

Fighting Back Against Cybercrime: What Works

Alan Paller

Director of Research

The SANS Institute

paller@sans.org

www.sans.org

Four Questions For Today

- Is physical damage really possible?
- What other damage is being done to government systems and other Internet users?
- Why are the attacks so easy?
- What model initiatives have proven to work in fighting back against cybercrime and in building better defenses?



Hacker jailed for revenge sewage attacks

By [Tony Smith](#)

Posted: 31/10/2001 at 15:55 GMT

An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel.

"Marine life died, the creek water turned black and the stench was unbearable for residents," said Janelle Bryant of the Australian Environmental Protection Agency.

The Maroochydoore District Court heard that 49-year-old Vitek Boden had conducted a series of electronic attacks on the Maroochy Shire sewage control system after a job application he had made was rejected by the area's Council.

Lesson One

- Electronic attacks do cause the infrastructure to fail

What else happens?

And why?

How many .gov & .mil sites were hacked in 100 days?

- Administrative Office of the U.S. Courts (www.mab.uscourts.gov)
- Army Signal Command (cpocner.apg.army)
- Army Signal Command (www.mears.redstone.army.mil)
- Aviation Systems Division, NASA Ames (www.aviationsystemsdivision.arc.nasa.gov)
- ci.washington.dc.us (www.ci.washington.dc.us)
- Defense Automated Printing Service (dodssp.daps.mil)
- DISA Information Systems Center (maestro.den.disa.mil)
- DOI US Bureau of Reclamation (www.mp.usbr.gov)
- DOI US DOI, Bureau of Land Management (adoptahorse.blm.gov)
- DoT National Transportation Safety Board (www.nts.gov)
- DoT United States Department of Transportation (stratplan.dot.gov)
- Energy Sandia National Laboratories (samt4831.sandia.gov)
- Federal Maritime Commission (www.fmc.gov)
- Government Printing Office (www.gpo.gov)
- Multistate Tax Commission (www.mtc.gov)
- NASA #2 Technical Info, Jet Propulsion Labs (NASA) (techinfo.jpl.nasa.gov)
- NASA LARC NASA (se-pc7.larc.nasa.gov)
- NASA National Aeronautics and Space Administration (toyota.gsfc.nasa.gov)
- NASA Technology Server, NASA (technology.nasa.gov)
- National Highway Traffic Safety Administration (www.nhtsa.dot.gov)
- National Institutes of Health (intra.ninds.nih.gov)
- National Library of Medicine SIS5 Server, NIH (sis5.nlm.nih.gov)
- **MORE...**

More .gov and .mil sites hacked

- NOAA Central Administrative Support Center, NOAA (`www.casc.noaa.gov`)
 - NOAA National Oceanic and Atmospheric Admin (`storms-dev.nos.noaa.gov`)
 - NOAA National Oceanic and Atmospheric Administration (`vortex.cmdl.noaa.gov`)
 - NSF National Science Foundation (`roga.nsf.gov`)
 - U.S. Fish and Wildlife Service (`www.fws.gov`)
 - Uniformed Services University of the Health Science (`bb.lrc.usuhs.mil`)
 - Uniformed Services University of the Health Science (`rcslinux.lrc.usuhs.mil`)
 - US Navy Naval Computer and Telecommunications Station (`med01.nctsw.navy.mil`)
 - US Navy Jaxm Navy (`www.jaxm.navy.mil`)
 - US Navy Naval Ocean Systems Center (`iph-nt5.nosc.mil`)
 - US Navy Naval Pacific Meteorology and Oceanography Center, Yokosuka, Japan (`www.yoko.npmoc.navy.mil`)
 - US Navy NLMOC Navy (`jf.nlmoc.navy.mil`)
 - US Navy `www.nasjax.navy.mil` (`www.nasjax.navy.mil`)
 - US Office of Surface Mining (`feecomp.osmre.gov`)
 - USGS United States Geological Survey (`mrdata.usgs.gov`)
- Total Reported and Mirrored at `attrition.org` August 1 to November 10: **37**
- Last spring on average one new site was defaced every day.

How could that many be defaced in such a short time?

Lesson Two

- Systems are delivered with known vulnerabilities.
- In other words they are vulnerable to immediate attack
- The Cisco router password is
 - You care because

IIS4 / IIS5 ISAPI Vulnerability

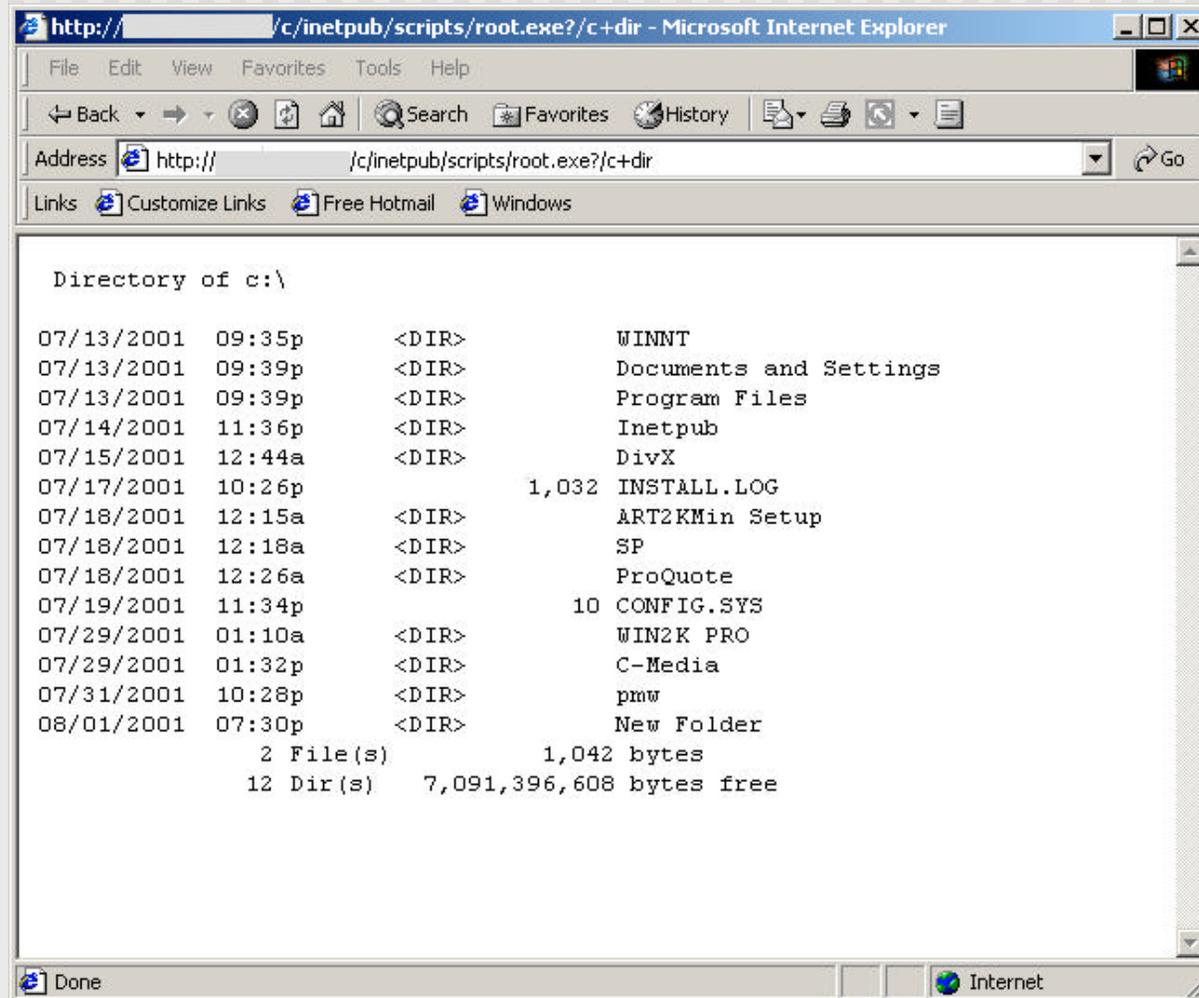
The screenshot shows a Microsoft TechNet page for a security bulletin. The header includes 'Microsoft' and 'TechNet Worldwide'. A search bar contains the text 'I want to: Select from this list'. The breadcrumb trail is 'TechNet Home > IT Solutions > Security > Bulletins'. The main heading is 'Microsoft Security Bulletin MS01-033'. The title of the bulletin is 'Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise'. The original post date is 'June 18, 2001'. The section 'Summary' contains the following text: 'Who should read this bulletin: System administrators of web servers using Microsoft® Windows NT® 4.0 or Windows® 2000. Impact of vulnerability: Run code of attacker's choice. Recommendation: Microsoft strongly urges all web server administrators to apply the patch immediately. Affected Software: Microsoft Index Server 2.0, Indexing Service in Windows 2000. Note: Indexing Service in pre-RC1 versions of Windows XP is also affected by the vulnerability. As discussed in the FAQ, Microsoft is working directly with the small number of customers who are using a pre-RC1 beta version in production environments to provide remediation for them.'

Nearly all systems with this vulnerability were infected with Code Red II

Code Red II installed a back door.

The back door was still there after installing patches

Code Red made 150,000 systems vulnerable to instant attack



Lesson Three

- Widespread vulnerabilities lead to indiscriminant worms and loss of control of your systems – just because you have the vulnerability.



THE COMPAQ ADAPTIVE INFRASTRUCTURE IS ABOUT TO CHANGE EVERYTHING.

Good Morning America | World News Tonight | 20/20 | Downtown | Primetime | Nightline | This Week

TECH



SEARCH

ABCNEWS Keyword

Find

SIDEBARS

[Complete Coverage of the Cyber Attacks](#)

RELATED STORIES

Denial of service attack takes FBI site down all day

[Protection Center](#)
[GO Network Hacking Links](#)
[SecurityFocus.com](#)
[attrition.org](#)

3rd time

- ▶ HOMEPAGE
- ▶ NEWS SUMMARY
- ▶ U.S.
- ▶ INTERNATIONAL
- ▶ MONEYScope
- ▶ WEATHER.com
- ▶ LOCAL NEWS
- ▶ ENTERTAINMENT
- ▶ SPORTS
- ▶ SCI / TECH
- ▶ POLITICS
- ▶ HEALTH
- ▶ LIFESTYLES
- ▶ TRAVEL



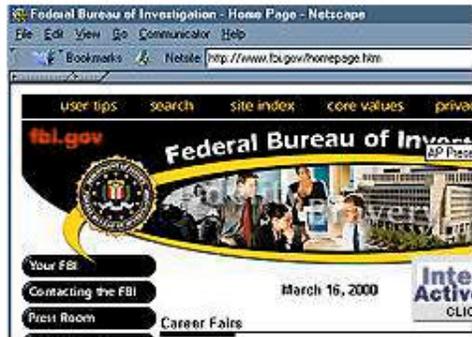
- REFERENCE
- TURBO NEWS
- SEND THIS PAGE TO A FRIEND
- EMAIL
- ABCNEWS.com
- HELP & TOOLS



GO TO: Select a Topic

HOME PAGE » TECH » FEATURE

FBI Under Attack Web Site Knocked Offline Again



(www.fbi.gov)

By Jonathan Dube
abcNEWS.com

March 16 — The FBI's Web site was knocked offline by another denial-of-service attack this week, but officials won't say whether they believe the incident is related to last month's spate of similar attacks.

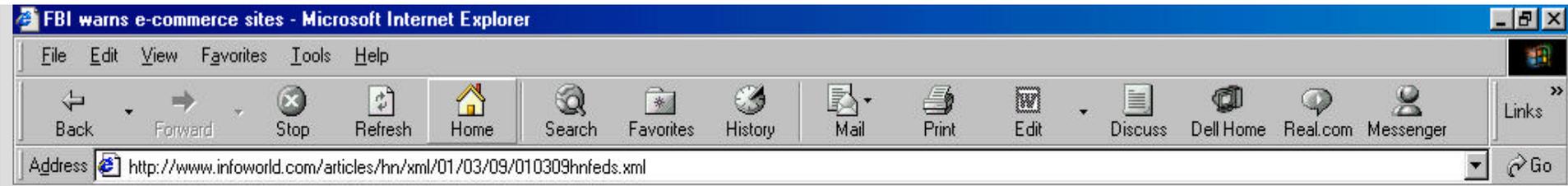
The site was attacked Tuesday, just as the FBI was celebrating the 50th anniversary of its "Ten Most Wanted Fugitives" program. The site came under attack at around 9 a.m. and was down until early evening, FBI spokeswoman Debbie Weierman told ABCNEWS.com. "We were indeed attacked and taken down," Weierman said. "The problem was assessed and we are back up and running now."

Third Time Attacked

This is the third time the FBI site has been taken offline by a denial-of-service attack. The site was attacked last spring and then again on Feb. 18, one week after the spate of attacks that took down leading Web sites.

Lesson Four

- Web and Internet activity can be stopped by denial of service attacks
- New SNMP vulnerability changes the requirement from hundreds of machines for hours to one machine and one packet.



More than 100 organizations report extortion...

SITEMAP News Test Center Opinions Events Webcast Forums Careers Stock Quote Subject Indexes About Us Search SUBSCRIBE HOME



News

Friday, Mar. 9, 2001 3:40 am PT

More articles on [Security](#)

FBI warns e-commerce sites

By [Margret Johnston](#) and [Joris Evers](#)

THE U.S. FEDERAL Bureau of Investigation (FBI) is again warning electronic-commerce Web sites to patch their Windows-based systems to protect their data against hackers.

The FBI's National Infrastructure Protection Center (NIPC) has coordinated investigations over the past several months into organized hacker activities targeting e-commerce sites, the FBI said in a statement issued Thursday. More than 40 victims in 20 states have been identified in the ongoing investigations, which have included law enforcement agencies outside the United States and private sector officials.

The investigations have uncovered several organized hacker groups from Russia, the Ukraine, and elsewhere in Eastern Europe that have penetrated U.S. e-commerce and online banking computer systems by exploiting vulnerabilities in the Windows NT operating system, the statement said. Microsoft has released patches for

[Click Here for more](#)

40 victims in 20 states

[Webcasts](#) See and hear the experts as they tackle hot topics and technologies.

Today in InfoWorld

[U.S. companies take scissors to IT spending](#)

[Sun to unveil 64-bit Serend](#)

[Qwest](#)

[Voices: appr](#)

[Telekom merger](#)

[HP targets multimedia](#)

Organized crime groups in Russia and Ukraine

E-mail this article

Print this article

In News

[This week: News and Features](#)

[Microsoft under fire](#)

[Features](#)

[Mentor's Corner](#)

[CTO](#)

Lesson Five

- Cyber extortion works
- Extradition is very hard

Denies fallacious press release on their own website

[Back to News Releases](#)

- Corporate Information
- Management Overview
- News Releases
- Employment Opportunities
- Home

AASTROM BIOSCIENCES, INC. DENIES FALLACIOUS PRESS RELEASE

Ann Arbor, Michigan, February 17, 2000 - Aastrom Biosciences, Inc. (Nasdaq: ASTM) today reported that its website has been corrupted by sabotage. A fallacious press release announcing that Aastrom was merging with Geron, Inc. was posted to the Aastrom website, apparently by a computer hacker. Aastrom stated that there is no truth to the merger announcement. The Company has alerted Nasdaq authorities and Geron to the violation and is investigating the matter further.

"We are appalled by this ruthless attempt to manipulate markets and potentially harm the shareholders of both companies," said R. Douglas Armstrong, President and CEO of Aastrom. "While we have no idea how this occurred, we are currently investigating the security of the website. In the meantime, we apologize to our shareholders for any disruption in the trading of Aastrom's stock and wish to assure financial markets that we will work closely with the appropriate authorities to pursue those who are responsible."

Appalled by the ruthless attempt to manipulate

Aastrom Biosciences, Inc. is pioneering the development of proprietary clinical systems including the AastromReplicell™ System, a first of its kind product, to enable physicians and patients greater accessibility to cells used for therapy. Aastrom has received patents covering methods and devices for the ex vivo production of human stem and other types of cells, as well as for the genetic modification of stem cells. The AastromReplicell™ System is under development, and is not available for sale at this time in the U.S., except for research and investigational use.

Contact:

Todd E. Simpson
VP Finance & Administration, CFO
Aastrom Biosciences, Inc.
734-930-5777

Investor & Media
Francesca T. DeVellis
Feinstein Kean Partners Inc.
617-577-8110

Lesson Six

- Hackers change web pages for personal profit or spite.
- Small changes on web pages can have big impacts.

Primary Points of Vulnerability

- Vendors sell systems with known and unknown vulnerabilities
- Vulnerable services are turned on without the buyer's full knowledge
- System administrators don't maintain security patch levels and configurations
 - because they don't know the services are running
 - because it is hard or dangerous,
 - because it is not a priority, and
 - because they have not learned how
- System and security administrators often do not know how to defend their systems

Promising Practices

What Works?

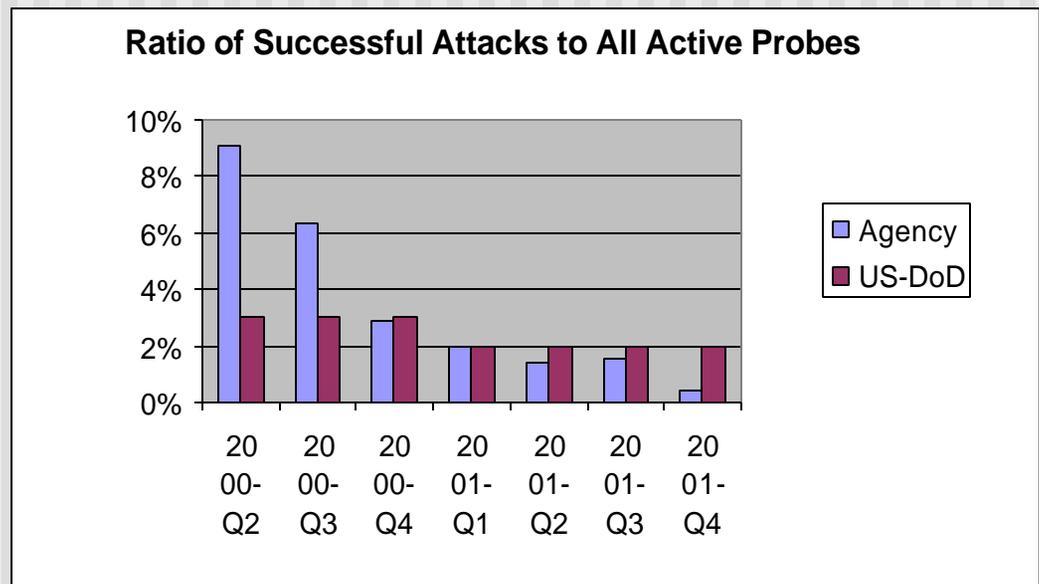
Problems and
Solutions

1. Too many vulnerabilities

- Problem facing most organizations
 - Systems are delivered with unnecessary services, vulnerable services and other known problems
 - Scanners are used to find hundreds of vulnerabilities
 - Sysadmins do not have time to fix them all so their fixes are uneven
 - Weaknesses in “unimportant systems” allow the hackers to get inside and do major damage.

NASA's Universal Monitoring of Top 50 Vulnerabilities

- Picked the top 50 vulnerabilities attackers actually have used
- Scanned every system, every quarter
- Charted and compared all Centers
- Repeated with new vulnerabilities – 3 times



- Result 1: 93% reduction in high priority vulnerabilities across all of NASA
- Result 2: Significant reduction in rate of successful attacks: best in benchmarks

2. Unsafe Installations

- Problem facing most organizations:
 - Systems are delivered with known vulnerabilities
 - Every system administrator must learn what is needed to harden Solaris and then must do it right, every time.
 - Sysadmins have found that attack programs probe while patches are being downloaded; they're rooted before the patches are installed.

Sandia's Procurement of "Safer" Systems from Sun

- Gain agreement on what it takes to harden Solaris.
- Keep the specification up to date.
- Contract with Sun to deliver a Solaris installation disk that contains the safe configuration.
- Have every sysadmin install the safer Solaris.

3. Confusing/Conflicting Alerts

- Problems facing most organizations:
 - Sysadmins get multiple alerts; none are authoritative; many are incomplete
 - They don't know which apply to their systems
 - They don't know which are critical

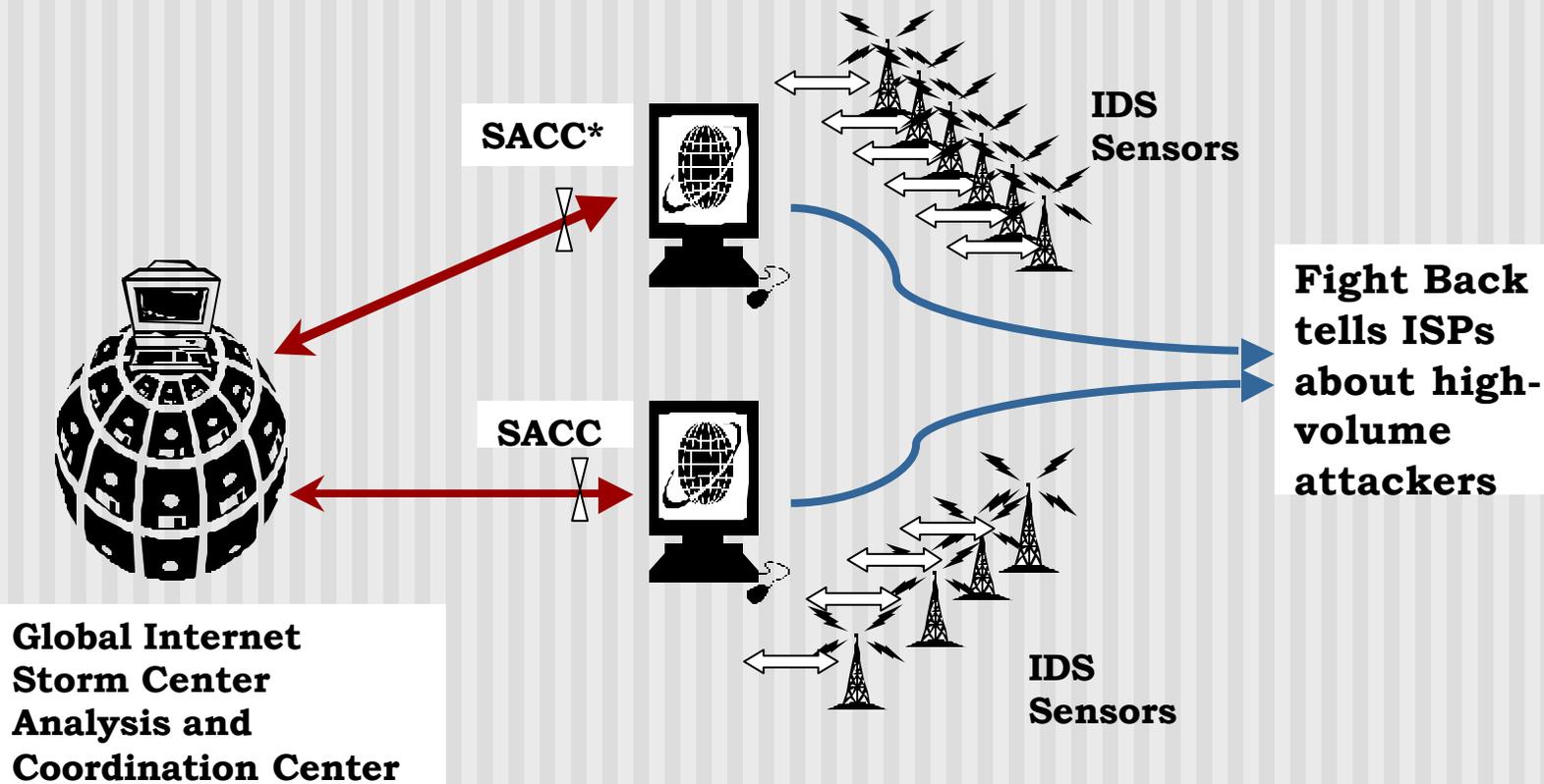
GSA's new alert/patching system

- GSA Contracted with SAIC/Vigilinx
- Sysadmin registers configuration (40 most common systems/applications)
- Registered sysadmins receive:
 - Alerts when they apply to configuration
 - Verified library of patches as soon as patches are available
- Free for all Federal sysadmins
- Starts June 24

4. Thousands of Rooted Systems Running Attack Scripts

- Problem:
 - Vulnerable systems are exploited and used by hackers to run attack scripts searching the Internet for new victims
 - Owners do not know about it.
 - ISPs get thousands of complaints a day; can't decide which are critical.
 - Systems continue to attack innocents: At MIT, 5 minutes on average, before attack program probes.

Storm Center



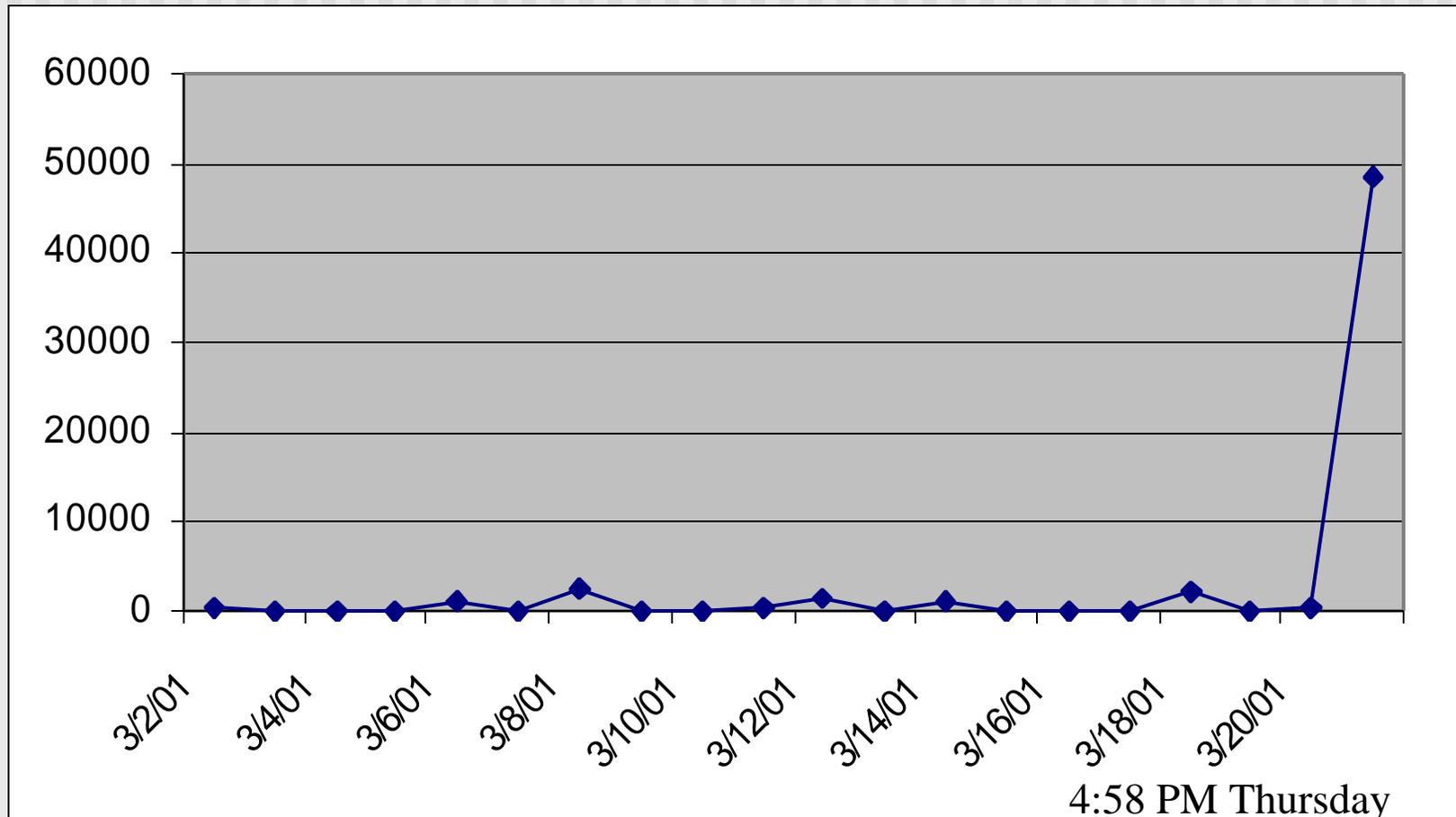
*SACCs may be PDD63 ISACs, national government CERTs, ISPs and other managed service providers, large user organizations, and independent SACCs.

5. Need for early warnings

- When a worm starts to spread, most people are unaware.
- Instant action is necessary to stop the damage, but if we don't know it is spreading we cannot act.
- Storm Center also serves as the Internet's Early Warning System for worms

Knowing an attack has been launched?

Combined data from 120 sites show that unwanted traffic to port 53 spiked on 3/21.



How do you find the worm code?

- It's hard to find one of a few thousand infected systems out of 100 million systems on the Internet.
- So you need a large community made up of folks who are skilled, have the right systems, and are willing to help look for it.
- 91,000 subscribers of the weekly Security Alert Consensus fit that profile.
- They found the code less than 3 hours after a note went out to them.

The Lion Worm

- Uses a well-known BIND vulnerability
- Steals password files and sends them to china.com
- Installs multiple back doors and a DDoS attack tool.
- Forces the infected system to search the Internet for more vulnerable systems and infect them.

How do you analyze the code and develop a tool to find machines that have been infected – overnight!

- Recruit volunteers from a small circle of trusted people who have proven their ability to analyze code and develop diagnostics.
- Jointly analyze the code and test the tool
- Deliver beta to small group of sites
- Fix and post the tool. (20,000 downloads the first day)

12:10 AM – 7:15 AM Friday, 3/23

How do you tell the people who need to know?

- Use an alerts-only announcement to 200,000 security professionals.
- Involve other distribution points.
- Complement the announcements with technology news coverage.

Follow-Up

- UUNET black-holes traffic to China.com where the worm sent password files – providing more immediate damage reduction than all our announcements.
- Analysts infiltrate the worm author's IRC chat room – identify new strains before they are launched.

Saturday 3/24 – Wednesday 3/28

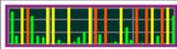
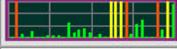
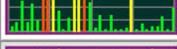
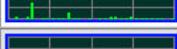
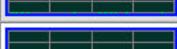
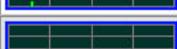
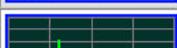
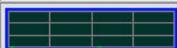
Ten most probed ports

Dshield - Top 10 Target Ports - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Top Ten Target Ports

This list shows the top 10 most probed ports. You may also want to check the [Port of the Day](#) which will discuss a recently active port in more detail. Our [Internet Primer](#) explains what these terms mean.

Service Name	Port Number	Activity Past Month	Explanation
domain	53		Domain name system. Attack agains old versions of BIND
ftp	21		FTP servers typically run on this port
sunrpc	111		RPC. vulnurable on many Linux systems. Can get root
printer	515		lpdng exploits in RedHat 7.0
???	6346		
ingreslock	1524		
???	34258		
???	34255		
telnet	23		
???	1029		

Internet

Internet Storm Center

Welcome to incidents.org - By The SANS Institute - Microsoft Internet Explorer

File Edit View Favorites Tools Help



www.incidents.org

by The SANS Institute

SANS 2001
MAY 13 - 20, 2001
BALTIMORE, MD



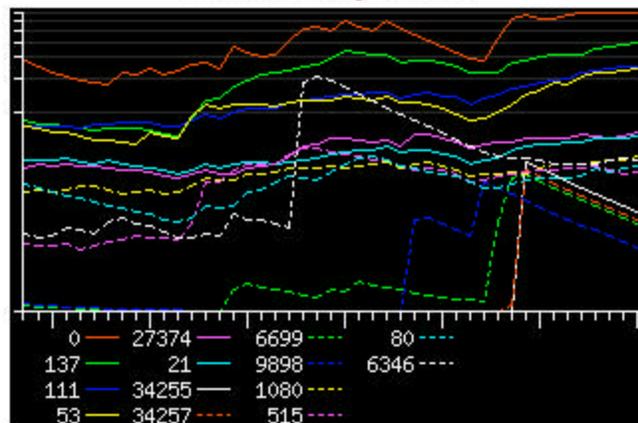
INTERNET STORM CENTER™

- [Internet Storm Center™](#)
- [Background](#)
- [How It Works](#)
- [ISW Management](#)
- [ISW Services](#)
- [Global ISW Services](#)
- [How to Participate](#)

CONSENSUS INTRUSION DATABASE

- [CID](#)
- [Partners](#)
- [Graphs](#) **NEW**
- [FAQ](#)

Current CID Graph 05/04/01



[How to read the CID Graph](#)

THREAT LEVEL ▶ ■ ■ ■ ■

ALERTS AND NEWS

[Carko](#)
[News](#)

PROTECT

[Perimeter Protection Reading](#)
[Egress Filtering](#)
[Dynamic ACL Generator](#)

DETECT

[CID](#)
[Intrusion Detection Reading](#)

6. Uneven Security Skills

- Most security skills are learned on the job
- MCSE, Solaris, CCNA certifications do not require mastery of stopping vulnerabilities
- When attacks succeed sysadmins claim “no one ever told me about the problem” and often blame the security people.
- Gartner: “By 2004, technical information security certifications will be required of 40% of all technical operations staff. (.8 probability)”

SANS Training and GIAC Certification

- 26,000 alumni
- More than 3,000 have earned certification in firewalls and perimeter protection, auditing, security management, intrusion detection, incident handling and hacker exploits, Windows, UNIX
- Training competition – 9 years
- Problem: limited capacity
- New strategy: Online and mentored training

Mentored Training

- Students use online audio and text system that mimics live lecture and notes
- Online includes hourly quizzes for mastery and confidence building
- Mentor meets with students every two weeks to emphasize key points and go over hands-on exercises
- Great way to give something to the security community.

7. Lack of consensus on security

- What does it mean to have a secure configuration of Solaris or RedHat or Windows 2000 or Oracle?
- How do you tell your system administrators what they have to do in security?
- How do you test whether your systems are secure? And audit the tests?
- How do you tell management that your systems are secure?

Windows 2000

- SANS Step-by-Step Securing Windows 2000
- National Security Agency 19 guides on securing Windows 2000
- National Institute of Standards and Technology Windows 2000 secure configuration guide
- The Center for Internet Security Benchmark and Testing Tool
- April 18, 2002 – Consensus!

Center for Internet Security

- 170 organizations: from VISA to US National Institute of Standards and Technology, to Singapore Government, to Royal Canadian Mounted Police, to Shell, Hallmark, Intel ...
- Agree on benchmarks, produce tools that automatically test systems and give them a score on meeting benchmarks
- Cisco IOS, Windows 2000, Solaris – five more coming shortly
- www.cisecurity.org

With Consensus

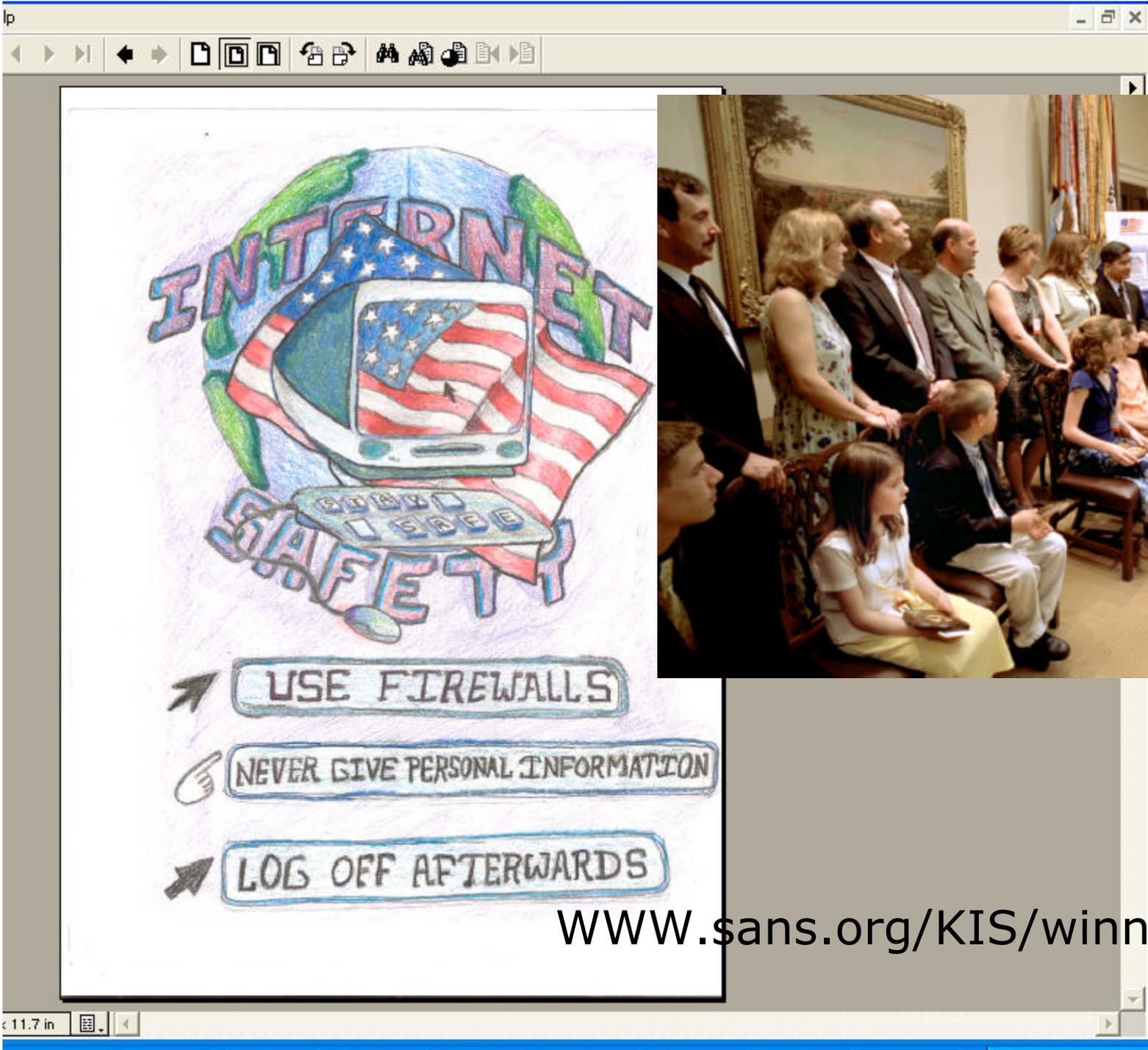
- Application developers can program to the safe configuration
- Auditors and operations staff can agree on what to test – removing some of the “gotcha” game
- CIOs can order systems configured safely; vendors can deliver optional “safe configurations”

SANS Consensus High Priority Vulnerabilities

- ISS, Qualys, Symantec, ICAT, Nessus all helping
- Identifying the consensus list of the most critical vulnerabilities
- Will be used for site certification – equivalent of “Good Housekeeping Seal of Approval”

8. Kids don't think security is cool

- They lionize the hackers
- They leave their systems vulnerable
- They become hackers themselves



www.sans.org/KIS/winners.htm

Questions