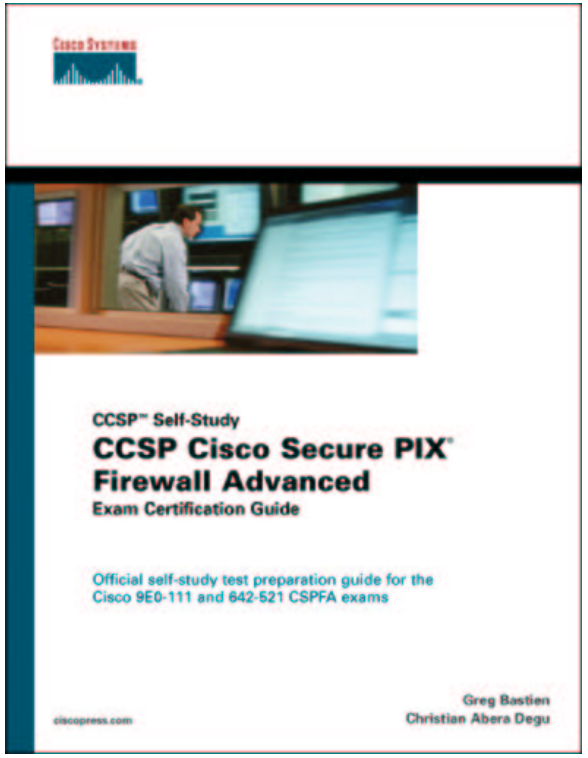
Recommended Reading

Cisco.com

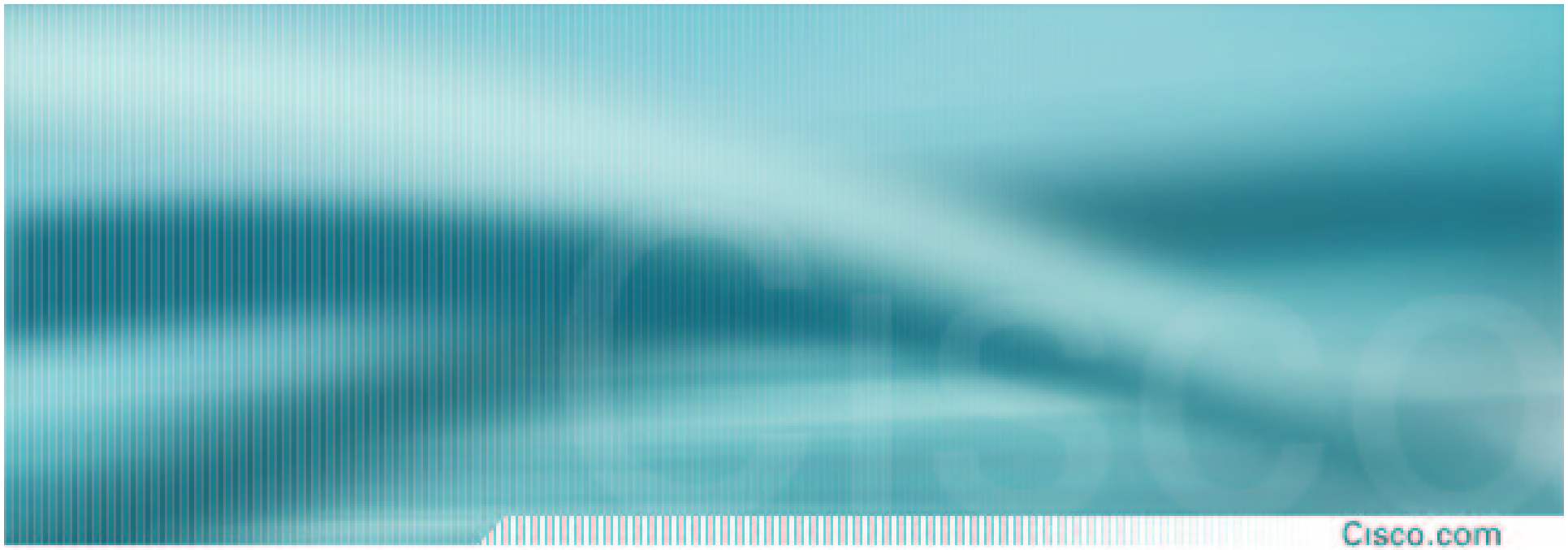
Managing Cisco Network Security
ISBN: 1578701031

Cisco Secure Internet Security Solutions
ISBN: 1587050161

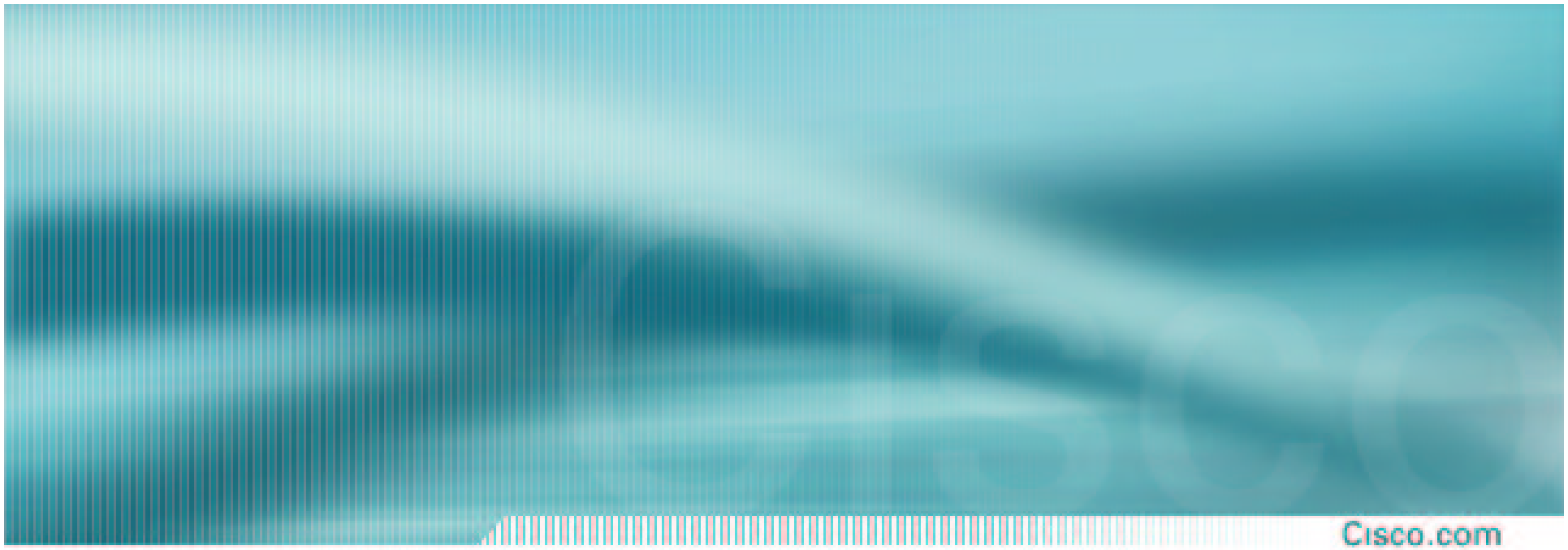
Designing Network Security, Second Ed.
ISBN: 1587051176
Avail in Oct 2003.



Available on-site at the Cisco Company Store



Thank You



Questions

Please Complete Your Evaluation Form