

Multi-Layer Defense: Protection Against Worms & Viruses

WAVV 2004, 3 pm EST Session - U2
May 3, 2004

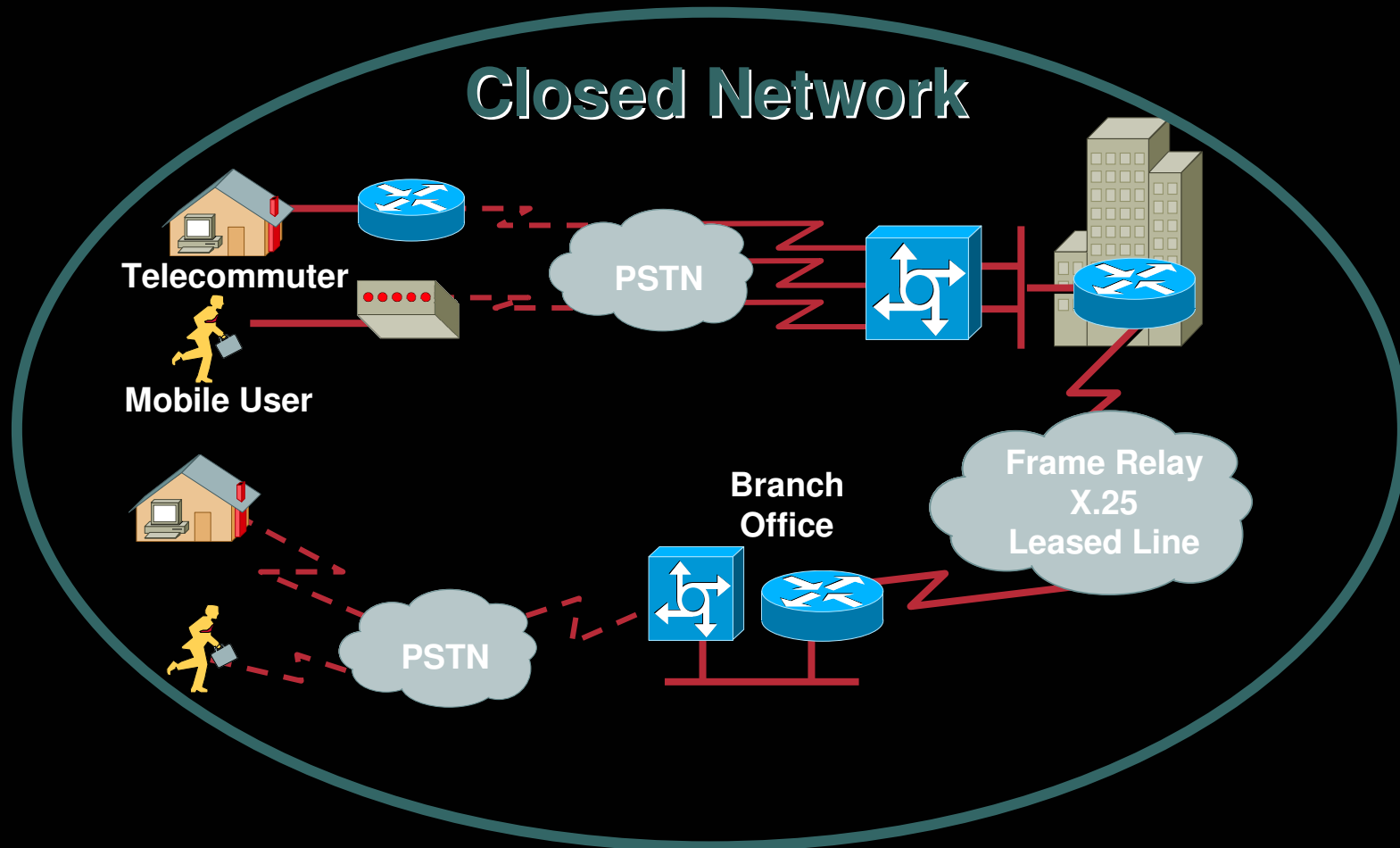
Rich Taylor, CISSP
Security Market Specialist
Cisco Systems, Inc.
richtayl@cisco.com

(678) 352-2600

The World Has Changed...

Networks Of The 90's

Cisco.com



Most security devices were designed to secure networks like this

Networks of Today

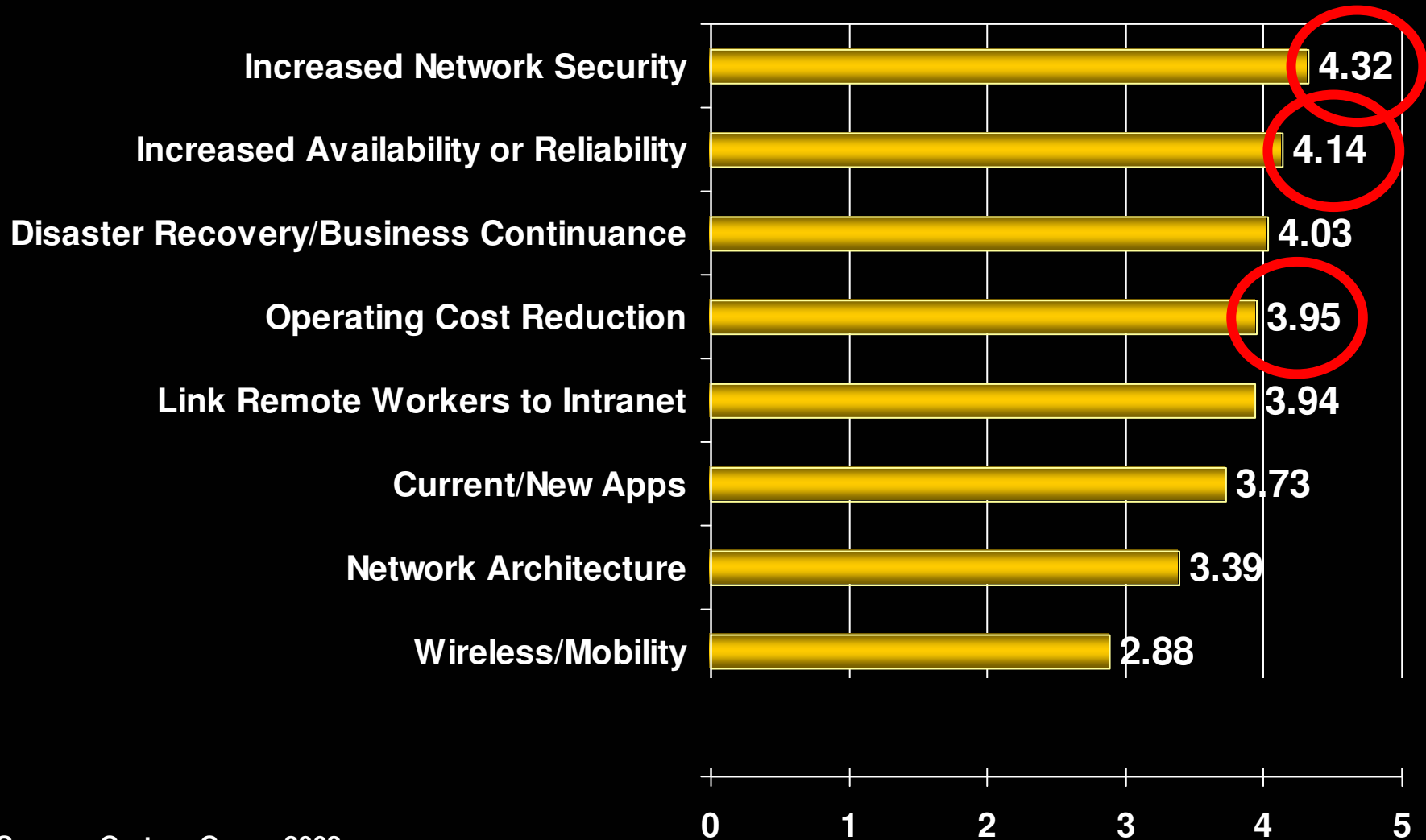
Cisco.com



Security Challenges

Networking Priorities in 2003

Cisco.com



Source: Gartner Group 2002

956183-03
4043_01_2002_c5

© 2002, Cisco Systems, Inc. All rights reserved.

1 = Not Important; 5 = Very Important

Security Challenge for Enterprises

Cisco.com

- **Security is no longer a 'network only' proposition**
 - Data must also be protected where it resides....the endpoint (server/desktop)
- **Day Zero attacks**
 - Rapidly propagating attacks (Slammer and Nimda) evade signature recognition to attack and proliferate through servers and desktops
- **Server and desktop maintenance**
 - Increasing # of vulnerabilities makes the task of patching systems an 'update race' without end
 - Security maintenance in enterprises must scale to hundreds of thousands of endpoints
- **Legacy endpoint security TCO challenge**
 - Inherently reactive products provide point solutions for endpoints forces deployment of multiple agents and management paradigms

Cisco Security Strategy Evolution

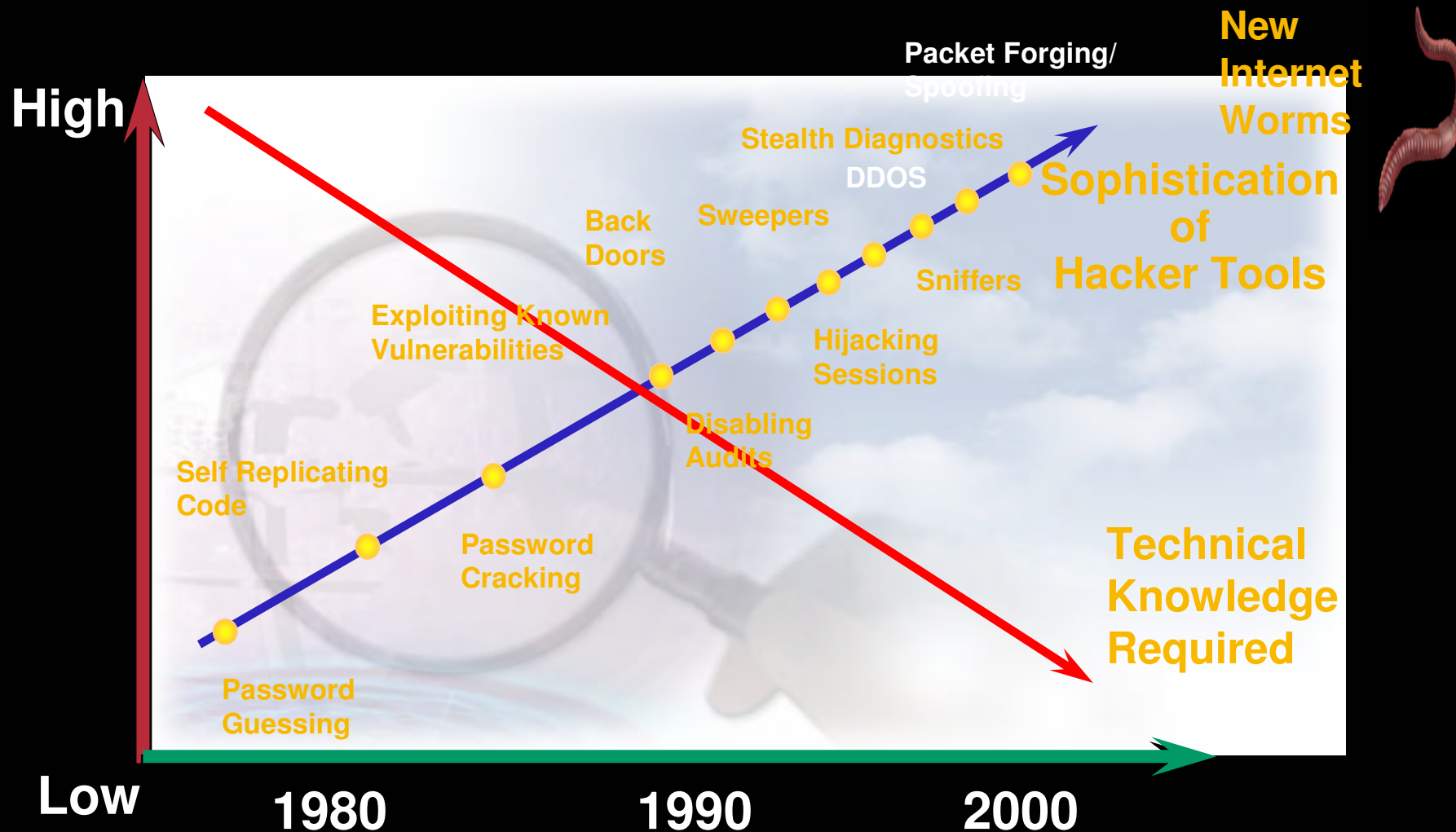
Cisco.com

Severity of
Security Threats



Threat Capabilities

Cisco.com



The Sapphire Worm or “Slammer”

Cisco.com

- Infections doubled every 8.5 seconds
- Infected 75,000 hosts in first 11 minutes
- Caused network outages, cancelled airline flights and ATM failures

Minutes after Release

At Peak,
Scanned 55 Million Hosts per Second



11

8

6

2

0

Let's Look at Blaster

The Blaster Worm: What Happened??

Cisco.com



- **Monday August 12, 2003
Worm Released**
- **Also known as W32.Blaster,
MSBlast and W32/Lovsan**
- **Exploited flaw in Microsoft RPC
code**
- **Spread worldwide within hours**
- **CERT estimates over 1.4 million
devices infected**
- **Could end up being most widest
attack on Internet to date**
- **Speed of infection is slower than
Slammer worm of 1/03**

Effects Of The Blaster Worm

Cisco.com

- **Crashes infected devices**
- **Root control of device could be gained by attacker**
- **Replication action floods networks**
- **Significant system outages reported worldwide including Federal Reserve Bank of Atlanta, Maryland Department Of Motor Vehicles, City of Philadelphia, US Postal Service and others.**

The Blaster Worm: How It Works

Cisco.com



Exploits vulnerability in Microsoft RPC code dealing with message exchange over TCP/IP resulting in the incorrect handling of malformed messages

Flaw is stack-based buffer overflow occurring in low-level Distributed Component Object Model (DCOM) interface within the RPC process listening on TCP/IP port 135

Affected systems: Microsoft Windows NT 4.0, Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Server 2003

Vulnerability published in July 2003. Patch was made available from Microsoft at that time.

Worm executes code and installs a copy of itself into the infected computer's memory – which infects other hosts.

Anatomy Of A Worm

Cisco.com

**1—The Enabling
Vulnerability**

**2—Propagation
Mechanism**

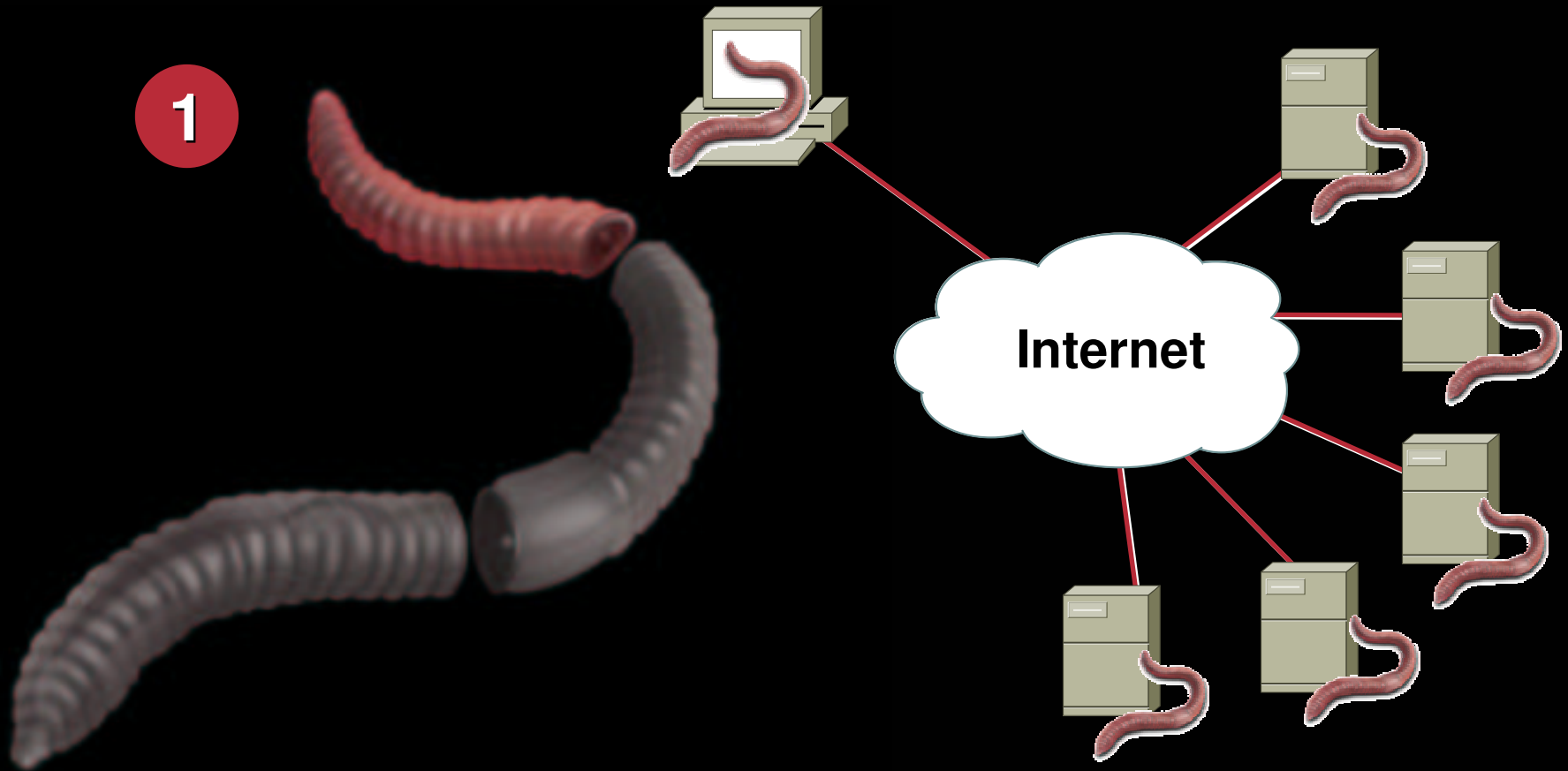
3—Payload



The Enabling Vulnerability

Cisco.com

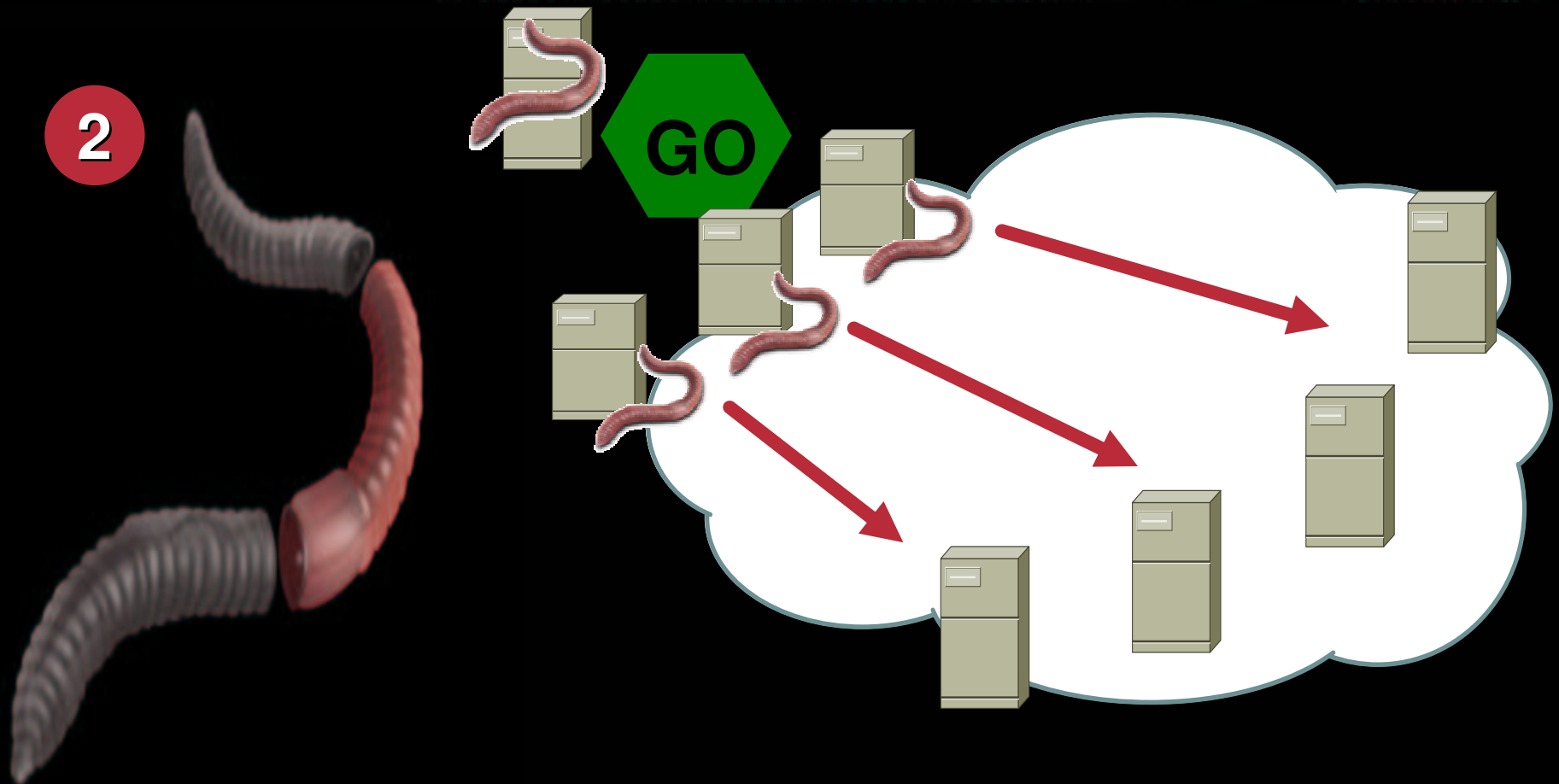
1



Using the RPC Flaw, worm installs itself on Windows devices.

Propagation

Cisco.com

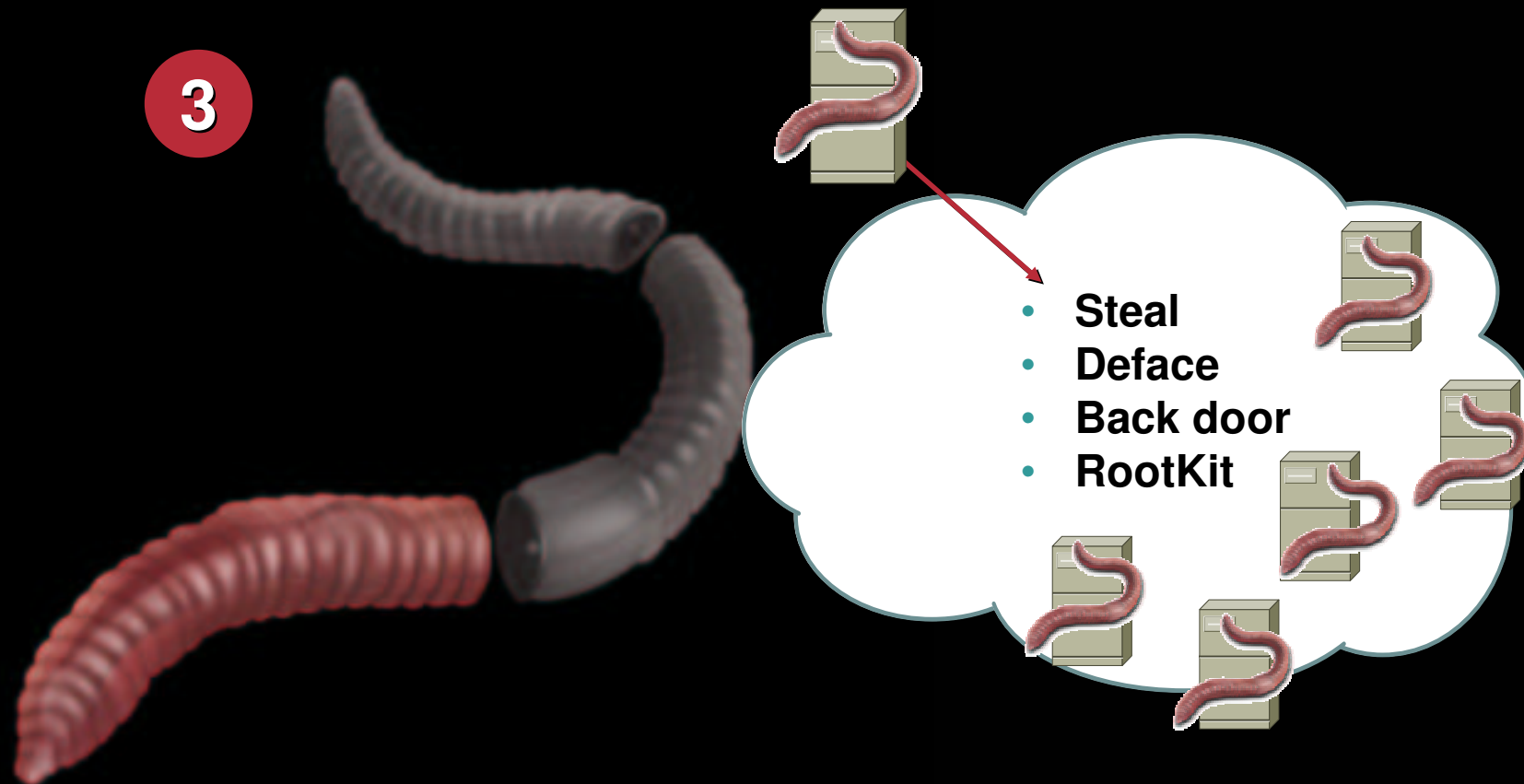


**After gaining access to devices,
worm replicates itself and selects new targets.**

Payload

Cisco.com

3



When the device is infected with a worm, the attacker has access to the host as the SYSTEM user. Attacker could use a local exploit to escalate their privilege level to Administrator

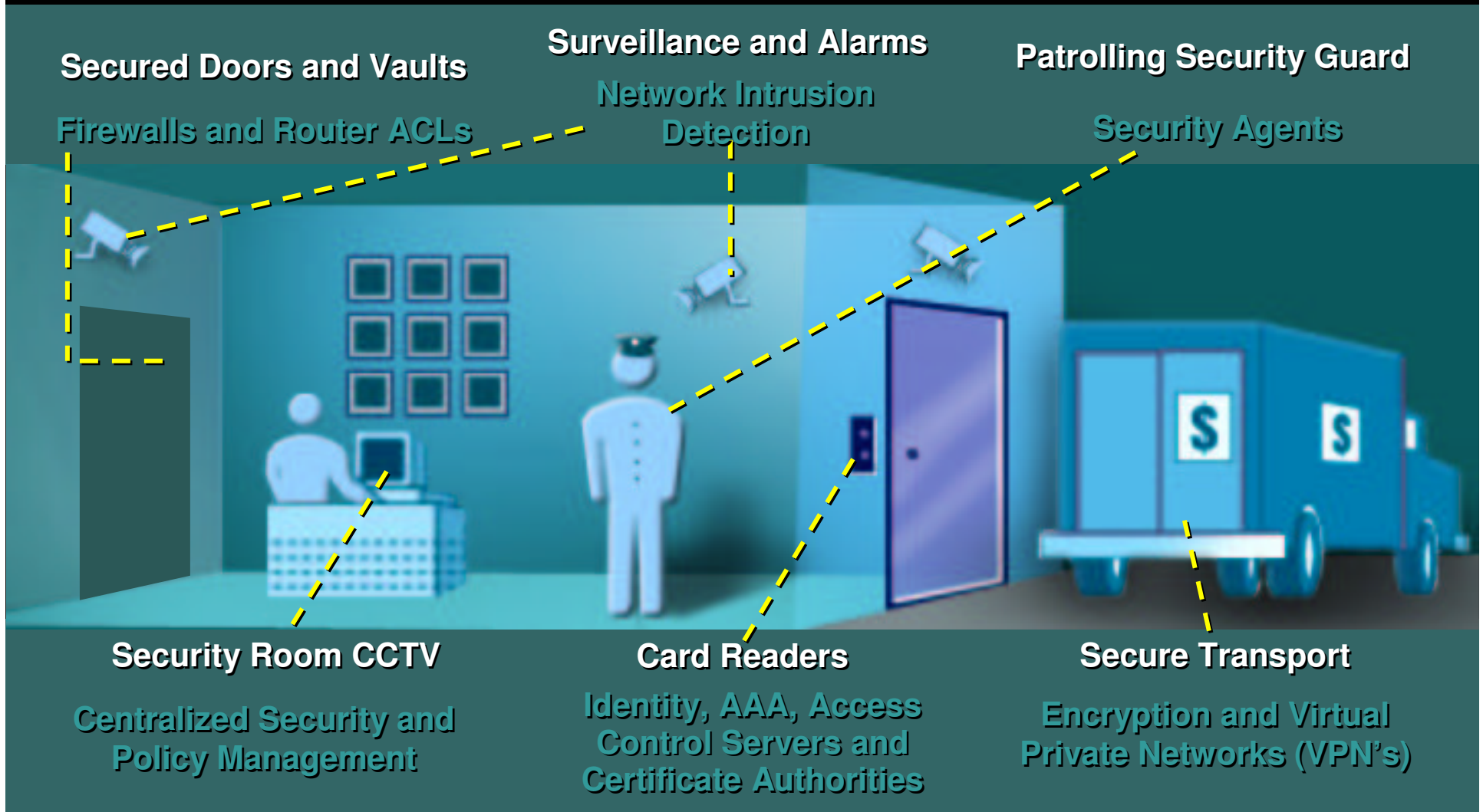
So, What Can You Do?

Implement a Defense in Depth Strategy

www.cisco.com/go/safe
www.cisco.com/go/selfdefend

Integrated Security System Is An Imperative

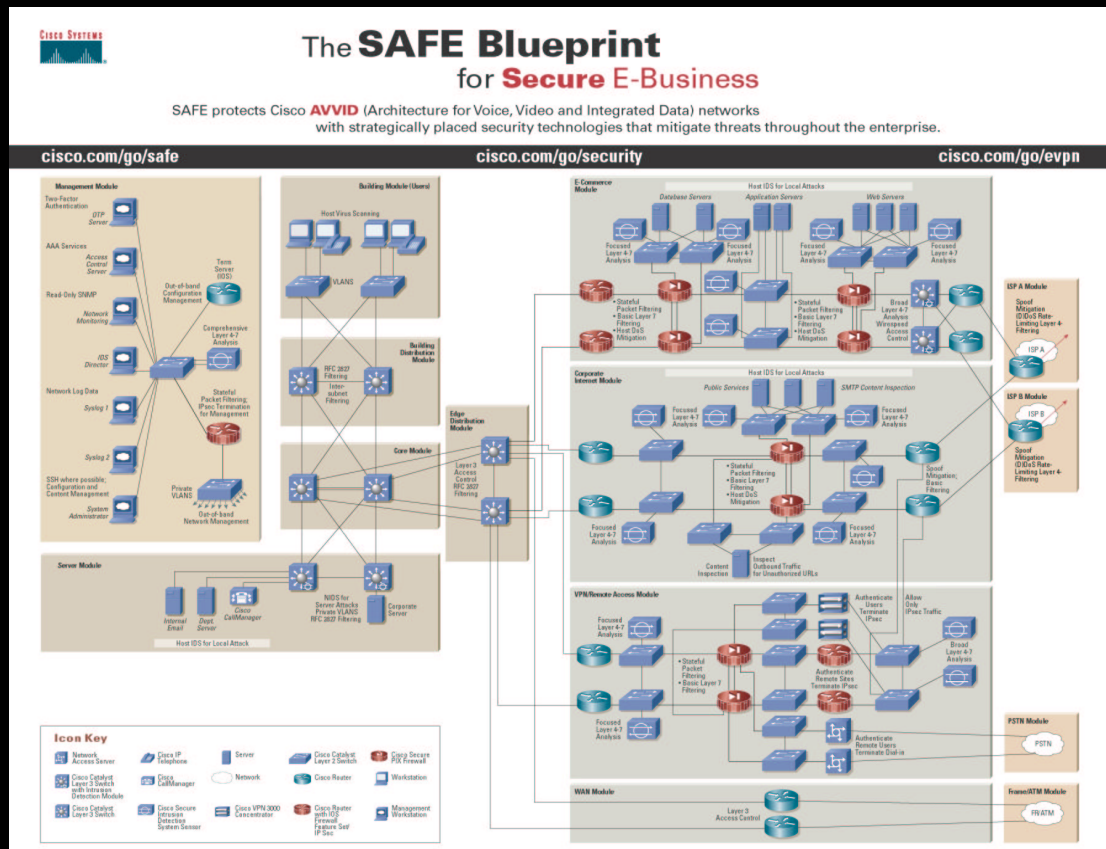
Cisco.com



SAFE: How to Put it All Together

Cisco.com

“Best practices” security blueprints for implementing integrated network security


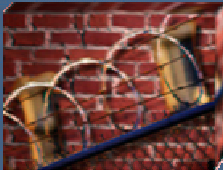








Blueprints available for:

- Enterprise
- Small Business
- IPsec VPNs
- Voice
- Wireless
- e Commerce (w/ content security)

Cisco's Security Offerings

Cisco.com

<p>Secure Connectivity</p> 	<p>Extended Perimeter Security</p> 	<p>Intrusion Protection</p> 	<p>Identity Services</p> 	<p>Security Management</p> 
<p>Appliances VPN 3000 Series PIX Firewalls 6503, 6506</p>	<p>Appliances PIX Firewalls 6503, 6506</p>	<p>Appliances 4200 Series PIX Firewalls Host Based CSA Agent</p>	<p>Cisco Access Control Server</p> <p>"IBNS" (Identity-Based Networking Services)</p>	<p>IP Solution Center (ISC)</p> <p>CiscoWorks VMS v2.2 (VPN/Security Management Solution)</p>
<p>Integrated Switch VPN Module</p>	<p>Integrated Switch Firewall Module</p>	<p>Integrated Switch & Router IDS Module</p>	<p>802.1x Extensions (per port, per user AAA)</p>	<p>SIMS 3.1 (Security Information Management Solution)</p>
<p>Cisco IOS VPN</p> 	<p>Cisco IOS Firewall</p> 	<p>Cisco IOS IDS</p> 	<p>Network Admission Control</p>	<p>CiscoWorks HSE (Hosting Solution Engine)</p>
<p>SOHO 90, 830, 1700, 2600, 3600, 3700, 7000 Series Routers</p>				

© 2003, Cisco Systems, Inc. All rights reserved.

Cisco Recommendations: First Steps

Cisco.com

- **Patch ALL vulnerable systems!**
- **Attack mitigation information from Microsoft:**
<http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp>
- **Use security scanner to discover systems running Windows RPC service. Including remote sites, dial-up users and VPN connections**
- **Apply ingress and egress filters or access control lists (ACLs) blocking access to ports 135 and 139 (TCP and UDP) as well as port 445 (TCP and UDP).**

Next Steps: Intrusion Prevention On The Host

Cisco.com

- **Cisco Security Agent (CSA)**
 - The default CSA 4.0 server and desktop policies stop successful execution of Blaster attack
 - On servers, the default server policy prevents the SVCHOST from attempting to execute CMD.exe. This prevents the exploit shell code from running.
 - On desktop systems the default desktop policy prevents the SVCHOST from accepting a connection on port 4444. Additional protection is provided by the default policy's prevention of any application from executing CMD.exe
- **Install Cisco Security Agent on servers and desktops.**

CSA in Action: Protection Against MsBlast

Cisco.com

Management Center for Cisco Security Agents - Microsoft Internet Explorer

Address: https://radams-storm/csamc/webadmin

CISCO SYSTEMS Management Center for Cisco Security Agents

Monitor Systems Configuration Maintenance Reports Profiler Search Help

Policy: All
Events per page: 50

Latest + Earliest

#	Date	Host	Severity	Event
73	8/13/2003 4:18:13 PM	rob-xp-pro	Alert	TESTMODE: The program 'C:\WINDOWS\System32\msblast.exe' was downloaded from the network and is now trying to execute. This is an unusual event, but can happen during automated software installation. This would normally trigger a user query. Details Rule 97 Wizard Find Similar
72	8/13/2003 4:18:11 PM	rob-xp-pro	Warning	TESTMODE: The process 'C:\WINDOWS\System32\ftp.exe' (as user NT AUTHORITY\SYSTEM) tried to rename to the file 'C:\WINDOWS\system32\msblast.exe'. This would have caused the user to be prompted as to the action to take. Details Rule 277 Wizard Find Similar
71	8/13/2003 4:18:00 PM	rob-xp-pro	Alert	TESTMODE: The current application 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\SYSTEM) would not have been permitted to execute the new application 'C:\WINDOWS\System32\CMD.EXE'. Details Rule 287 Wizard Find Similar
70	8/13/2003 4:18:00 PM	rob-xp-pro	Alert	TESTMODE: The process 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\SYSTEM) tried to open/read the file 'C:\WINDOWS\system32\cmd.exe'. This would have been denied. Details Rule 280 Wizard Find Similar
69	8/13/2003 4:18:00 PM	rob-xp-pro	Alert	TESTMODE: The process 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\SYSTEM) tried to accept a TCP connection from 10.5.64.127 on port 4444. This would have been prevented. Details Rule 325 Wizard Find Similar

No rule changes pending [Generate rules](#) Logged in as: admin



d'.
age is

CSA in Action: Protection Against MyDoom

Cisco.com

1/26/2004 4:32:22 PM: The process 'D:\Documents and Settings\gdepetro\Local Settings\Temp\message.scr' (as user AMER\gdepetro) tried to open/create the file 'C:\WINNT\system32\shimgapi.dll' and the user was queried. The user responded by choosing 'No'.

1/26/2004 4:32:26 PM: The process 'D:\Documents and Settings\gdepetro\Local Settings\Temp\message.scr' (as user AMER\gdepetro) tried to open/create the file 'C:\WINNT\system32\taskmon.exe' and the user was queried. The user responded by choosing 'No'.

1/26/2004 4:32:26 PM: The process 'D:\Documents and Settings\gdepetro\Local Settings\Temp\message.scr' (as user AMER\gdepetro) tried to open/create the file 'D:\Documents and Settings\gdepetro\Local Settings\Temp\taskmon.exe' and was denied.

1/26/2004 4:32:38 PM: Potential worm propagation: The process 'D:\Documents and Settings\gdepetro\Local Settings\Temp\message.scr' (as user AMER\gdepetro) has read downloaded content (file D:\Documents and Settings\gdepetro\Local Settings\Temp\message.scr) and attempted to access an email or network related resource (gdepetro.wab). This is considered suspect. The user chose 'Terminate'.

1/26/2004 4:32:45 PM: The process 'D:\Documents and Settings\gdepetro\Local Settings\Temp\message.scr' (as user AMER\gdepetro) tried to write-value the registry key '\REGISTRY\USER\S-1-5-21-1801674531-2025429265-839522115-189223\SOFTWARE\MICROSOFT\Windows\CURRENTVERSION\Explorer\Shell Folders', value 'History' and the user was queried. The user responded by choosing 'No'.

Next Steps: Intrusion Detection In The Network

Cisco.com

- **Network Based Intrusion Detection (NIDS)**
 - **Attack detection triggers NIDS to send alarm and/or either shun or reset connection**
 - **Network Based Intrusion detection can be performed via dedicated appliances, routers, firewalls or IDS modules on Catalyst 6500 switches**

Next Steps: Access Control

Cisco.com

- **Stateful Firewalling**
 - **Stateful inspection engine can control connection attempts at a level more granular than normal by validating proper protocol adherence**
 - **Limit number of inbound connections to server**
 - **Disallow outbound connections from devices**
 - **Limits self-propagation of worm**
 - **Stateful firewalling can be performed on dedicated security appliances, routers or firewall modules for Catalyst 6500 switches.**

Next Steps: Access Control

Cisco.com

- Ingress Filtering

- Block access to ports 135, 139, 445 (UDP & TCP)
- Proper ingress filtering will block Blaster attempts at user systems

```
access-list 101 deny udp any any eq 135 log-input
access-list 101 deny tcp any any eq 135 log-input
access-list 101 deny udp any any eq 139 log-input
access-list 101 deny tcp any any eq 139 log-input
access-list 101 deny udp any any eq 445 log-input
access-list 101 deny tcp any any eq 445 log-input
access-list 101 permit ip any any
```

Next Steps: Access Control

Ingress Filtering - Fine Tuned Approach

Cisco.com

Fine-tuned approach Step 1: *Create ACL*

```
access-list 101 permit udp any any eq 135
access-list 101 permit udp any any eq 139
access-list 101 permit udp any any eq 445
access-list 101 permit tcp any any eq 135
access-list 101 permit tcp any any eq 139
access-list 101 permit tcp any any eq 445
```

Next Steps: Access Control

Ingress Filtering - Fine Tuned Approach

Cisco.com

Ingress Filtering Fine-tuned approach Step 2: *Match on ACL and packet length*

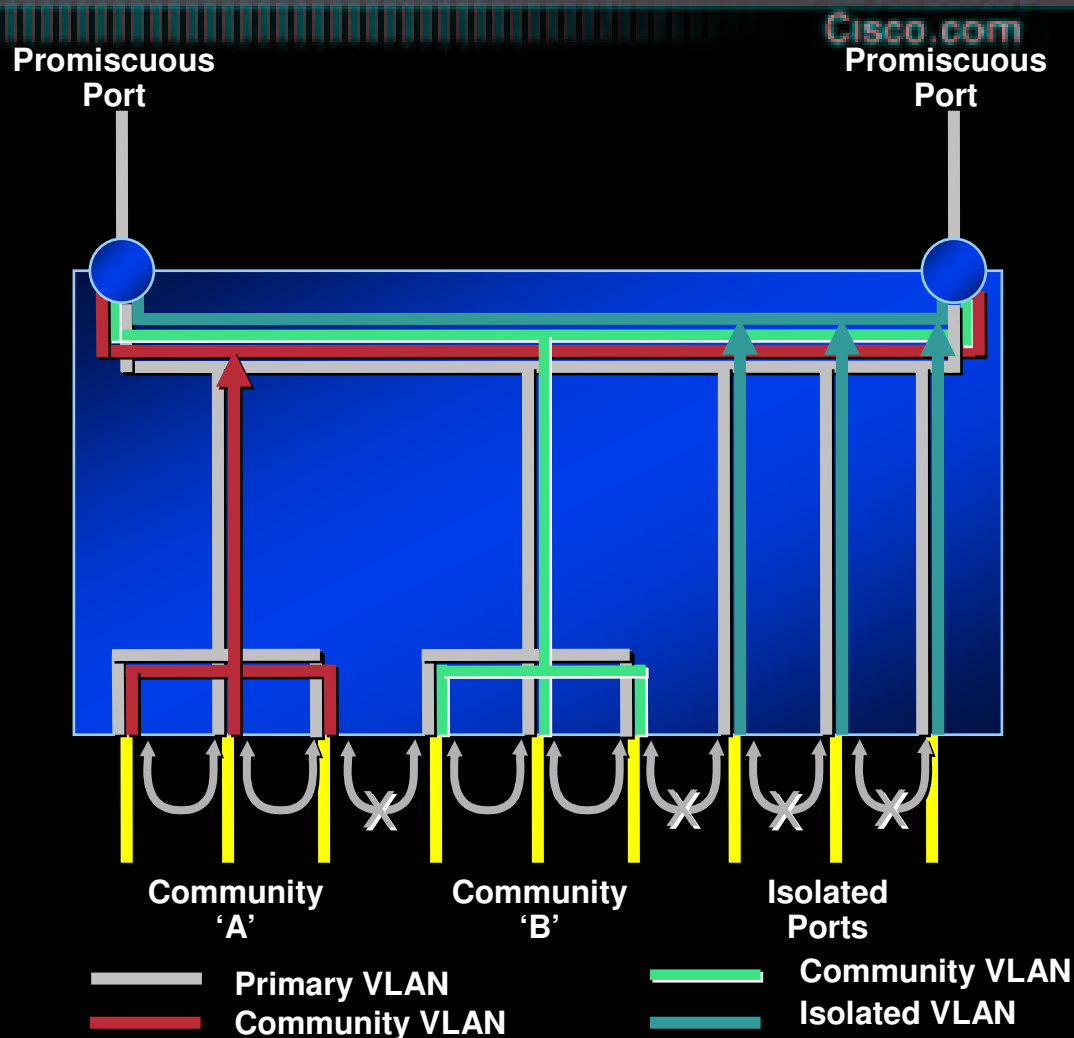
```
class-map match-all rpc_dcom  
match access-group 101
```

Ingress Filtering Fine-tuned approach Step 3: *Use class-based policing to drop matching packets at the ingress interface*

```
policy-map drop-rpc-dcom  
class rpc_dcom  
police 8000 1000 1000  
          conform-action drop exceed-action drop violate-action drop
```


Next Steps: Private VLANs

- Hosts on given segment can only communicate with default gateway – NOT other hosts on network
- Compromised device could not infect others
- For more info on Private VLANS



<http://www.cisco.com/warp/public/473/90.shtml>

Next Steps: Network Based Application Recognition

Cisco.com

- **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 the Blaster worm**
 - **NBAR can immediately classify the NetBIOS traffic and drop the packet before it reaches the device.**

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

Next Steps: Netflow Switching

Cisco.com

NetFlow switching is a high-performance, network-layer switching path: captures wide range of traffic statistics including user, protocol, port, and type of service information. This can be used to identify network traffic patterns and assist in response to Blaster.

Netflow configuration information:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_configuration_guide_chapter09186a00800880f9.html

Next Steps: Committed Access Rate (CAR)

Cisco.com

- **Blaster worm contains code for a DoS attack against the system *windowsupdate.microsoft.com***
- **CAR can rate-limit traffic based on a set of criteria and provides configurable actions such as transmit, drop, set precedence, or set QoS group when the traffic meets or exceeds rate limit**
- **Criteria include such metrics as incoming interface, IP precedence, QoS group, or IP access list criteria as well as others**
- **CAR performs two QoS functions:**
 - **Bandwidth management through rate-limiting**
 - **Packet classification**
- **CAR Information**
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800c75ce.html

Additional Information

Cisco.com

- Cisco Security Information:
www.cisco.com/go/security
- Cisco SAFE and “Blaster” Whitepapers:
www.cisco.com/go/safe
- Cisco Product Security Incident Response Team (PSIRT):
www.cisco.com/go/psirt
- Cisco Self-Defending Network:
www.cisco.com/go/selfdefend
- Microsoft Security:
www.microsoft.com/technet/security

End-Point Protection

Cisco.com

- **Cisco Security Agent Demonstration**
- **Eric Ahlm of Vigilar, Inc.**
- **4:15 pm EST Session – U2**

Thank You

