The Self-Defending Network
Innovations in Meeting Tomorrow’s Blended Threats

Ricky Elias
Business Development Manager
Advanced Technology
Cisco Systems (USA) Pte Ltd
relias@cisco.com
Top Security Issues for 2005

“Chief Security Officers from several top technology firms and government agencies say computer worms, viruses and regulatory compliance are likely to be the hot button issues that will keep them awake at night in 2005”

2nd CSO Interchange – New York, December 2004

• The need to quickly patch vulnerabilities is becoming a major security pain point

• Customers are considering using hyper-patching and mass roll-out systems (push technology) to start solving hyper-patching problems
Security Threat Evolution
Increased Risk of Theft and Disruption

Target and Scope of Damage
- Global Infrastructure Impact
- Regional Networks
- Multiple Networks
- Individual Networks
- Individual Computers

Weeks
1st Gen
- Boot viruses

1980s

Days
2nd Gen
- Macro viruses
- Email
- DoS
- Limited hacking

1990s

Minutes
3rd Gen
- Network DoS
- Blended threat (worm + virus + trojan)
- Turbo worms
- Widespread system hacking

Today

Seconds
Next Gen
- Infrastructure hacking
- Flash threats
- Massive worm driven DDoS
- Damaging payload worms
- Wide-spread data theft

Future
The Year in Review
Bot, Phishing, Spyware, Blended Attack

Phishing
The Year in Review
Increased Mobility

- Even the most effective perimeter defense will not stop “piggy-back” infections
- It is not cost effective to manually check each laptop and device as it comes in from the outside
The Year in Review
Emerging Threats in the Corporate Interior

- Works for traffic within or outside of a building
- Attacker only needs to be attached on same subnet as one victim
- Tools easily downloadable and is simpler than most video games (GUI or CLI, your choice)

# ettercap -NCsz                           [captures username/password combinations- highlighted below]
ettercap 0.6.3.1 © 2001 AloR & NaGA

Your IP: 192.168.0.70 with MAC: 00:03:FF:BE:F0:52: eth0
Loading plugins... Done.
Resolving 1 hostnames...
Press 'b' for help...
Sniffing (IP based): ANY:0 < -- > ANY:0
TCP packets only... (Default)
Collecting passwords:
00:22:10 192.168.0.70:1107 < -- > 192.168.0.42:80       www
USER: root
PASS: hamhocks4#age

http://mail.victim.com/root.asp  <- [the site where username and password was entered]
Evolution of Security Requirements

PAST

Reactive

Standalone

Product Level

NEEDED NOW

Automated, Proactive

Integrated
Multiple Layers

System-level Services

A Collaborative Systems Approach
A Logical Strategic Response
Self-Defending System

An integrated system
- Endpoint security solutions know security context and posture
- Policy servers know compliance/access rules
- Network infrastructure provides enforcement mechanisms

Intelligent Linkage of Endpoint with Network
Multiple Layers of Network Defense

Risk-ometer

High
Medium
Moderate
Low

Risk has been minimized!
You Can Protect The Interior
Keep the Insiders Honest

Catalyst Integrated Security Features
Layered Cisco Integrated Security Prevents Common Attacks

- Catalyst Integrated Security Features help administrators prevent and track man-in-the-middle attacks
- Prevents DHCP starvation attacks
- Prevents IP Spoofed DoS Attacks
- Hardens the Ethernet standard

IP Source Guard
Dynamic ARP Inspection
DHCP Snooping
Port Security

Protect the Interior
Cisco.com
Segment The Campus
Assign Access Based on Identity

- Based upon user’s credentials via 802.1x (user identity)
- Guest users or those without 802.1x running on their laptop can be denied or placed into a guest VLAN

Unauthenticated User Is Blocked Access to the Network
Network Admission Control
Detect and Remediate

1. Non-compliant endpoint attempts connection
2. PC is denied access to the corporate Net
3. Quarantine area and remediation

BRANCH OR CAMPUS

NAD
CTA

Corporate Net
Remediation
Quarantine Area

CAMPUS

NAD
Network Admission Device
CTA
Cisco Trust Agent
ACS
Access Control Server
Multiple Layers of Endpoint Behavior Protection

**Probe phase**
- Ping scans
- Port scans

**Penetrate phase**
- Transfer exploit code to target

**Persist phase**
- Install new code
- Modify configuration

**Propagate phase**
- Attack other targets

**Paralyze phase**
- Erase files
- Crash system
- Steal data

Distributed Firewall
O/S Hardening
Host IDS/IPS
File Monitoring
System Policy Control
Patch Management
Malicious Code Protection

Protect the Endpoints
Self Defending Network Strategy

SELF-DEFENDING
NETWORK

Dramatically Improve the Network’s Ability to Identify, Prevent, and Adapt to Threats

INTEGRATED SECURITY
- Secure Connectivity
- Threat Defense
- Trust and Identity

SECURITY TECHNOLOGY INNOVATION
- Endpoint Security
- Application Firewall
- SSL VPN
- Network Anomaly Detection

SYSTEM-LEVEL SOLUTIONS
- Endpoints + Networks + Policies
- Services
- Partnerships
Questions?
The Self-Defending Network
Innovations in Meeting Tomorrow’s Blended Threats

Ricky Elias
Business Development Manager
Advanced Technology
Cisco Systems (USA) Pte Ltd
relias@cisco.com