

# **The Changing Face of Cyber Crime**

## **Top Cyber Menaces for 2008 and Promising Initiatives to Fight Back**



**September 9, 2008**  
**SANS SCADA Security Summit**  
**Amsterdam**

**ALAN PALLER**  
**Director of Research**  
**THE SANS INSTITUTE**  
**APALLER@SANS.ORG**

# Questions for Today



- Who are the cyber criminals?
- What are their new targets?
- What are the most promising initiatives to deter attacks?

# The Three Faces of Cyber Crime



- 1. ORGANIZED CRIME**
- 2. TERRORIST GROUPS**
- 3. NATION STATES**

# 1. A Massive Financial Cyber Crime Wave



- Many billions of dollars.
- FBI senior exec: “we are getting more than one new cyber extortion case every day.”
- Online Broker e-Trade lost \$18 million
- Pump & dump moves the stock market
- Bankers tell of 400% increases in cyber fraud from 2005 to 2006

# COMPUTERWORLD

THE VOICE OF IT MANAGEMENT

## News

### Banks want lax customers liable for Internet fraud

Code of Conduct under review

Sandra Rossi 19/01/2007 18:14:05

Australian banks...  
Transfer (E...  
The financi...  
activity can...  
Today, the...  
very real th...

- Australian annual bank losses to cyber fraud: A\$25 million
- US annual bank losses to cyber fraud: \$250 - \$300 million

BW Online | August 9, 2004 | Gambling Sites, This Is A Holdup - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print

Address http://www.businessweek.com/.../magazine/content/04\_32/03095106\_10063.htm

Google bing sites cyber extortion Search Web PageRank 2598 blocked

**BusinessWeek online**

BW HOME | BW MAGAZINE | TOP NEWS | INVESTING | GLOBAL BIZ | TECHNOLOGY | SMALL BIZ | B-SIDE

AUGUST 9, 2004 - Edition: N. America | Europe | Asia | Edition Preferences

Customer Service Register  
Subscribe to BW  
Get Four Free Issues

Full Table of Contents  
Cover Story  
International Cover Story  
Up Front  
The Great Innovator  
Reader Report  
Commentary & Clarifications  
Books  
Technology & You  
Economic Viewpoint  
Business Outlook

Subscribe to Soundview

**INFORMATION TECHNOLOGY**

### Gambling Sites, This Is A Holdup

Organized criminal hackers threaten to paralyze their networks if they don't pay up

Something nasty was up. It was an autumn afternoon in the offshore gambling haven of Costa Rica. The banks of computers at online bookmaker Betcris.com whirled away, processing thousands of bets on the Cowboys, Patriots, and Buckeyes. All at once a flood of blank incoming messages inundated the computers, slowing traffic to a crawl. Within hours, the manager of Betcris.com, Mickey Richardson, received a threatening e-mail. The English was broken, but the message was clear: What he had experienced was a mere taste of a massive denial-of-service attack. If he wanted his computers to stay up and running through the football season, he was to wire a total of \$40,000 to 10 different accounts in Eastern Europe.

**STORY TOOLS**

- Printer Friendly Version
- E-Mail This Story

**RELATED ITEMS**

Graphic: Extortion At Online Casinos in Three Easy Steps

Address http://www.aastrom.com/



# Aastrom

Biosciences, Inc.

Corporate Information | Product Pipeline | Business Strategy | Investment Info | Contact Us

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

[Back to News Releases](#)

**Ann Arbor, Michigan, February 17, 2007** - AASTROM BIOSCIENCES, INC. (NASDAQ: AAST) today reported that its website has been corrupted by sabotage. A fallacious announcement was posted on the AASTROM website, apparently by a computer hacker. Aastrom stated that there is no truth in the announcement. The Company has alerted Nasdaq authorities and Geron to the violation and is investigating further.

"Denies fallacious press release" on their own website

"We are appalled by this ruthless attempt to manipulate markets and potentially harm the share companies," said R. Douglas Armstrong, President and CEO of Aastrom. "While we have no idea how this currently investigating the security of the website. In the meantime, we apologize to our shareholders for..."



# The first face of cyber crime



**Alexey  
Ivanov**



**Vasiliy  
Gorshkov**

- Stole data from ecommerce sites that used Microsoft IIS
- Threatened to disclose customers' credit card data
- Did disclose when the first victim refused
- \$160,000 dollars each instance
- “They threatened to killed my parents”

# Plus two more we will cover shortly



- Terrorists who use the techniques pioneered by organized crime
- Nation states that will spend any amount of money to control US computers and steal sensitive information.

# What Are the Greatest Cyber Menaces of 2008?



## **THEMES:**

- 1. VICTIMS BEING ATTACKED WHILE DOING WHAT THEY SHOULD BE DOING**
- 2. BLENDED ATTACKS**
- 3. AUTOMATION**
- 4. SOPHISTICATION AND HUGE BUDGETS**



# How Do We Know? SANS is...



- **Largest security training & education organization**
  - 85,000 alumni, 15,000 students per year
  - 60+ network security, app security and secure coding courses; 150+ events annually
- **Licensed, degree granting graduate education institution**
- **GIAC is an ANSI-accredited certification body**
  - More than 22,000 technical security certifications
- **Internet Storm Center – early warning for the Internet – 24 x 7**
- **Instructors are top guns in information and application security**
  - Information Warfare Officer – Ballistic Missile Defense Org
  - Chief Info Security Mgr – Naval Surface Warfare Center
  - Technical Director, JTF-CNO (now GNO)
  - CIA Red Team Leader
  - Director of Communications Infrastructure Protection, National Security Council
  - Ed Skoudis, Marc Sachs, Eric Cole, Steve Northcutt, Tom Liston, Josh Wright, more.

# Top 5 Cyber Menaces of 2008



- 5. SUPPLY CHAIN ATTACKS**
- 4. VOIP & TARGETED GROUP PHISHING**
- 3. WEB APPLICATION ATTACKS**
- 2. CYBER ESPIONAGE ADVANCES**
- 1. SOPHISTICATED BROWSER ATTACKS**

# 5. Supply Chain Attacks



The screenshot shows a news article on the SFGate.com website. The article is titled "Malware's new infection route: photo frames" and is written by Deborah Gage, a Chronicle Staff Writer, dated Saturday, January 26, 2008. The article discusses a malware attack on a digital photo frame. The text reads: "It wasn't a pretty picture when Rick Sandy plugged in the digital photo frame his wife had given him for Christmas. When he started downloading pictures to the device, his computer froze. He restarted it, and his Norton anti-virus software went blank. Then, the files that controlled his computer disappeared. And Sandy - an information technology expert himself - was shut out of his own machine. 'It was the nastiest virus I've ever encountered,' said Sandy, who spent 12 hours rebuilding his computer." A small image of a digital photo frame is visible on the right side of the article.

- Digital picture frames infecting buyers' systems
- Thumb drives and CDs at conferences infected
- And it is spreading. "I got a present of a set of MP3 playing sunglasses for Christmas that came with an extra gift, infection, AVG called it PSW.OnlineGames. It was a hidden .scr file with a hidden Autorun.inf file ." Company said "Seems something went wrong in China during Quality Control checks."

# 4. Phishing+: Blended VoIP Phishing and Targeted Group Phishing



- **VOIP Phishing**
  - Inbound email, apparently from credit card company,
  - Asks recipients to "re-authorize" credit card by calling a 1-800 number.
  - Number leads (via VoIP) to an automated system in a foreign country that, quite convincingly, asks that they key in their credit card number, CVV, and expiration date.
- **Targeted Group Phishing**

# News Blog

Recent posts on technology, trends, and more

October 1, 2007 12:23 PM PDT

## Phishing e-mails drive FTC chief 'insane'

Posted by Anne Broache

WASHINGTON--If your in-box is pelted by a seemingly ever-growing supply of inquisitive e-mails purporting to come from the likes of PayPal and Bank of America, the federal agency charged with consumer protection says it feels your pain.



FTC Chairman Deborah Majoras

The deceptive technique--in which crooks dispatch e-mails requesting sensitive personal information, typically by masquerading as financial institutions--"is one practice that absolutely drives me insane," Federal Trade Commission Chairman Deborah Platt Majoras told attendees at the first National Cybersecurity Awareness Summit, which was put on here Monday by a nonprofit partnership of federal government agencies and software vendors.

That's because phishing, more so than some other forms of cyber malice, is a prime example of a tactic that would all but evaporate if more consumers were better informed of what to look out for, she suggested. (After all, it's also an only slightly higher-tech variant of one of the oldest scams in the book--the "ph" comes from the original telephone-based variety of phony information-seeking.)

"I feel like if we could just teach every consumer what this means, never respond to that kind of contact, and train them to hit delete and not reply, we could clear this up," she said.

To that end, the agency is concocting a new video to supply "important information about phishing" and plotting other ways to "revitalize consumer education efforts," Majoras said. Working with the financial sector to spread the word will be critical because the messages so often rely on confusing consumers with the real thing, she added.

Attempting to go after the enterprising e-mailers in court will play some role, too. Majoras said



Advertisement

**Apply now: www**  
DC Public Schools is looking for a record of success in making schools

washingtonpost.com > Technology

[Subscribe to The Post](#)

### RECENT POSTS

- Targeted Attacks Use Unpatched Excel Flaw
- Scareware Program Targets Mac Users
- Safeguarding Your Passwords
- Report: TSA Site Exposed Travelers To ID Theft
- Barbara Moratek Is Not Your Friend

### Stories by Category

- Fraud
- From the Bunker
- Warning Warnings
- News
- Piracy
- Safety Tips
- U.S. Government

Stories By Date  
• Full Story Archive

### RELATED LINKS

- The Archives
- Security Fix Live: Web Chats
- About This Blog
- Password Primer
- 7 Security Tips
- Technology Section

### SYNDICATE

[RSS Feed](#)

**SECURITY FIX**  
Brian Krebs on Computer Security

[About This Blog](#) | [Archives](#) | [XML RSS Feed](#) (What's RSS?)

## Salesforce.com Acknowledges Data Loss

Business software provider **Salesforce.com** acknowledged that a recent spate of targeted e-mail virus and phishing attacks against its customers resulted from one of its own employees falling for a phishing scam and turning over the keys to the company's customer database.

On Oct. 19, Security Fix reported that payroll giant **Automatic Data Processing (ADP)** and several banks -- including **Suntrust** -- were among a number of institutions that were victimized by [a series of highly-targeted phishing scams](#) that addresses recipients by name and asked them to click on a link - which tried to download password-stealing malicious software. A Suntrust executive alleged that the scammers obtained their list of Suntrust customers via a data compromise at Salesforce.com.

A Salesforce.com executive would not answer direct questions about the incident at the time. Salesforce.com data also was implicated in [a pair of targeted malware attacks](#) that appeared to have been sent from the **Federal Trade Commission**, an attack that installed password-stealing software on PCs of more than 500 victims.

Now, in [an e-mail](#) sent Monday to nearly a million customers, Salesforce.com is finally owning up to a data loss.

"We learned that a salesforce.com employee had been the victim of a phishing scam that allowed a salesforce.com customer contact list to be copied," the company wrote. "Information in the contact list

# Salesforce.com owns up



- *"We learned that a salesforce.com employee had been the victim of a phishing scam that allowed a salesforce.com customer contact list to be copied," the company wrote. "Information in the contact list included first and last names, company names, email addresses, telephone numbers of salesforce.com customers, and related administrative data belonging to salesforce.com.*
- *As a result of this, a small number of our customers began receiving bogus emails that looked like salesforce.com invoices, but were not--they were also phishes. Unfortunately, a very small number of our customers who were contacted had end users that revealed their passwords to the phisher."*
- *However, a few days ago a new wave of phishing attempts that included attached malware--software that secretly installs viruses or key loggers--appeared and seemed to be targeted at a broader group of customers." (QUIZ: How did the phishing install a keylogger?)*

# Executives: Targeted FTC Scam



- Hackers compromise Salesforce.com customer database (mostly business managers)
- Each customer gets email “from the FTC” saying that there is a complaint lodged against their firm; “respond to attached letter within xx days”
- Site where they visit has a series of exploits that infect their systems
- Their computers become zombies; keystroke logger installed

# More sophistication: The Tax Refund Scam



- Criminals buy Google ads to draw victims; “Maximize your refund.”
- Appears official
- Victim completes the form with all needed data
- Criminals submit the data but change the address for the refund; cash the check
- Fully automated!!!



# Why all this cyber crime matters



- Multiple al Qaeda speakers finish their talks with the directive:

“ Study the computer along with the Q’uOran; in that way we will bring America and its cronies to their knees.”

1. Bank fraud funds ended up in the account that pays for Iraqi terrorist bombs.
2. Imam Samudra, the “Bali bomber,” used computer fraud to raise money and wrote an amazingly good “how to” book to make Indonesian al Qaeda recruits into effective hackers.



# 3. Web application attacks: January: 87,000 web sites infected and infecting visitors who trusted them.

Are you getting paid  
what you're worth?

**COMPUTERWORLD**  
Networking & Internet



More Resources

SEARCH Google™ Custom Search GO

## Mass hack infects tens of thousands of sites

Then they serve visitors multiple exploits, including October RealPlayer attack

Gregg Keizer [Today's Top Stories](#) or [Other Networking and Internet Stories](#)

Comments (8)  Recommendations: 141 — [Recommend this article](#)

**January 07, 2008** (Computerworld) -- Tens of thousands of Web sites have been compromised by an automated SQL injection attack, and although some have been cleaned, others continue to serve visitors a malicious script that tries to hijack their PCs using multiple exploits, security experts said this weekend.

Roger Thompson, the chief research officer at Grisoft SRO, pointed out that the hacked sites could be found via a simple [Google](#) search for the domain that hosted the malicious JavaScript. On Saturday, said Thompson, the number of sites that had fallen victim to the attack numbered more than 70,000. "This was a pretty good mass hack," said Thompson, in a [post](#) to his blog. "It wasn't just that they got into a server farm, as the victims were quite diverse, with presumably the only common point being whatever vulnerability they all shared."

Symantec Corp. cited reports by other researchers -- including one identified only as "websmithrob" -- that fingered a SQL vulnerability as the common thread. "The sites [were] hacked by hacking robot by means of a SQL injection attack, which executes an iterative SQL loop [that] finds every normal table in the database by looking in the sysobjects table and then appends



### MORE RELATED CONTENT

- [FAQ: Why is enterprise search harder than Google Web search?](#)
- [Old exploit keeps on tickin' for hackers](#)
- [Office, Windows Server chief Jeff Raikes to retire from Microsoft](#)

### TODAY'S TOP STORIES

- [Macworld forecast: Thin, light notebook 'sure bet'](#)
- [Microsoft changes mind, goes public with Vista SP1 refresh](#)

# Why Are Applications A New Target?

- System software has become more secure
- Perimeter protection is tuned for system attacks
- Attackers discovered applications are vulnerable:
  - Back-up products
  - Anti-virus products



**TECHWORLD**  
site-wide navigation

- News
- Insight
- How-to's
- White papers
- Case studies
- Briefings
- Interviews
- Reviews
- Blogs
- Forums
- Topic Pages

Networking Storage Security

Home | [News](#) | [Insight](#) | [How-tos](#) | [Case studies](#)

The Online Home of: **CRN** **Business** **Government**

**ChannelWeb** NETWORK

News Reviews Research Tools

## Hackers Keep Sniffing For Buggy Veritas Backup Software

By TechWeb News  
2:19 PM EDT Thu. Aug. 11, 2005

Attackers are scanning for system running the vulnerable Veritas Backup Exec software, Symantec customers of its DeepSight Threat Management system Thursday.

In late June, Veritas released a slew of security advisories warning customers that its backup software was vulnerable to attack. Shortly after, [Symantec noted a spike](#) in scanning for one of the ports used by the software.

**COMPUTER & INTERNET SECURITY NEWS**  
31 May 2007

### F-Secure's antivirus lets in hackers

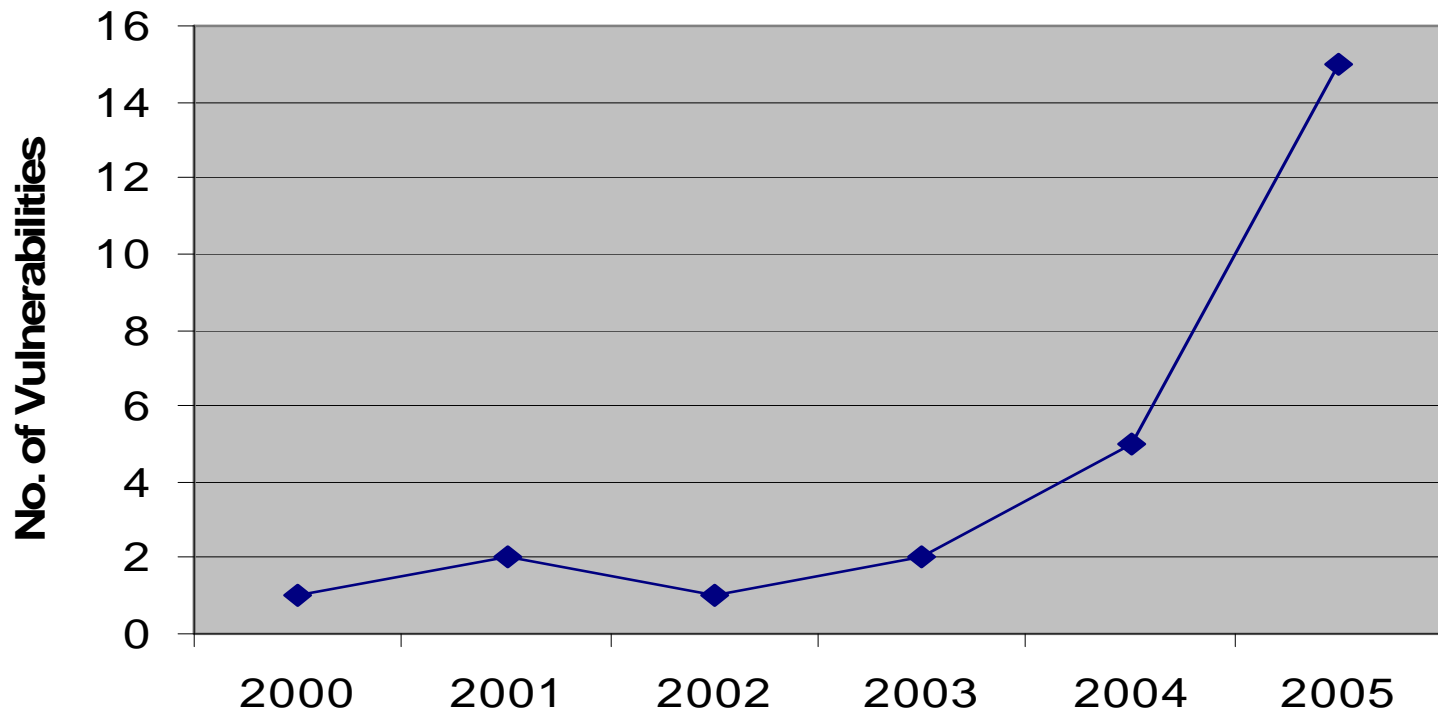
By Robert McMillan. IDG News Service

F-Secure has patched several vulnerabilities in its security products, the most critical of which could be used to run unauthorised software on a victim's computer.

# Symantec Backup Vulnerabilities



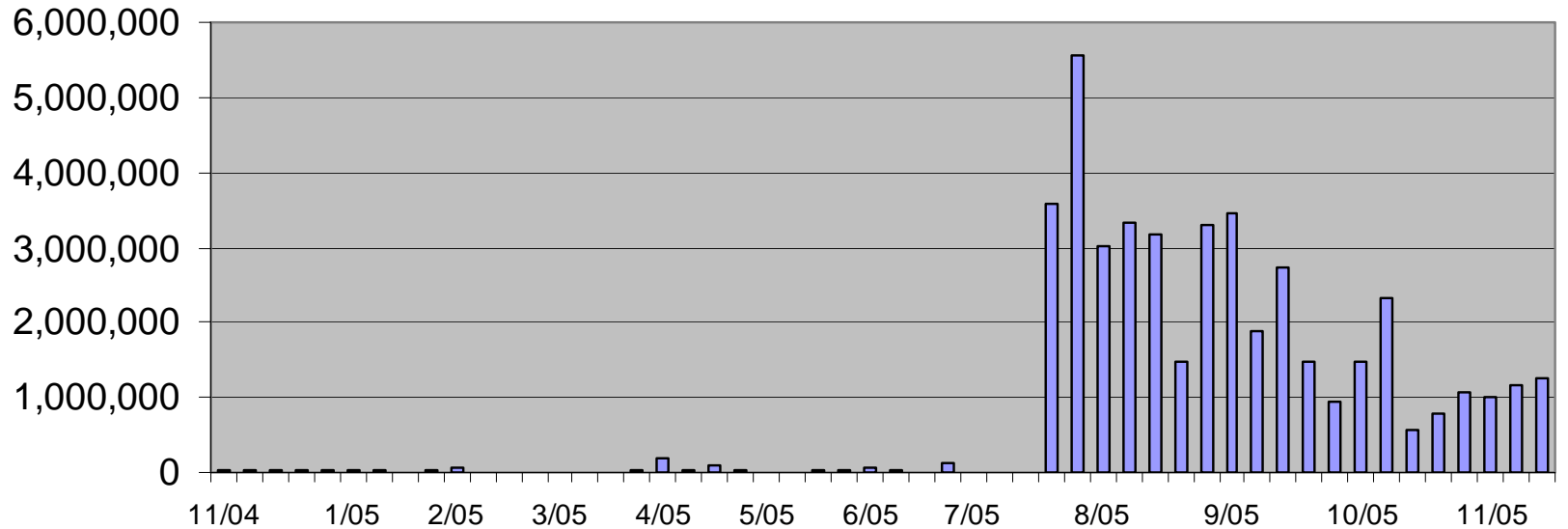
## Veritas Vulnerabilities



# Attacks against Symantec BackUp



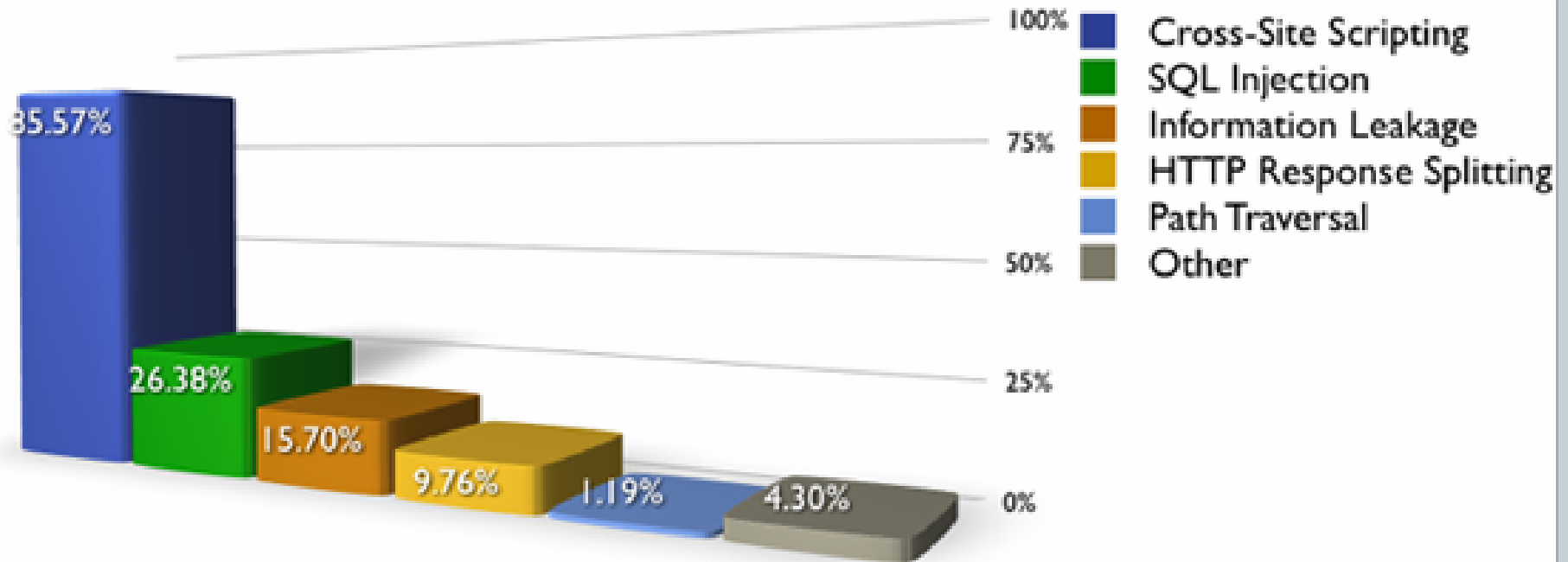
## Number of Packets Targeting BackUpExec Port 10000



# Web Applications: How Vulnerable?

## 2006 Vulnerability Statistics (31,373 sites)

Percentage of websites vulnerable by class (Top 5)



\*\* <http://www.webappsec.org/projects/statistics/>

## 2. Nation states attack military and civilian government sites



- Time magazine (09/05) Massive penetration of DoD
- Congressional hearings (07): State Department and Commerce Department
- Director of National Intelligence (2/5/08 Senate Select Committee on Intelligence)
  - Our information infrastructure is being targeted for exploitation and potentially for disruption or destruction. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious.
  - Russia and China have the technical capabilities to target and disrupt elements of the US information infrastructure and for intelligence collection. Nation states and criminals target our government and private sector information networks to gain competitive advantage in the commercial sector.
  - Terrorist groups-including al-Qa'ida, HAMAS, and Hizballah-have expressed the desire to use cyber means to target the United States.
  - Criminal elements continue to show growing sophistication in technical capability and targeting, and today operate a pervasive, mature on-line service economy in illicit cyber capabilities and services available to anyone willing to pay.

# Major General William Lord



“China has downloaded 10 to 20 terabytes of data from the NIPRNet”

“They’re looking for your identity so they can get into the network as you,”

“There is a nation-state threat by the Chinese.”

Maj. Gen. William Lord, director of information, services and integration in the Air Force’s Office of Warfighting Integration and Chief Information Officer

*8/21/06 Government Computer News, “Red Storm Rising”*



# How Damaging Are These Attacks?



From TIME Magazine, Sept. 5, 2005

“They hit hundreds of computers that night and morning alone

- “At 10:23 p.m. PST, they found vulnerabilities at the U.S. Army Information Systems Engineering Command at Fort Huachuca.
- “At 1:19 am PST, they found the same hole in computers at DISA in Arlington, Virginia.
- “At 3:25 am, the Naval Ocean Systems Center, a defense department installation in San Diego.
- “At 4:46 am PST, the United States Army Space and Strategic Defense installation in Huntsville, AL.”
- Counterpoint: “They didn’t get any classified data...”
- “from Redstone Arsenal, Army Aviation and Missile Command: they got the specs for the aviation-mission-planning system for Army helicopters, as well as Falconview 3.2, the flight-planning software used by the Army and Air Force.”

# The Third Face of Cybercrime



- 20 workstations in Guong Dong province
- 24 hours a day, 7 days a week
- Massive penetration and theft from DoD, contractors, and others in the US and allies
- PLA Doctrine: “The next war with the United States will be fought asymmetrically”



# Expanding to economic espionage



- Companies negotiating deals with people in China
- Chinese government penetrates the companies' computers, steals documents, and leaves back doors.
- They also penetrate accountants, lawyers and consultants computers.
- China's negotiators have the benefit of knowing exactly what the companies are willing to give.

# 1. Sophisticated Browser Attacks



- Targets trusted web sites
- Uses web app or system vulnerability
- Installs much more sophisticated infection tool
- Infection tool exploits apps (ex: Flash or QuickTime)  
–not automatically updated with browser updates
- Fools user twice: (1) trusted site and (2) unpatched web browser service.
- Victims subjected to financial fraud, and creates enough zombies to take down \*any\* site or to send billions of spam messages or “pump&dump.”

# Top 5 Cyber Menaces of 2008



- 5. SUPPLY CHAIN ATTACKS**
- 4. VOIP & TARGETED GROUP PHISHING**
- 3. WEB APPLICATION ATTACKS**
- 2. CYBER ESPIONAGE ADVANCES**
- 1. SOPHISTICATED BROWSER ATTACKS**

# Three Initiatives to Deter Attacks



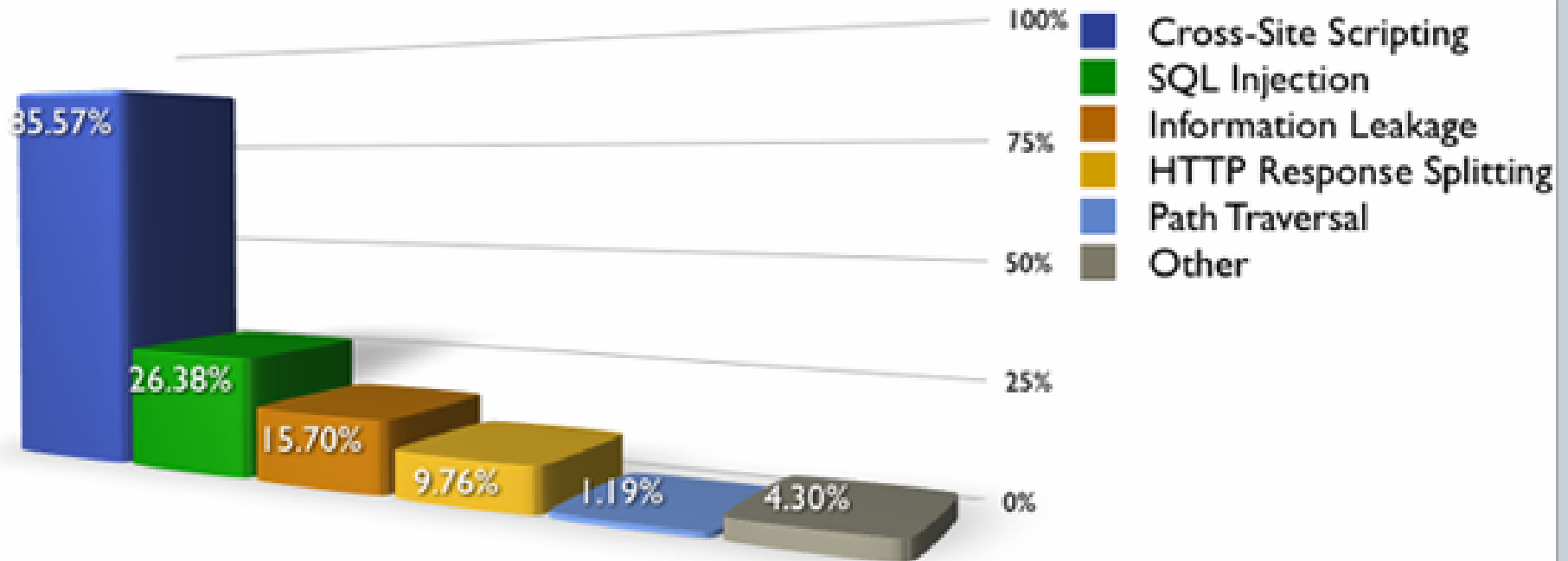
**WHERE YOU CAN MAKE A DIFFERENCE AND WHERE THE BIGGEST  
NEW PROFESSIONAL DEVELOPMENT OPPORTUNITIES WILL BE  
FOUND**

- 1. APPLICATION SECURITY**
- 2. CONFIGURATION & PATCH AUTOMATION**
- 3. FORENSICS – FINDING THE PERSISTENT PRESENCE**

# Web Applications: How Vulnerable?

## 2006 Vulnerability Statistics (31,373 sites)

Percentage of websites vulnerable by class (Top 5)



\*\* <http://www.webappsec.org/projects/statistics/>

# Making Applications More Secure



- Application security firewalls
- Application security scanners
- Source code analyzers (binary too)
- Application penetration testing
- Assessing programmers' security skills
  - **C and Java now; .NET and PHP and Perl soon**



# A test of secure programming skills and knowledge, not book learning



Consider the following program:

```
1.  #include <stdio.h>
2.  #include <string.h>
3.  void usage(char *ptCommand) {
4.  char usageInfo[1023];
5.      snprintf(usageInfo, 1023, "Usage: %s \n", ptCommand);
6.      printf(usageInfo);
7.  }
8.  int main(int argc, char * argv[]) {
9.      if (argc < 2)
10.         usage(argv[0]);
11. }
```

Q1. If in the above code `argv[0]` may be provided by a malicious user, what security problem can the code have?

- A. Format string vulnerability
- B. Out-of-bound array write
- C. String null-termination error
- D. String truncation

- The candidate is asked to find the best answer

# How are the tests to be used?



More than 400 organizations

- 83.7% said To identify our programmers' secure programming gaps and fill them
- 62.1% said To ensure consultants and vendors have security-skilled programmers
- 60.1% said To evaluate programming candidates.
- 57.4% said To select people with secure programming skills for critical projects.
- 44.1% said To persuade universities to ensure CS graduates know secure coding.
- 38.9% said To help give our customer confidence that we are delivering products that include code written by certified secure programmers.

# How people will take the tests



- **Assessments online – enterprise partners**
  - **(A-D) ABN AMRO, Amazon, American Express, AT&T, Boeing, Caremark, Carlson, CIBC, Cingular, Cisco, Depository etc. (International: Tata, Siemens, NRI)**
    - **Sometimes customized.**
- **GSSP certification on paper**
  - **Proctored paper exams two or three times a year – many locations**
  - **Colleges and universities: teaching programmers secure coding skills; researching new techniques for teaching secure coding; testing site for students and local businesses**

# It is working!



- Letter from one of the largest software companies to ten colleges where they hire most programmers – “teach the CS graduates to write secure code; use GSSP to ensure they have learned it, don’t make us to remedial training”
- Letter from one of the largest financial companies to outsourcers in India and China (5,000 total) “you must pass secure coding tests by next summer or you will not be allowed to touch any code.”

# Teaching Secure Coding Practices: Lessons Learned



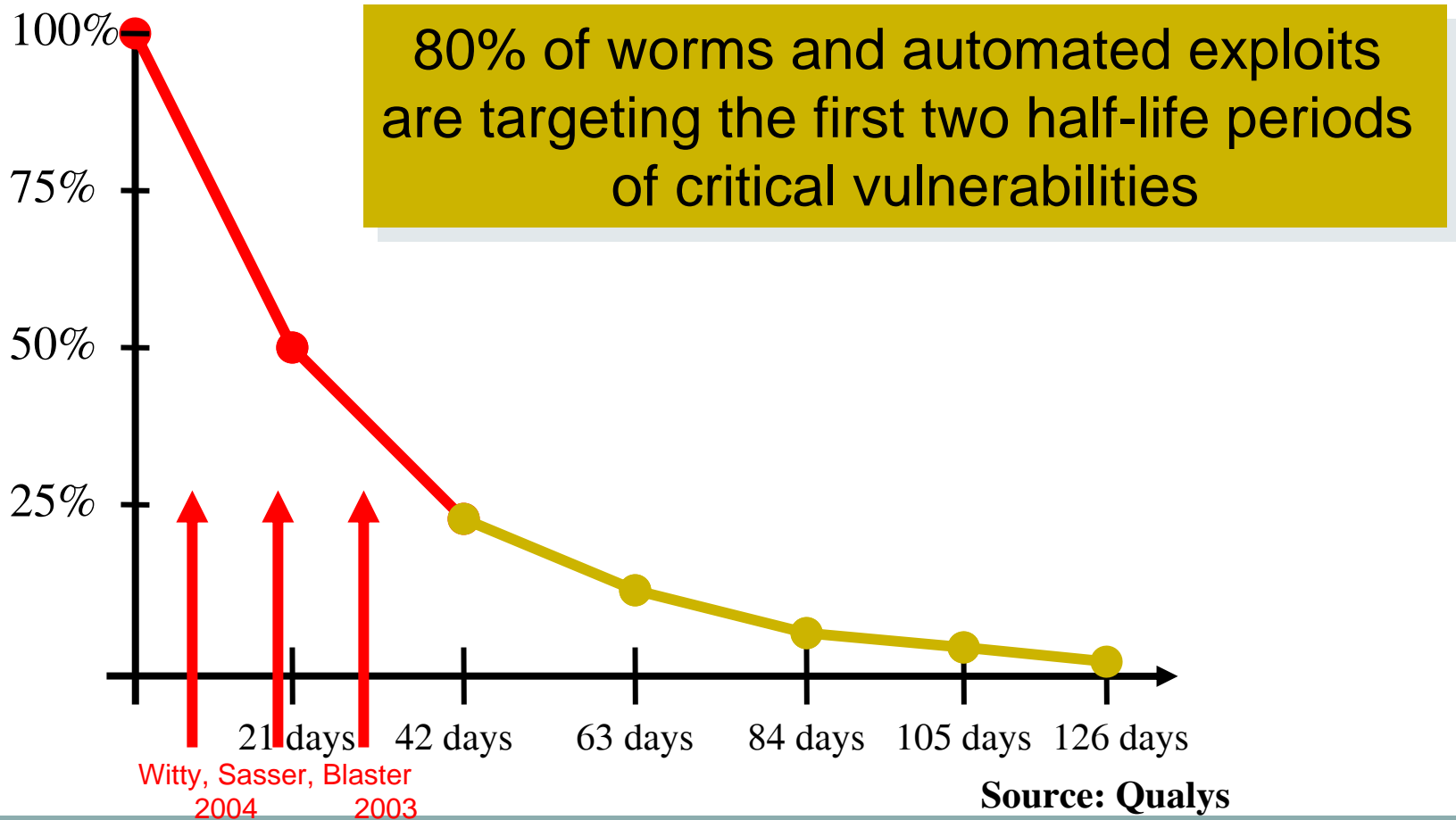
- Colleges
  - Faculty reluctance
  - The mentor program
- Enterprises
  - Relationship between security staff and programmers
  - Awareness
  - Assessment
  - Courses
- [www.sans.org/gssp](http://www.sans.org/gssp)

# Patching Is broken



- Exploits arrive before patches are installed (caused major defense agency penetrations)
- Why?
  - Applications force non-standard configurations
  - Patches must be tested on each non-standard configuration because untested patches can break applications
  - Vendors un-do security settings when they install patches
- Partial solution: common configurations that can be patched immediately

# The Impact of an Exploit



# Why all these problems?



- Applications force non-standard configurations
- Patches must be tested on each non-standard configuration because patches can break applications
- Vendors un-do security settings when they install patches



# The FDCC: Common Secure Configurations



- US Air Force – persuaded Microsoft to deliver Windows with security baked in (based on NSA/NIST/Air Force specs)
- Patch time reduced from 54 days to 72 hours
- White House now requires all agencies to use the consensus secure configuration and
- **The Big One:** White House requires all software vendors (and integrators) to certify software works on secure configuration without changing the configuration and without admin privileges.

# Vulnerabilities are coming too fast for human response



- Humans cannot do vulnerability testing fast enough or reliably enough
- Humans cannot determine whether test will break things because of special configuration requirements
- Humans do not know every version of every piece of software on every computers
- Humans cannot patch systems manually fast enough

# Key to S-CAP: DoD Procurement Power



- Software vendors deliver patches with S-CAP definitions
- Vulnerability testers use OVAL for testing; testing is identical across tools
- System managers use XCCDF for configuration definitions
- Patching tools know how to patch systems instantly
- Why would all those vendors do all that the development? DoD Procurement Power.

# The hardest problem leads to the biggest opportunity



**PERIMETERS ARE BEING PENETRATED**

# Bad guys are getting into well-protected systems?



**Spear Phishing** - Victims being attacked while doing what they should be doing

**What's wrong with this hypertext url?**

<http://www.microsoft.com/security>

# How Spear Phishing Destroys Your Perimeter



- An e-mail arrives from your commanding officer saying:

“ Microsoft has given us a heads-up about a major new vulnerability. They won't be making the patch public until tomorrow but have offered us early access to the patches. Before you leave work today go to the following Microsoft site and download the new patch

<http://www.microsoft.com/security/alert-windows.msp>



Search Microsoft.com for:



## Trustworthy Computing: Security

- Security Home
- Security Updates
- Recent Incidents
- Partners


### Information For

- Home Users
- IT Professionals (TechNet)
- Developers (MSDN)
- Small Businesses
- Worldwide Security Sites

### Trustworthy Computing

- Overview
- Privacy
- Reliability
- Business Integrity

**YOUR IT STAFF**



**IS ARMED AND READY**

GET SECURITY TOOLS AND TRAINING >

Microsoft

# Windows Security Update Summary for May 2005

Published: May 10, 2005

The security update for May 2005 is an important update for Microsoft Windows. If you have any of the software listed on this page installed on your computer, you should install the related update.



[Skip the details and get the updates now](#)

## Security Bulletin MS05-024

**Maximum severity:** Important ([What is maximum severity?](#))  
**Update number:** 894320 ([What is an update number?](#))  
**Supported software affected:**

- Windows 2000 Service Pack 3 (SP3) and

**Technical bulletin:** [Vulnerability in Windows 2000 Remote Code Execution \(894320\)](#)

### Check the Version

If you are not sure whether the software you are running is affected, check the version.

- [Get instructions for how to check](#)

### For More Information

Find support information about these security issues in the Microsoft Knowledge Base.

- [KB894320](#)

[↑ Top of page](#)

**Security Alerts**



Get e-mail or alerts about security updates

### Related Links

- [Technical Bulletins](#)
- [Software Life Cycle Support Information](#)
- [Security Bulletin FAQ](#)
- [How to Tell If a Security E-Mail Notice Is Really From Microsoft](#)
- [Protect Your PC](#)

**Why it went to the wrong place: html code was actually:**

`<a href="http://www.hackersite.com">http://www.microsoft.com/security/alert-windows.msp</a>`

**Would it have fooled anyone in your organization?**

# Then what happens?



- Malicious software causes the victim to make a legal web connection to a server controlled by the attackers.
- That server sends software and commands to control the now slave computer.
- Slave computer searches all other computers (note it is inside the firewall so it has access) and collects huge amounts of data.
- Slave computer compresses the data and sends it to a storage computer from which it is later moved to the attacker's systems.



# The hardest job – forensics to find the *persistent presence*



**THE PERIMETER IS POROUS.  
THE ENEMY IS ALREADY ON YOUR SYSTEMS.  
THE ENEMY IS INFECTING YOUR SUPPLY CHAIN.**

**THE TOP GUNS OF CYBER SECURITY IN THE NEXT FIVE  
YEARS WILL BE FORENSICS EXPERTS WHO FIND THE  
PERSISTENT PRESENCE AND WHO BUILD THE TOOLS  
OTHERS CAN USE TO FIND THEM**

# Questions?



- 1. THE THREE FACES OF CYBER CRIME – ORGANIZED CRIME, TERRORISTS, NATION STATES**
  - 2. THE MOST DAMAGING MENACES OF 2008**
  - 3. PROMISING PRACTICES: SECURE CODING ASSESSMENT AND CERT, FDCC, AND S-CAP.**
  - 4. STOPPING SPEAR PHISHING AND FINDING THE PERSISTENT PRESENCE**
-