Strategy and Technology to Fight Against Worms and DoS in the Enterprise

Electronic format of this presentation:
http://www.employees.org/~vincent/

Vincent Bieri

Cisco Systems EMEA

Security Technology & Marketing Manager

vbieri@cisco.com

Since the Morris Worm…

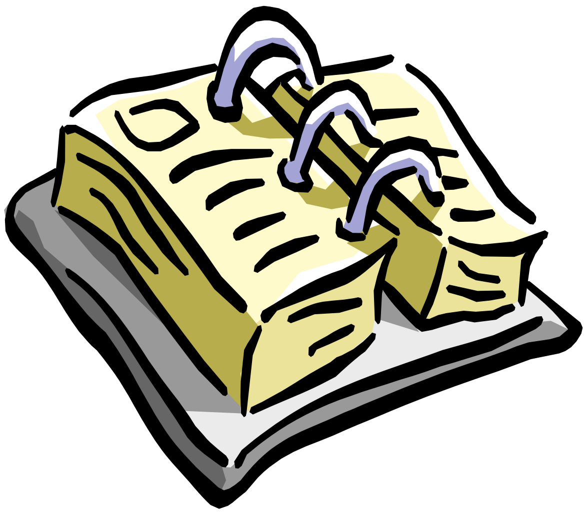
The Number of Security Incidents Continues to Rise Exponentially

The Complexity and Sophistication of Attacks and Vulnerabilities Continues to Rise

The Potential Impact to the Bottom Line Is Significant

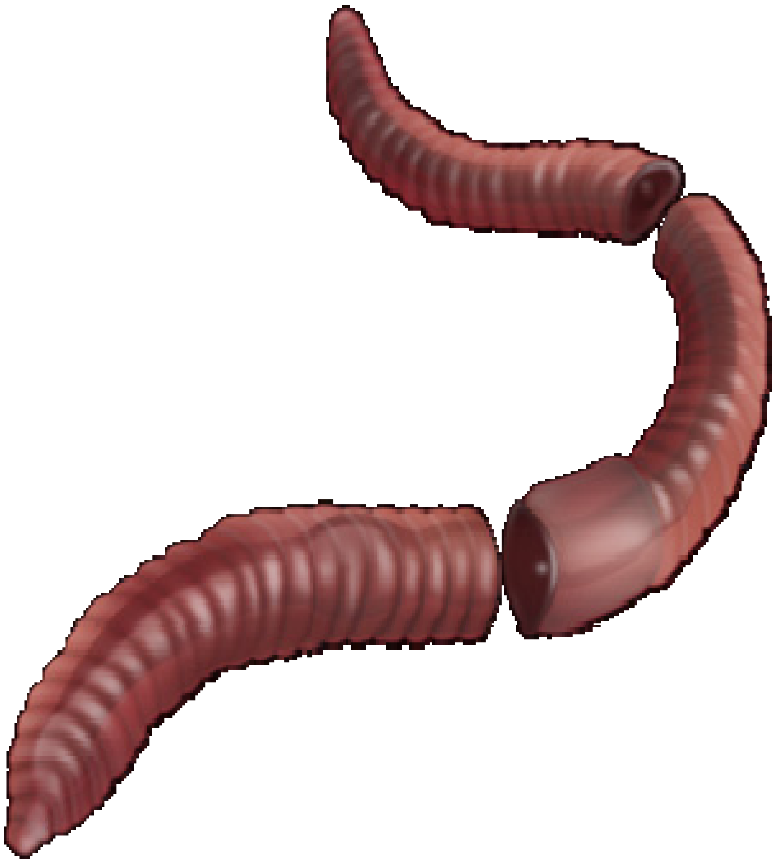
Agenda

Cisco.com



1. **Worms and DoS**
2. **Preparation**
3. **Detection and Classification**
4. **Counter-Measures**
5. **Learning from the Past: Blaster**
6. **Summary and Outlook**

Anatomy of a Worm



1: Enabling Vulnerability

The "entry door" into a system
e.g. web vulnerability

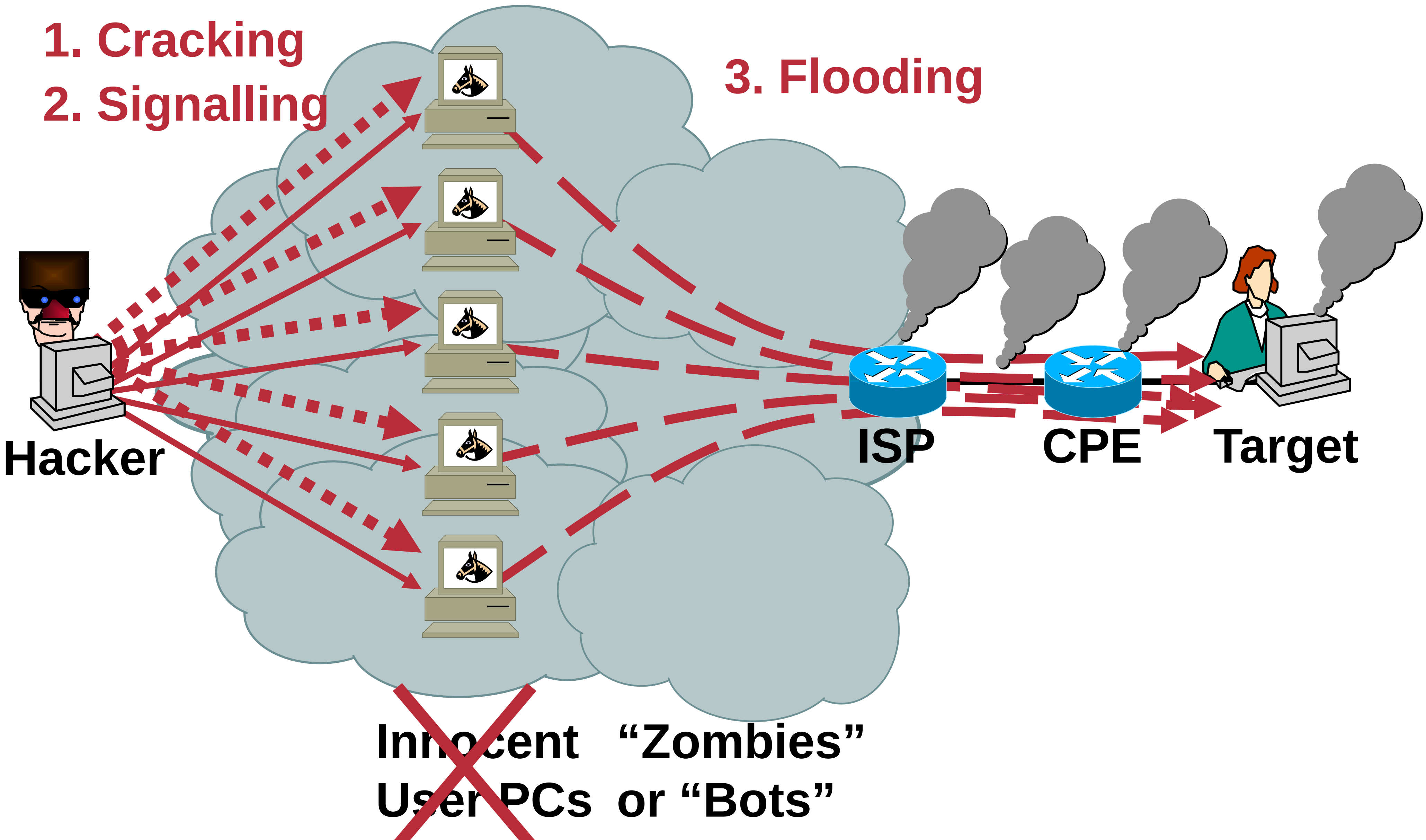
2: Propagation

From there to other systems
e.g. scans on TCP port 80

3: Payload

Bad things the worm could do
e.g. erase disk, attack a site, DoS, etc

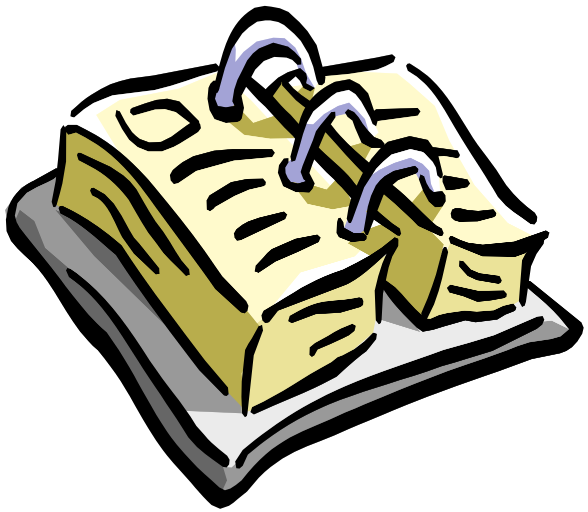
DoS: The Procedure



Difference Between Worms and DoS

	Worm	DoS
Origin of problem	inside/outside	outside only
Traffic	many to many	many to one
Spreads	yes	no
Hacker control	no “live on its own”	yes on/off
Protection	"easier"	harder
Preparation helps	yes!!	yes!!

Agenda



1. Worms and DoS
2. **Preparation**
3. Detection and Classification
4. Counter-Measures
5. Learning from the Past: Blaster
6. Summary and Outlook

Incident Response Methodology for Worms and DoS

Important!!

- **Preparation:** Best Practices / planning
- **Detection:** Something is wrong
- **Classification:** What is wrong
- **Traceback:** Find infection vector | Find ingress path
- **Reaction:** De-worming | Counter measures
  - Contain | - ACLs upstream
  - Quarantine | - Re-direction
  - Inoculate | - SP trace back
- **Post Mortem** Review

time critical

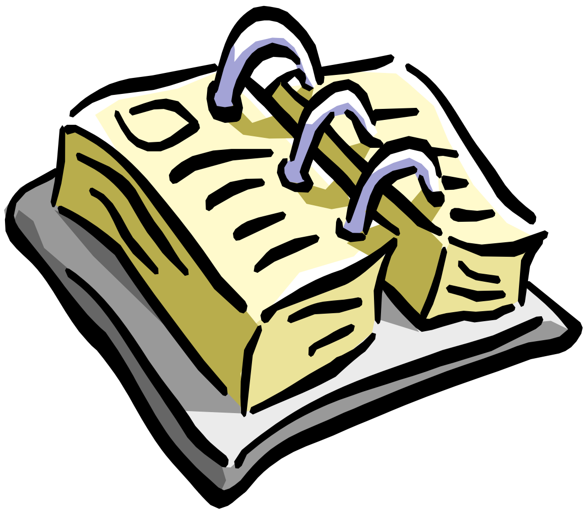
worm specific

common

DoS specific

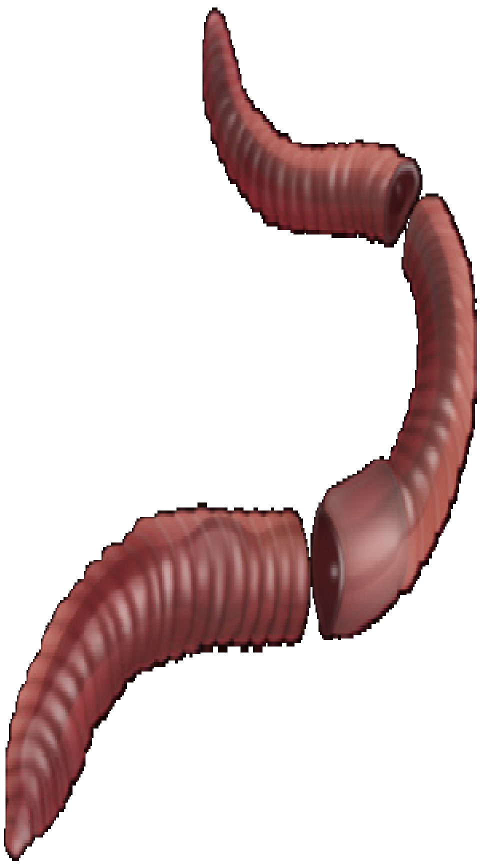
Agenda

Cisco.com



1. Worms and DoS
2. Preparation
3. **Detection and Classification**
4. Counter-Measures
5. Learning from the Past: Blaster
6. Summary and Outlook

Detecting Worms



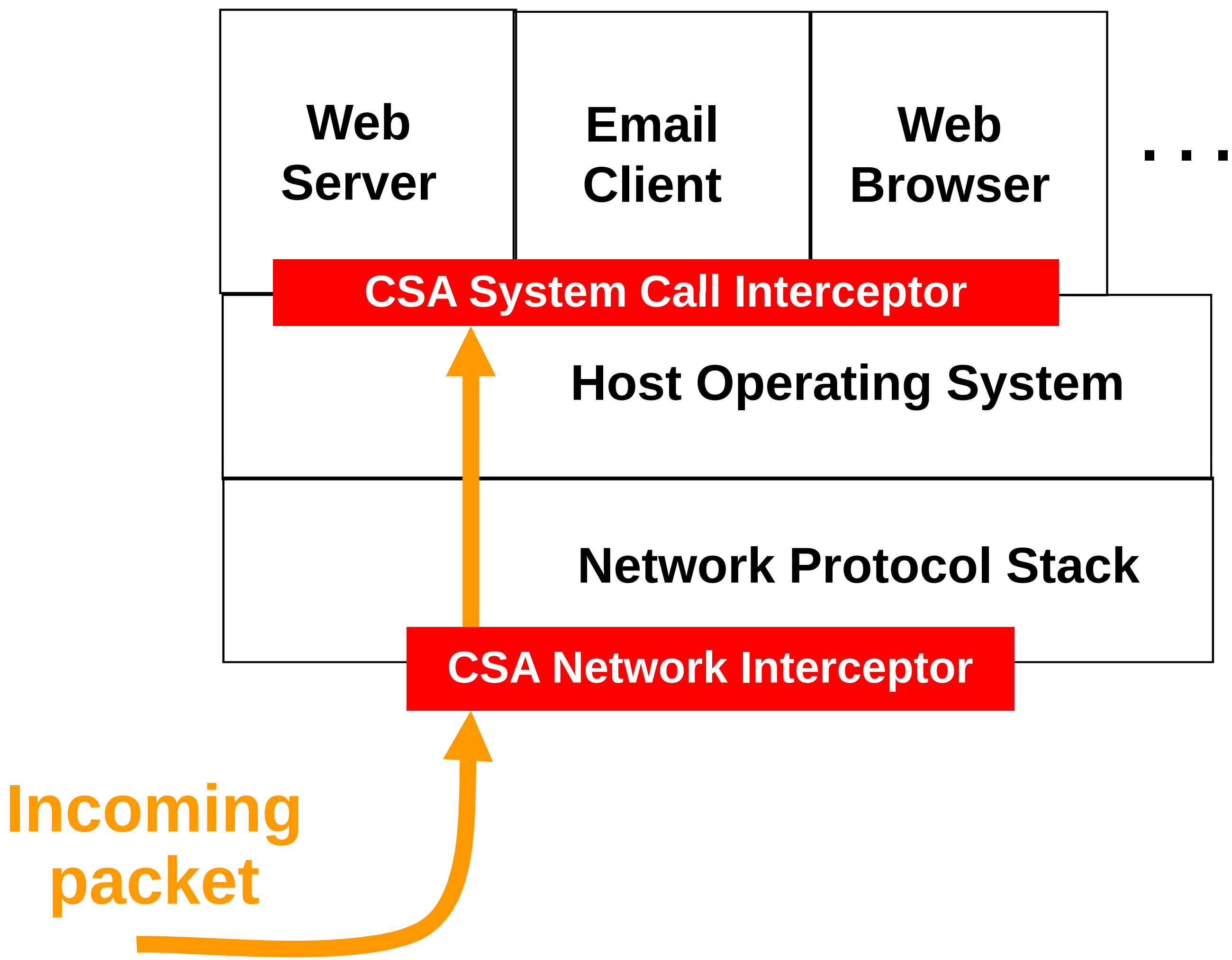
1: Enabling Vulnerability

2: Propagation

3: Payload

- More traffic, unusual traffic (e.g. lots of ICMP)
- Sink hole
- Host IDS/IPS or anti-virus s/w
- Side effects (e.g. network affected)

Host IDS/IPS: Cisco Security Agent Protection Against Illegal System Calls

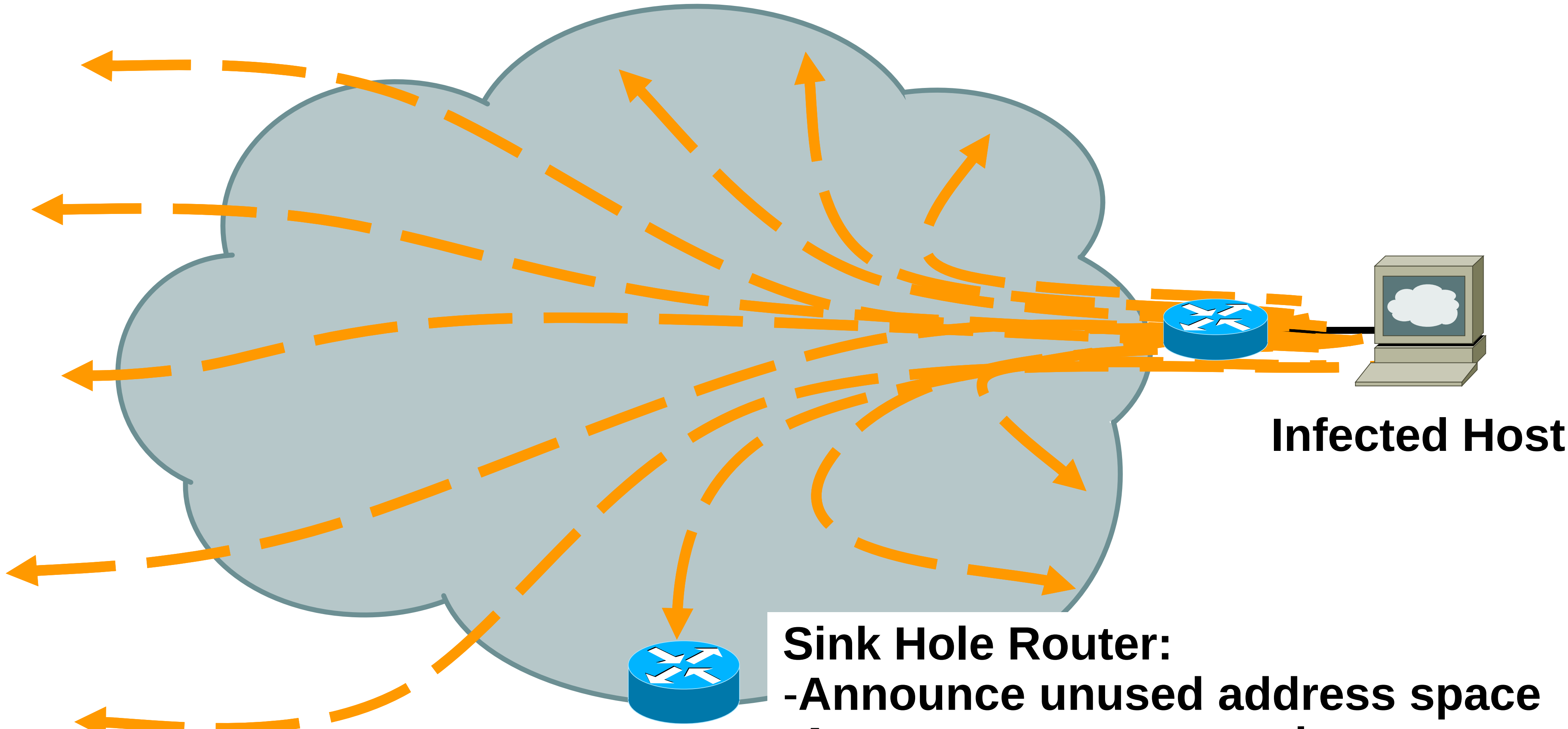


File System Access
Registry Access
COM Object Access
HTTP Access
Memory Access
Code Execution

Inbound packets
Outbound packets

Cisco Security Agent Home Page
www.cisco.com/go/csa

Sink Holes: Worms scan random destinations



Sink Hole Router:

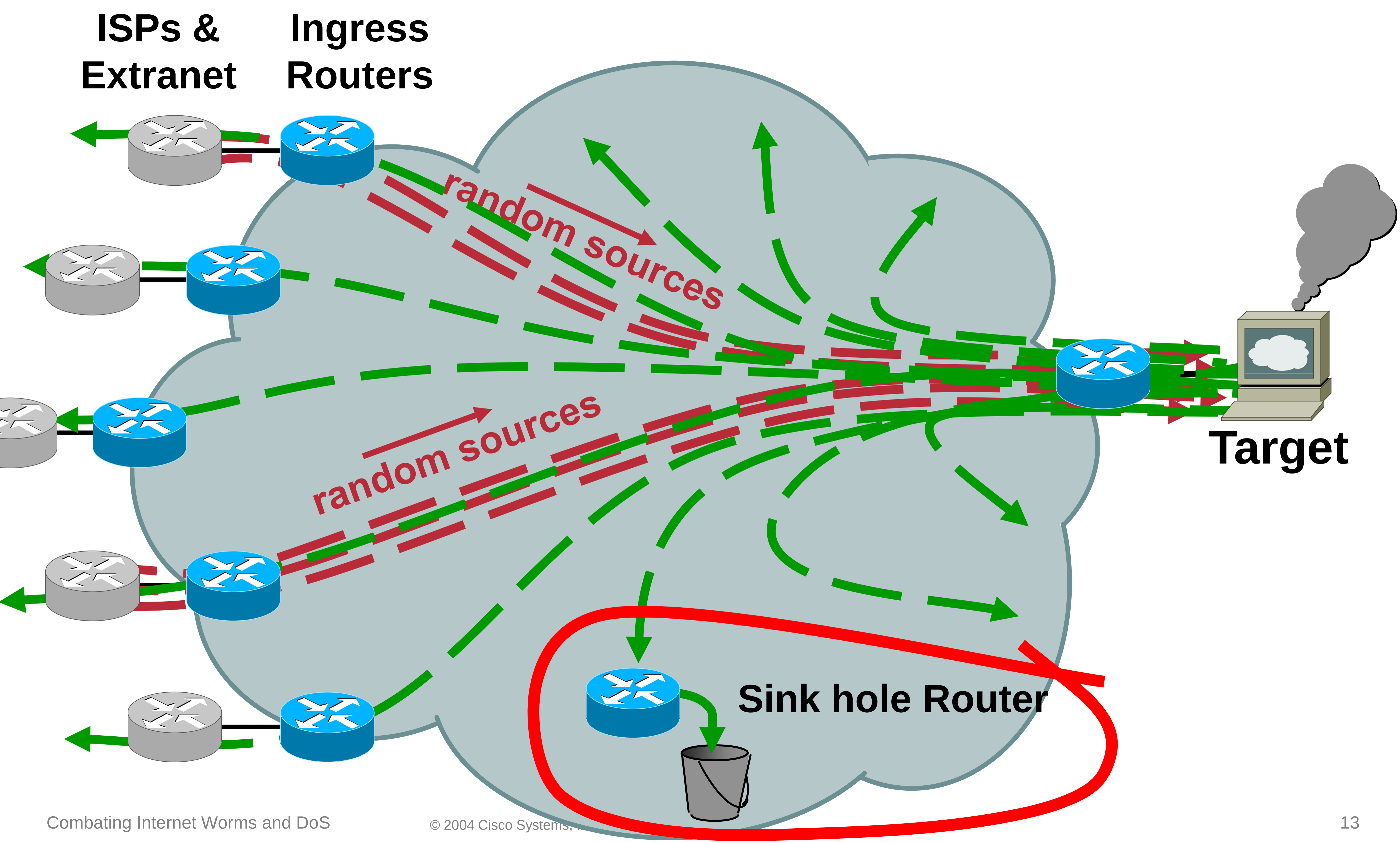
-Announce unused address space

-Attract some scan packets

-Log packets

Sink Holes: Victim replies to random destinations

Cisco.com



Detection and Classification with Netflow

Cisco.com

src_ip	dst_ip	in_if	out_if	s_port	d_port	pkts	bytes	prot	src_as	dst_as
38.209.126.58	xxx.xx.xx.240	22	32	1918	20	1	580	6	0	yyyy
80.88.43.151	xxx.xx.xx.240	22	32	2703	20	1	580	6	0	yyyy
221.12.52.138	xxx.xx.xx.240	22	32	1902	20	1	580	6	0	yyyy
46.150.82.128	xxx.xx.xx.240	22	32	1182	20	1	580	6	0	yyyy
10.11.8.241	xxx.xx.xx.240	22	32	1077	20	1	580	6	0	yyyy
125.82.192.61	xxx.xx.xx.240	22	32	2205	20	1	580	6	0	yyyy
…										

- **Huge number of flows**
- **Unusual flows / headers**
- **Many flows with the same byte count**

Cisco @work: NetFlow Case Study
http://business.cisco.com/prod/tree.taf%3Fasset_id=106882&IT=104252&public_view=true&kbns=1.html

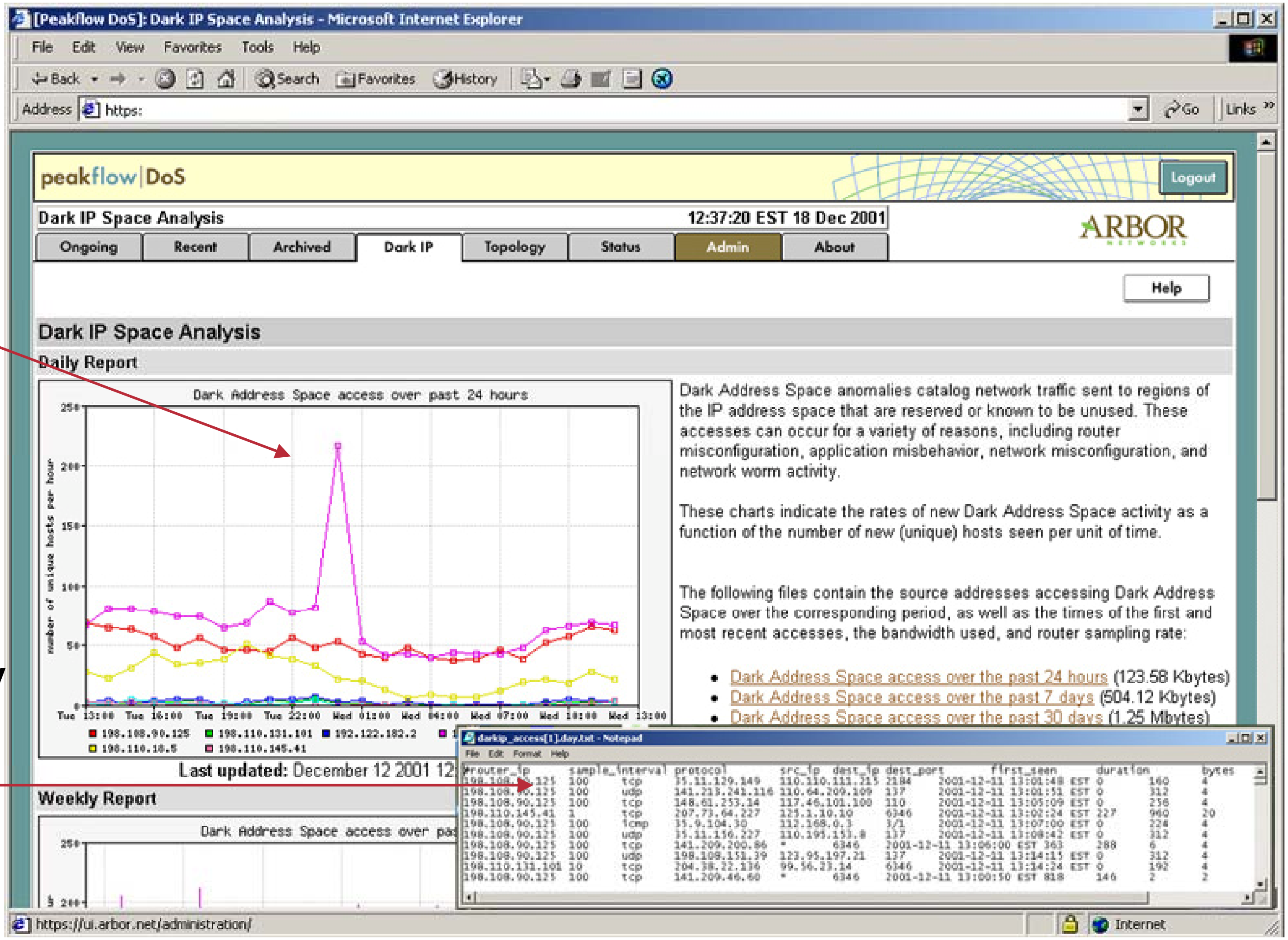
Netflow and Arbor

Cisco.com

Netflow Exports to Arbor's Peekflow

Operator instantly notified of Worm infection.

System automatically generates a list of infected hosts for quarantine and clean-up.



Side Effects:
Don’t miss the forest behind the tree!

Cisco.com

- **Worms can affect the network**
  - **→ High CPU on routers, potential instabilities**
- **Code Red / Nimda scanned port 80**
  - **→ Some web caches had serious performance issues**
- **Slammer also spread to multicast address range**
  - **→Switches and routers created multicast state (lots of…)**
  - **→Some became instable**
- **Many worms cause global routing effects**
  - **→Links at the edge flap → propagation through Internet**
- **Effects on routers running PAT, ARP, …**

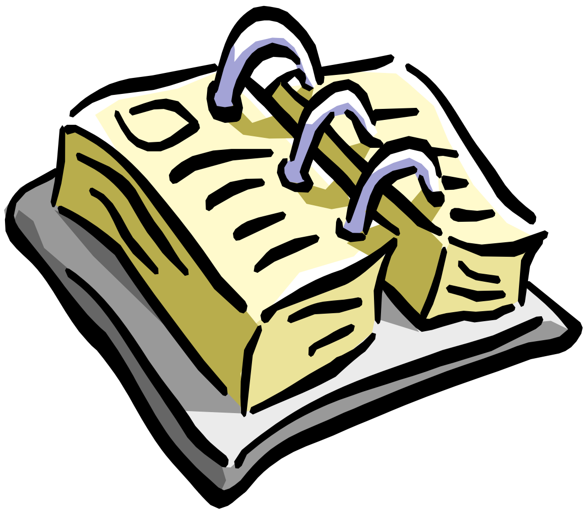
- **Check with the rest of the world! (cert, isc, nanog,…)**

Effects of Worms on Internet Routing Stability

http://www.securityfocus.com/infocus/1702

Agenda

Cisco.com



1. **Worms and DoS**
2. **Preparation**
3. **Detection and Classification**
4. **Counter-Measures**
5. **Learning from the Past: Blaster**
6. **Summary and Outlook**

Worm Mitigation Reaction Methodology

- **Containment** → **ACLs in critical Points in the network**

  contain the spread of the worm

- **Quarantine** → **“infected” VLAN, or limit through ACLs**

  Isolate infected machines

- **Treatment**

  Clean and patch infected systems

- **Inoculation**

  patching systems, vulnerability scans

Follow instructions from Microsoft, anti-virus vendors, Cisco, …

DoS Counter Measures

Cisco.com

- Redirect attack traffic to sink hole
  - May keep rest of network operational
- Apply ACLs to block attack traffic
  - As specific as possible
- Use Rate Limiting where applicable
  - ICMP attacks, some UDP
- Inform upstream service provider
  - Trace back, apply filters there

DoS counter measures: can we improve?

To be improved:

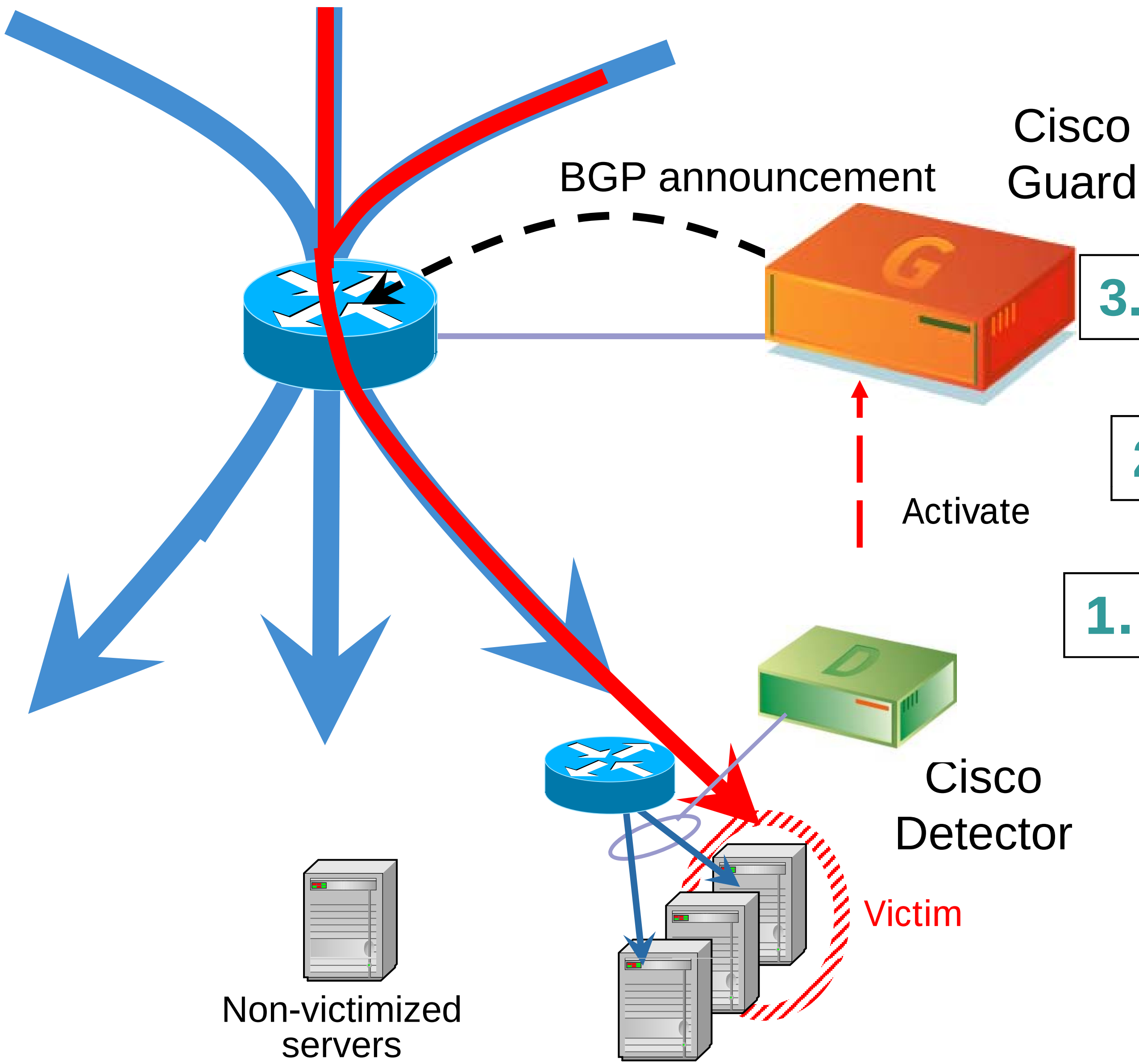
- Full disconnection (server, subnet, network)
- Good traffic dropped
- Router degradation
- Point of failure
- Throughput
- Scalability

Solution must be:

- Up stream
- Not on the critical path
- No point of failure
- Protects all resources
- No router impact
- Scales via sharing
- Dynamic and precise filtering

Cisco Guard Solution Overview (1/2)

Cisco.com

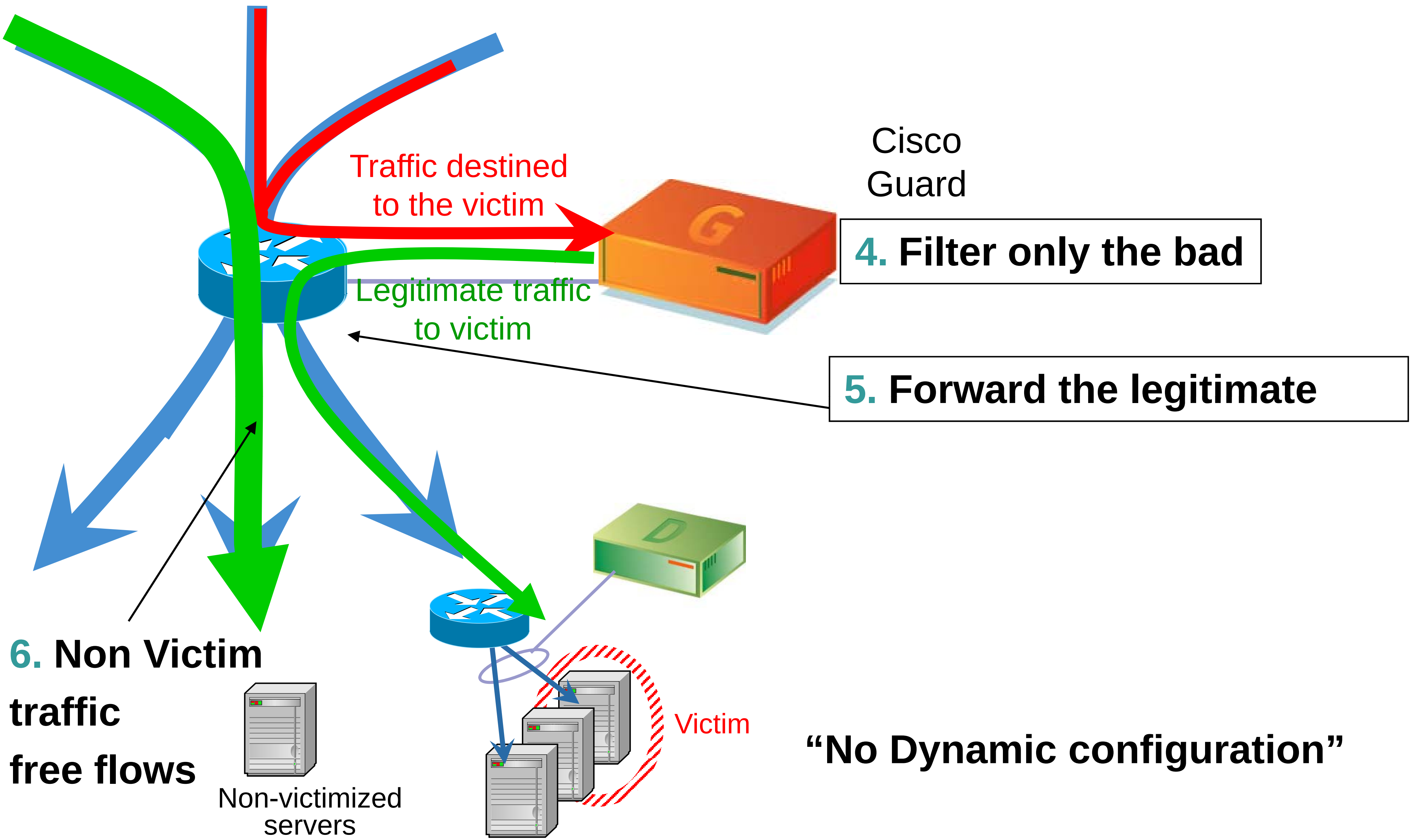


3. Divert only victim's traffic

2. Activate: Auto/Manual

1. Detect

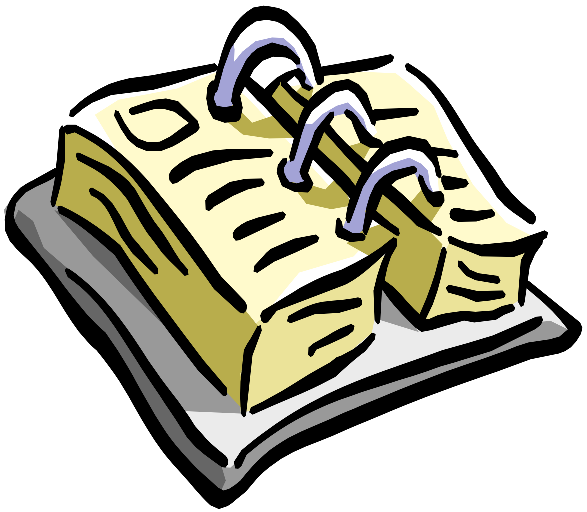
Cisco Guard Solution Overview (2/2)



"No Dynamic configuration"

Agenda

Cisco.com



1. Worms and DoS
2. Preparation
3. Detection and Classification
4. Counter-Measures
5. Learning from the Past: Blaster
6. Summary and Outlook

How Blaster Worked

time

Infector

TCP port 135 → random dst
- 80% of packets for XP
- 20% for Win2k

-Start TFTP server on UDP 69

Send cmd to TCP 4444:
-“download MSBlast.exe”

-“execute MSBlast.exe”

Victim

if system unpatched, and
if right OS (XP/Win2k)
then: open remote command shell on port TCP 4444

“GET” via TFTP the file

MSBlast.exe installs itself permanently, becomes infector

16 Aug, 00:00

SYN-attack against windowsupdate.com

SYN-attack against windowsupdate.com

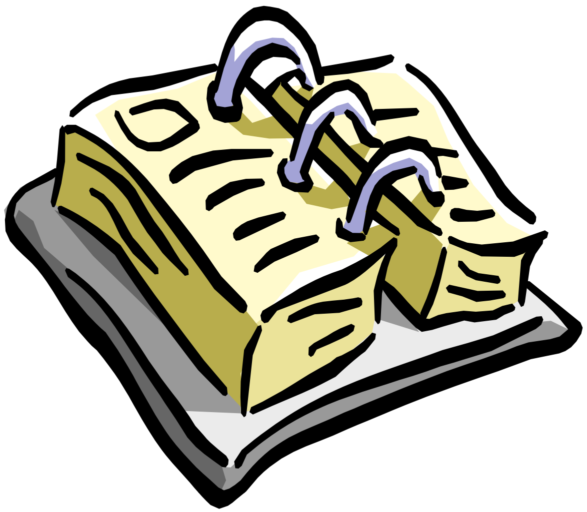
What We Learned From Blaster

- **NANOG mailing list discussed very early**
  - →Check with "rest-of-world"
  - →Lots of smart people out there! Listen!
- **Needs ports 135, 4444, 69 to propagate**
  - →Block unused / insecure ports. Everywhere!
  - →Also outbound!!!
- **Many potential entry points were overlooked!**

  Main firewall okay, but external laptop coming into enterprise, VPN connections, …
- **Cisco Security Agent (CSA) blocked the worm!**

  Behaviour based, not signature based!
- **Lots of features helped: Private VLANs, NBAR, …**
- **Netflow/Arbor's solution flagged Blaster within seconds!**

Worms and DoS in an Enterprise
Agenda



1. Worms and DoS
2. Preparation
3. Detection and Classification
4. Counter-Measures
5. Learning from the Past: Blaster
6. Summary and Outlook

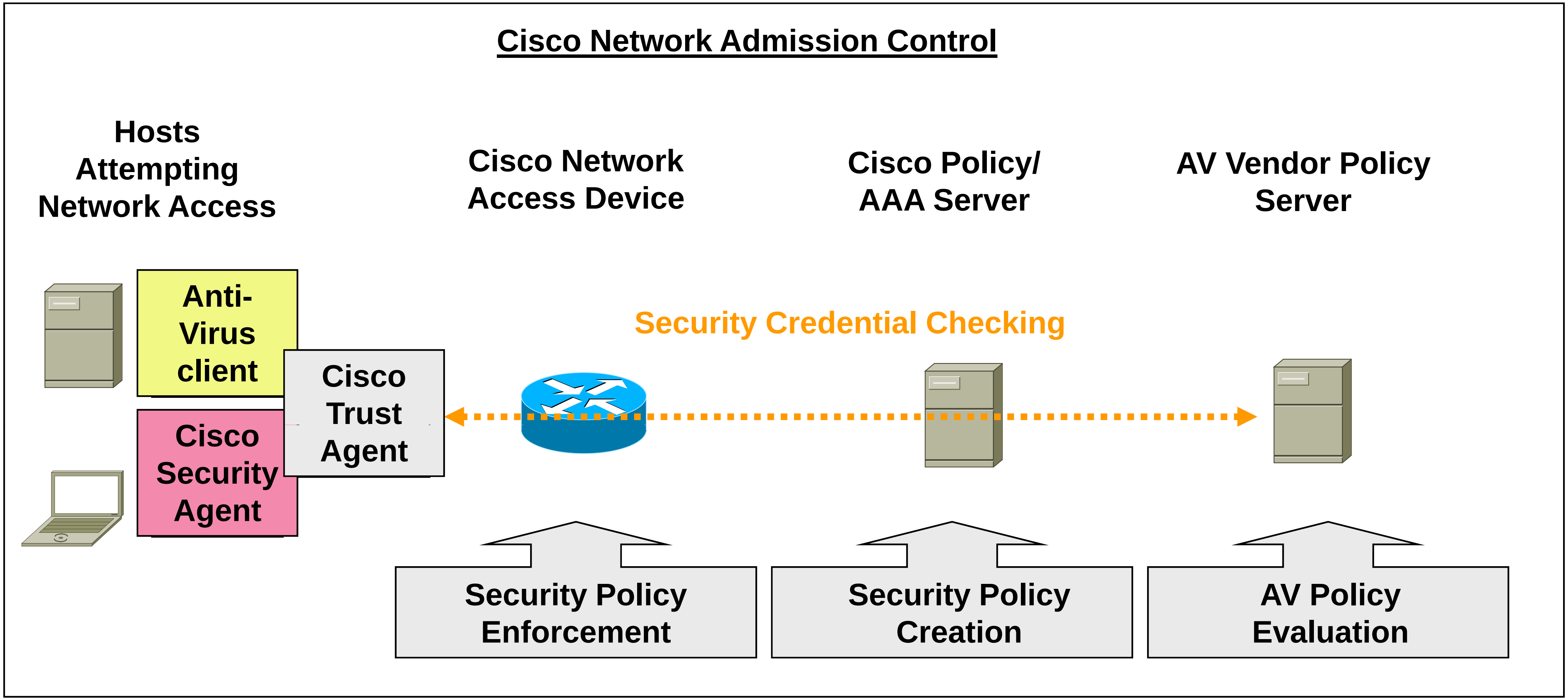
Summary

- Key to fighting Worms and DoS: Being prepared!
  - Know your network, practise “incidents”!
- Your Network is extremely powerful!
  - *Lots* of tools and techniques available
  - Are you prepared to use them?
- Very useful products and technology available
  - Netflow / Arbor
  - "Anti-DoS" (Cisco Guard)
  - Host Intrusion Prevention (CSA)
  - Network IDS/IPS
  - CAR / NBAR
  - uRPF
  - …

Worm and Virus Defence Outlook

Cisco Network Admission Control (NAC)

Cisco.com



- Based on endpoint security posture, appropriate admission policy will be enforced in the network
- Cisco & NAC co-sponsors to deliver this collaborative solution

References

- **Thread Defense System**

  www.cisco.com/go/tds

- **Self-defending Network and Network Admission Control**

  www.cisco.com/go/selfdefend

- **Safe: Best security practices, Blaster white paper**

  http://www.cisco.com/go/SAFE

- **Securing Cisco Routers:**

  http://www.cisco.com/warp/public/707/21.html

- **ISP Essentials:**

  ftp://ftp-eng.cisco.com/cons/isp/security/

- **PSIRT: Cisco's Product Security Team**

  http://www.cisco.com/go/psirt/

- **Cisco IT @Work Netflow Case Study**

  http://business.cisco.com/prod/tree.taf%3Fasset_id=106882&IT=104252&public_view=true&kbns=1.html

Strategy and Technology to Fight Against Worms and DoS in the Enterprise

Electronic format of this presentation:
http://www.employees.org/~vincent/

Vincent Bieri

Cisco Systems EMEA

Security Technology & Marketing Manager

vbieri@cisco.com

CISCO SYSTEMS

EMPOWERING THE
INTERNET GENERATION℠