



EMAGINED SECURITY



Global Threat Update

Dr. Eugene Schultz, CISSP, CISM

Chief Technology Officer

Emagined Security

EugeneSchultz@emagined.com

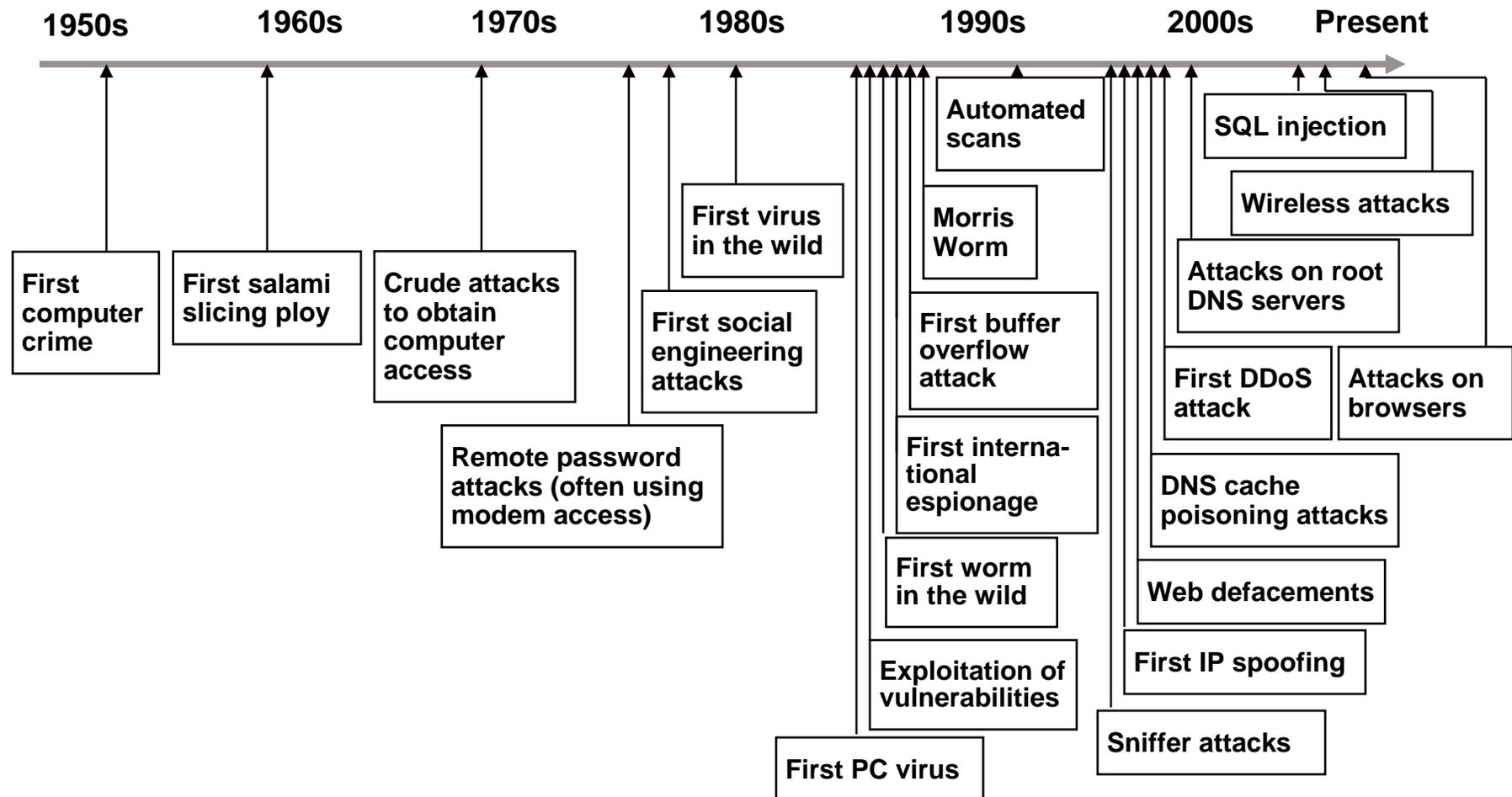
State of California

Sacramento, California CISO Lecture Series

September 30, 2009

- Introduction
- The nature of the threats
- Conclusion

Security threats—much change over time



Questions to be answered in this presentation



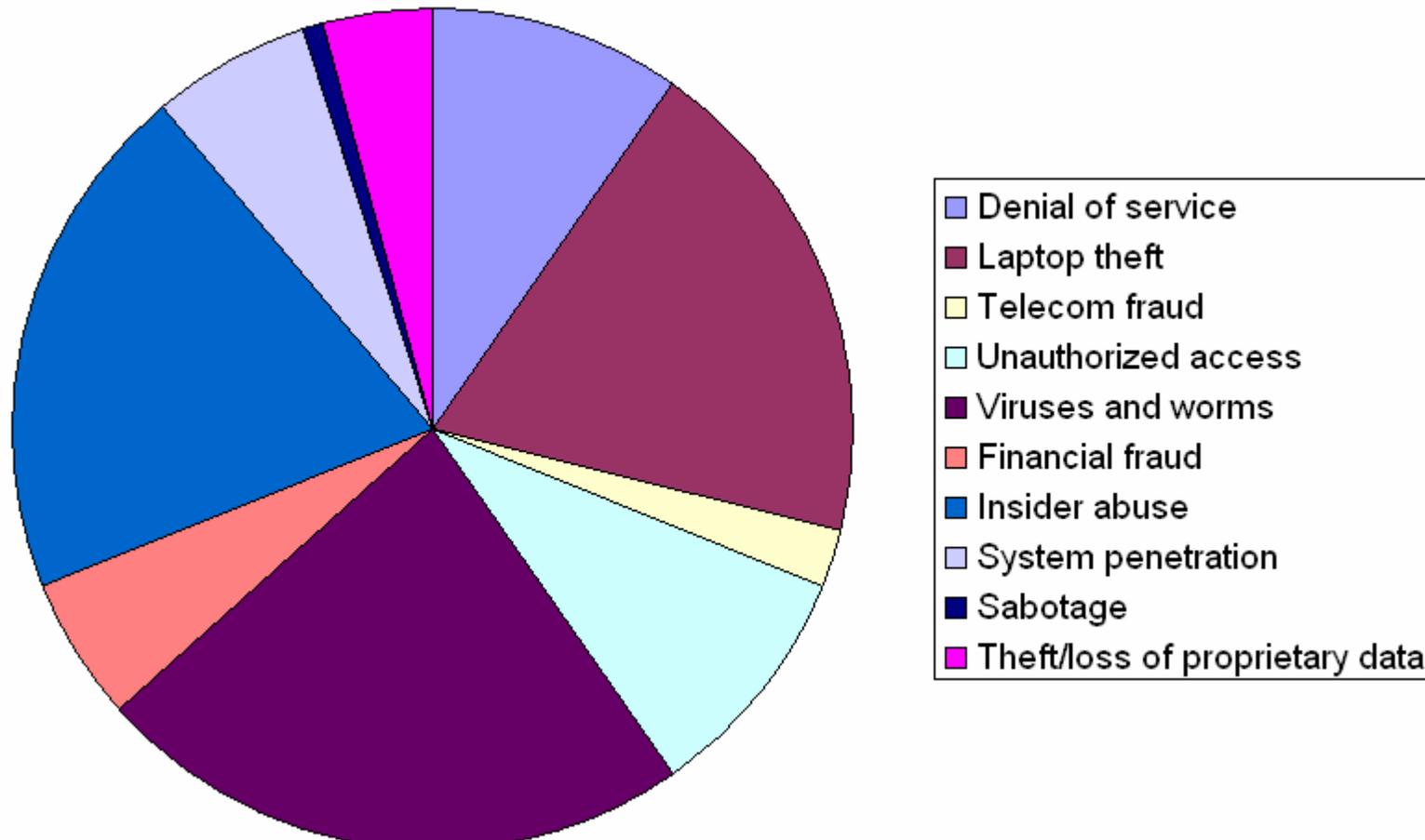
- What are the most prevalent security threats presently?
- How much risk is associated with each threat?
- How are threats changing?
- Which threats are most likely to be persistent over time?

Outline



- Introduction
- **The nature of the threats**
- Conclusion

FBI survey results: Types of incidents in 2008



Loss due to security incidents



- According to the Internet Crime Complaint Center (IC3), the cost of reported Internet security incidents has increased from approximately \$200 million in 2006 to approximately \$290 million in 2008

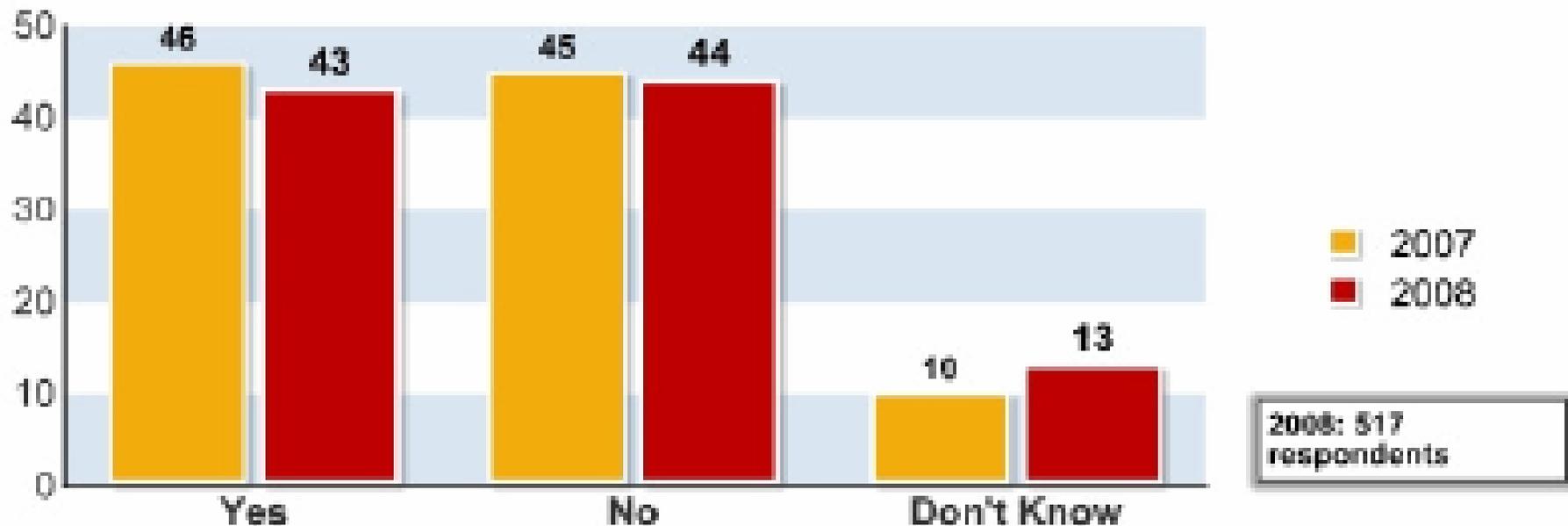


Example – Heartland Payment Systems

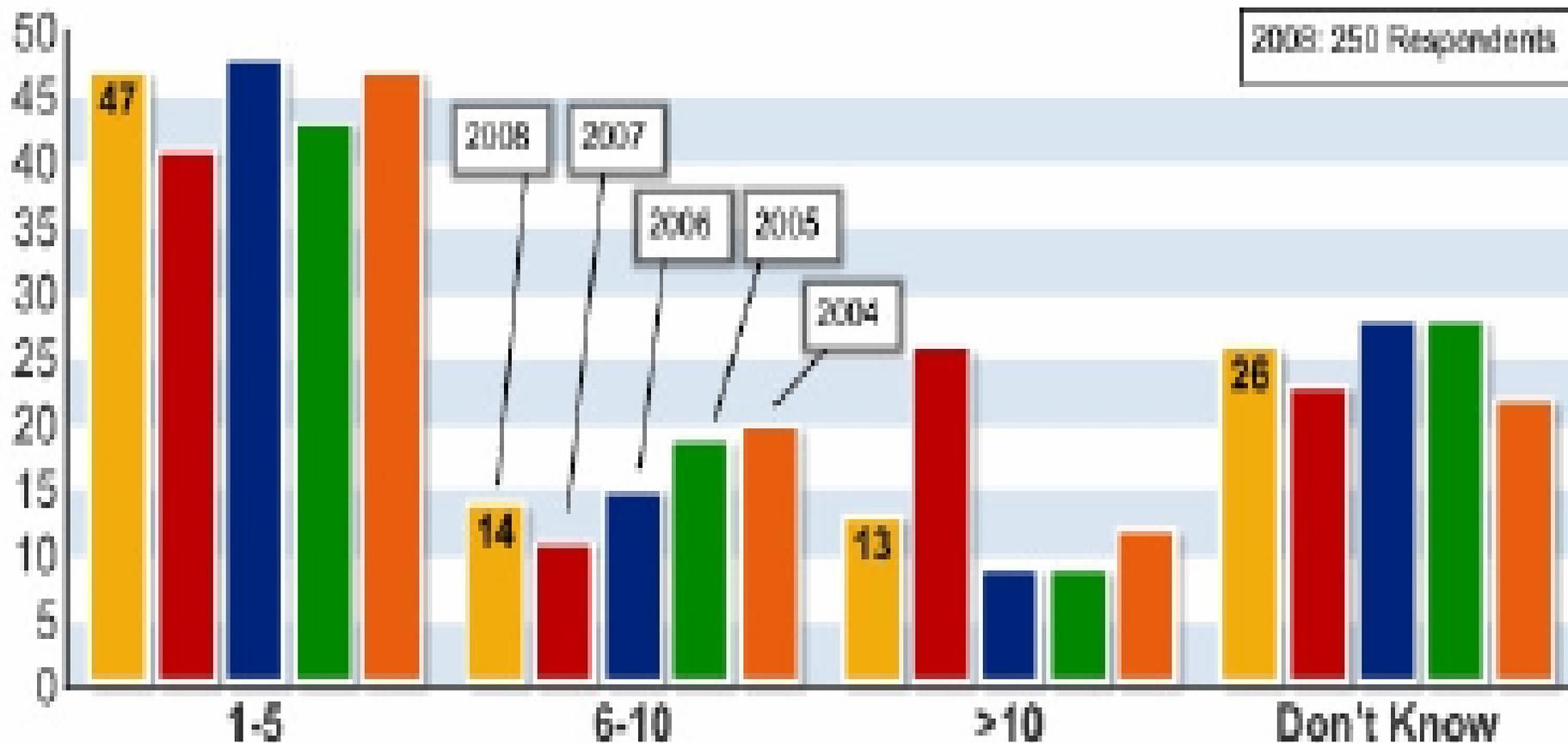


- Nearly 100 million credit cards from at least 650 financial services companies were compromised
- Digital information within the magnetic stripe on the back of credit and debit cards was copied by a keystroke logger
- Perpetrators created counterfeit credit cards
- Break-ins went undetected for nearly six months
- Visa temporarily declared Heartland to be PCI-DSS non-compliant
- Scores of lawsuits (including several class action suits) are pending

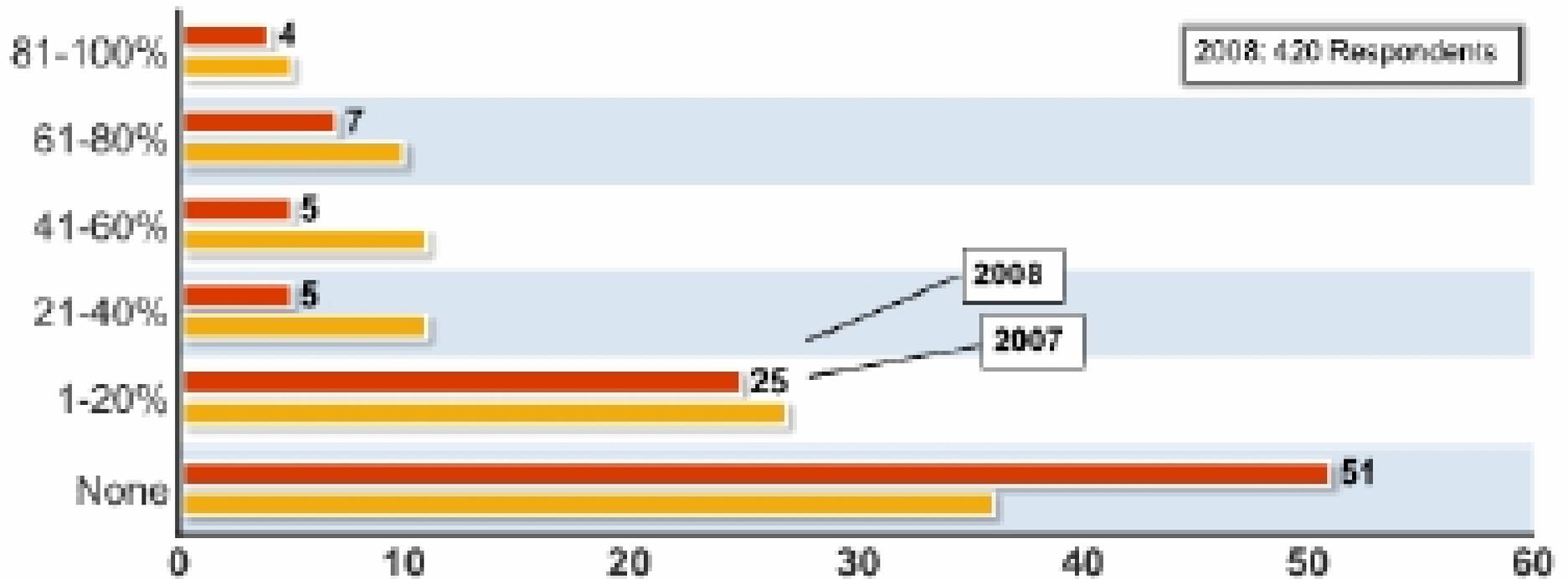
CSI 2008 Survey results—Did you have a security incident?



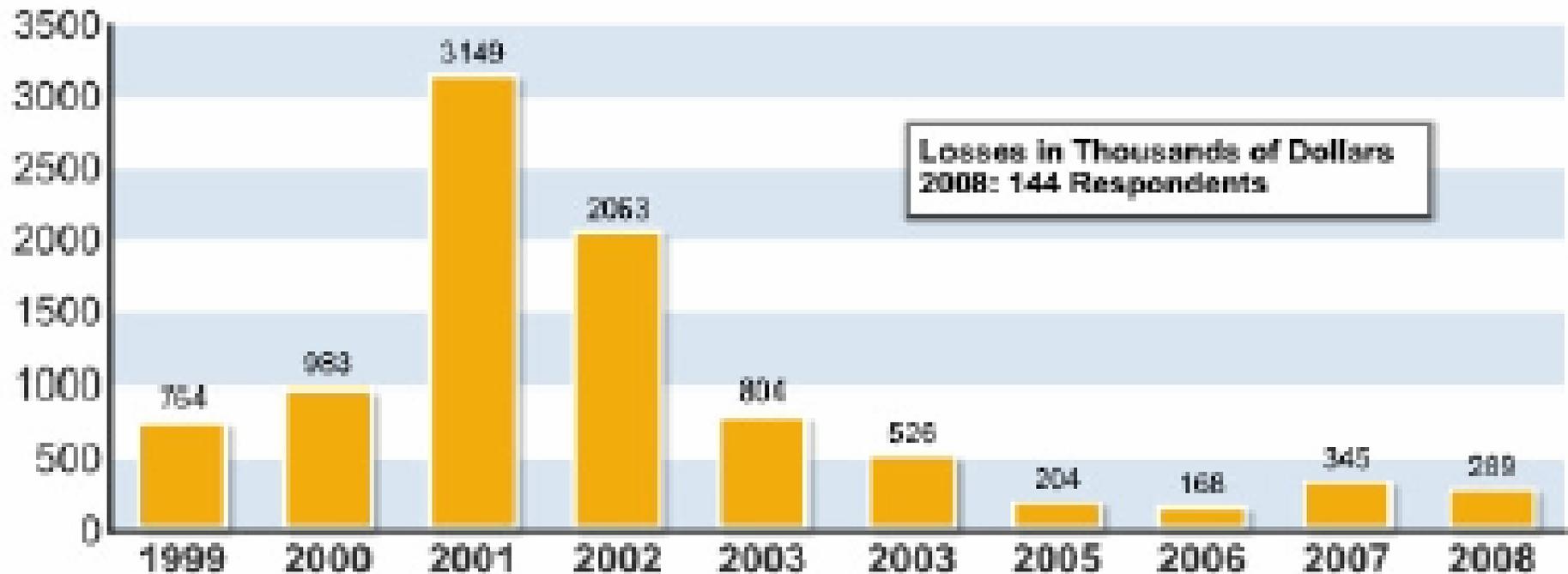
CSI 2008 Survey results—Number of incidents by percentage



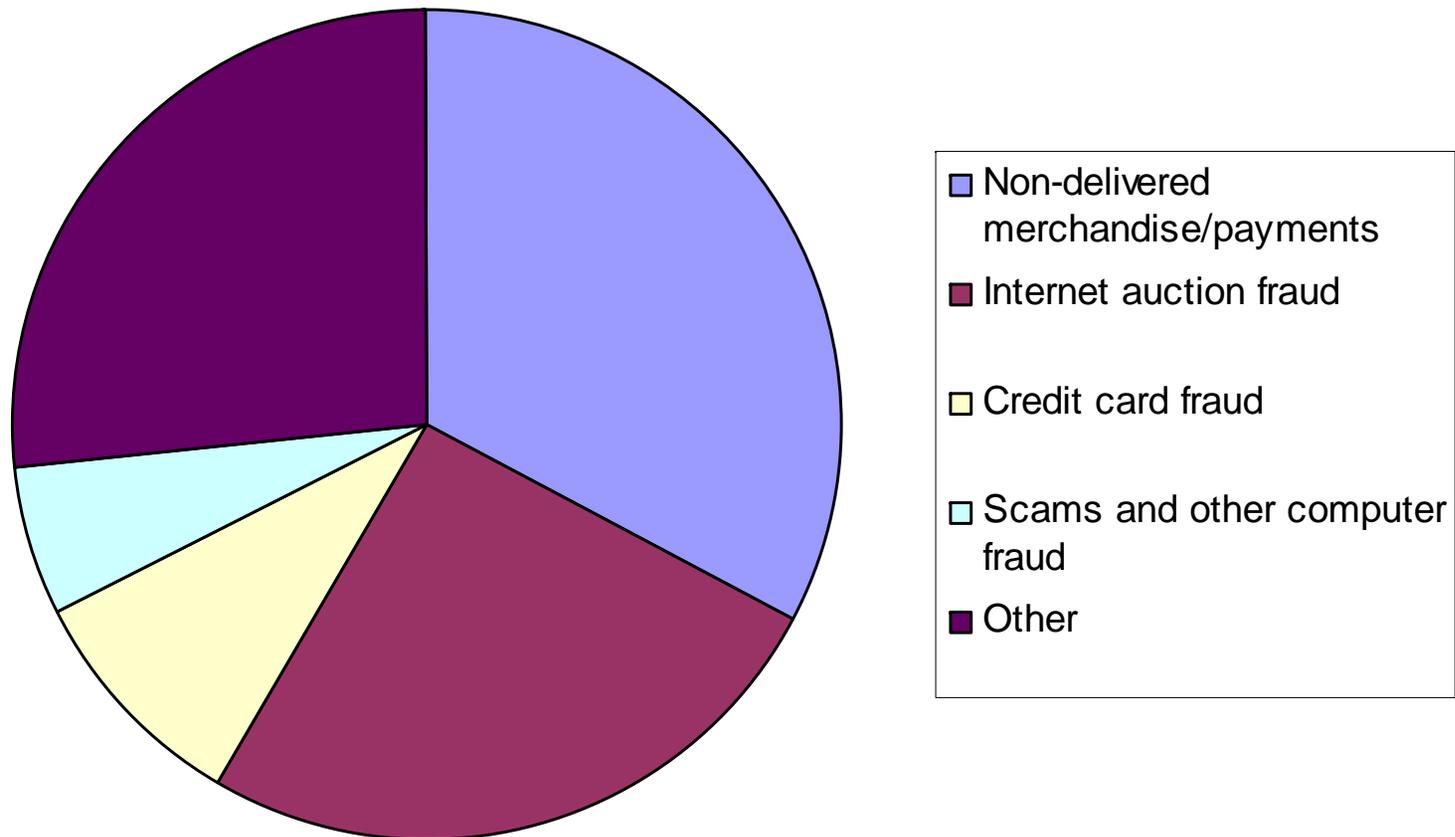
CSI 2008 Survey results—Percent of loss from insider attacks



CSI 2008 Survey results— Average loss per organization



Fraud statistics from 2008 FBI Survey



Users' PCs are most vulnerable



Unprotected PCs can be hijacked in minutes

By Byron Acohido and Jon Swartz, USA TODAY

SAN FRANCISCO — Surfing the Web has never been more risky.

Simply connecting to the Internet — and doing nothing else — exposes your PC to non-stop, automated break-in attempts by intruders looking to take control of your machine surreptitiously.

Shore up your cyberdefenses on these three cyberfronts

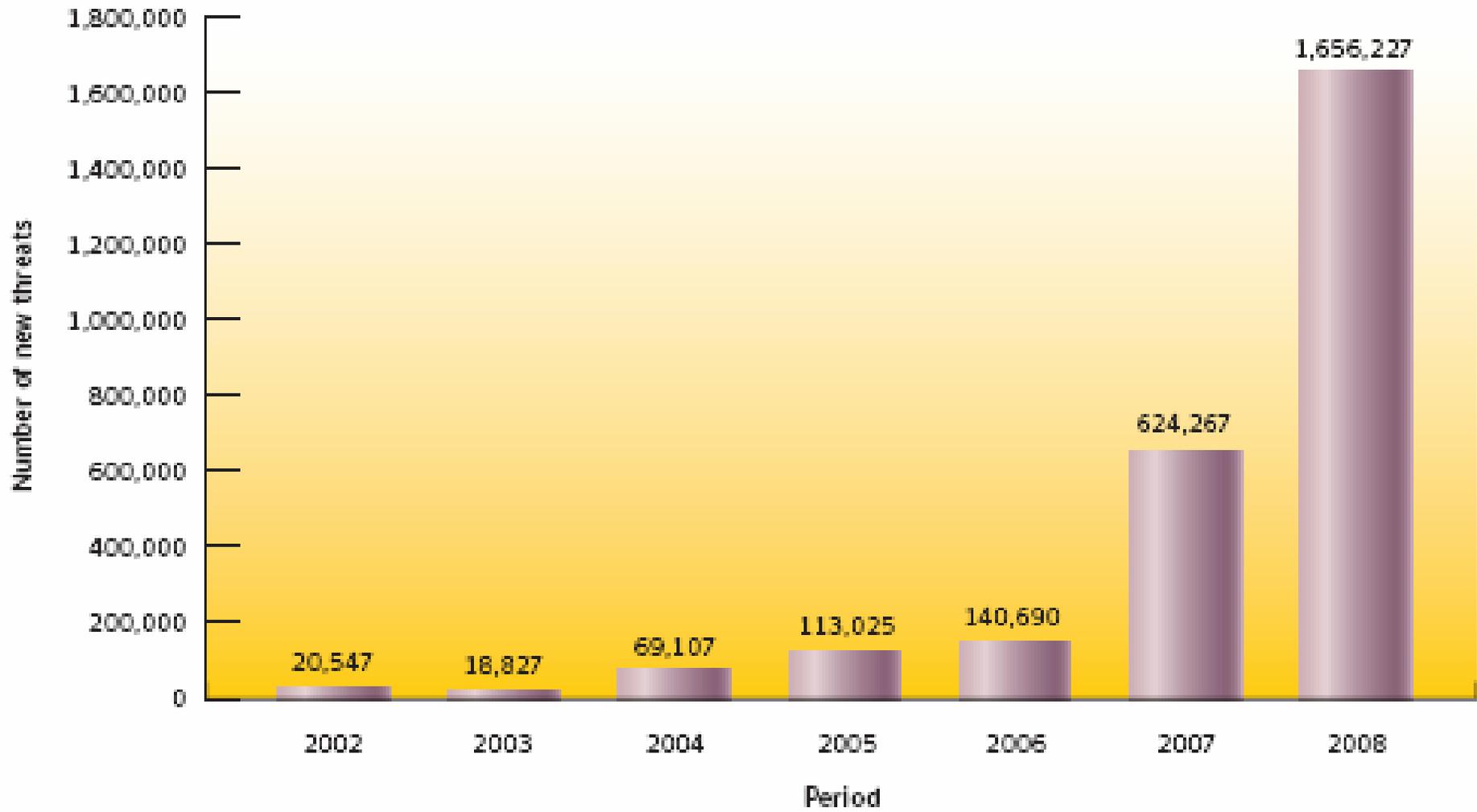
If an online intruder has infiltrated your Windows PC, you may notice recurring slowdowns of e-mail and Web browsing, or you may notice nothing at all. PC users must shore up defenses on three fronts:

• **Operating system vulnerabilities.** Always use a personal firewall and keep security patches up to date. As of early November, all new Windows XP PCs come with Service Pack 2, which includes a firewall and automatic patching. Owners of Windows XP PCs purchased earlier than that should download Service Pack 2 from

While most break-in tries fail, an unprotected PC can get hijacked within minutes of accessing the Internet. Once hijacked, it is likely to get grouped with other compromised PCs to dispense spam, conduct denial-of-service attacks or carry out identity-theft scams.

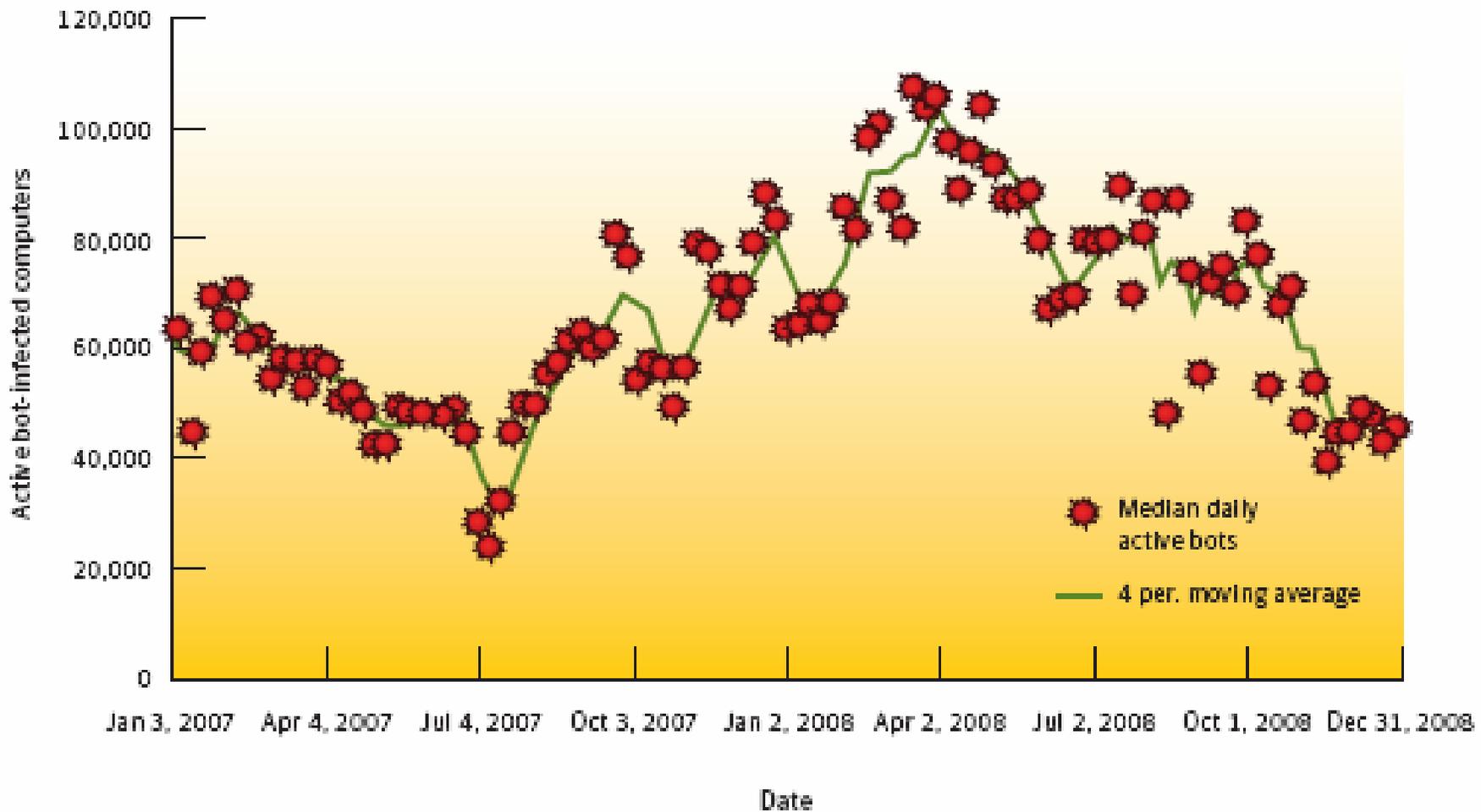
Those are key findings of a test conducted by USA TODAY and Avantgarde, a San Francisco tech

Symantec 2008 malware statistics

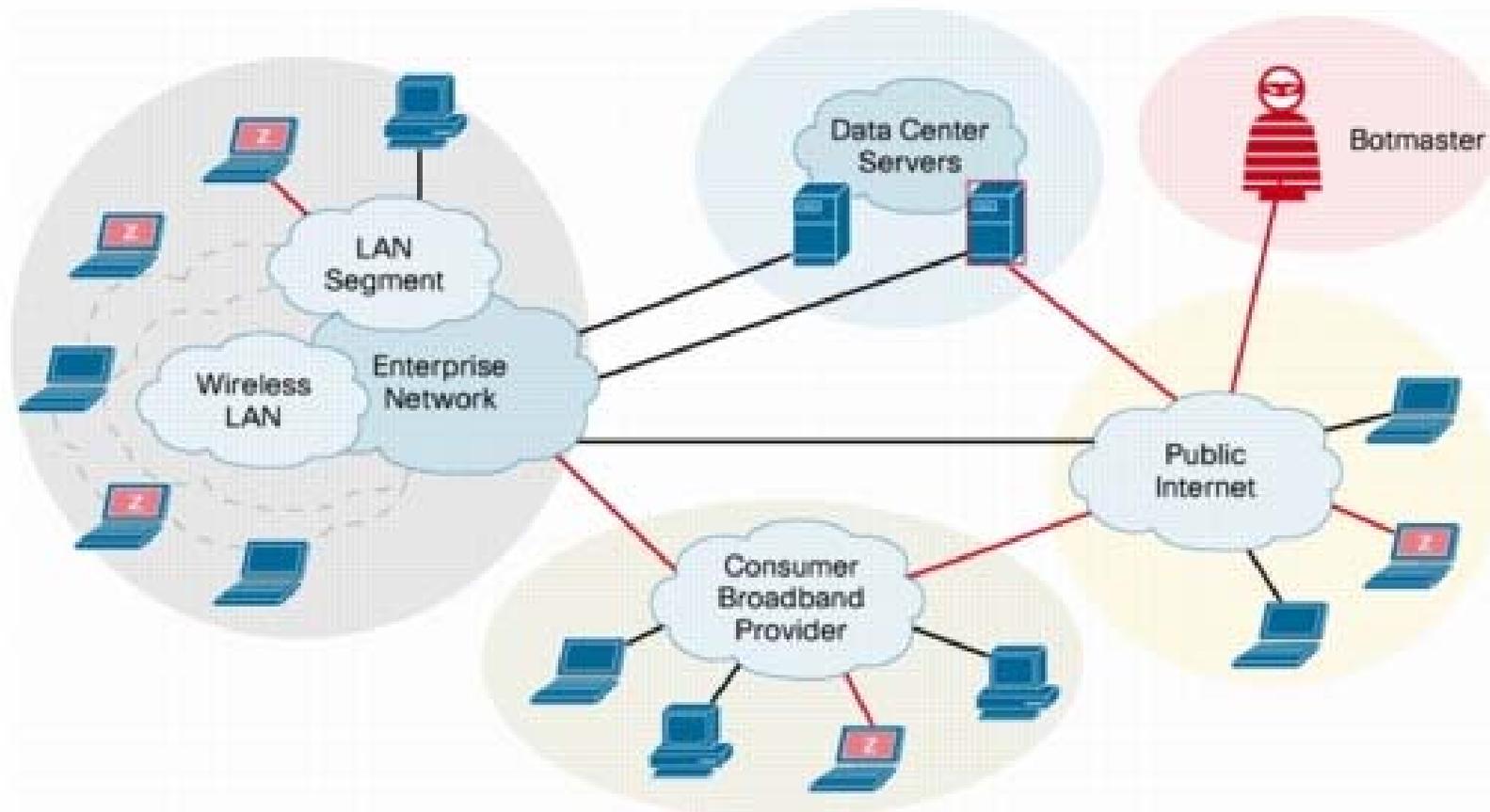


- According to a study by Prevx, 20% of computers connected to the Internet are infected by at least one rootkit
- Currently, the most frequently found rootkits (in order of prevalence) are
 - NTRootKit-J
 - Rootkit.Win32.Agent
 - Generic.dx
 - RTKT_AGENT.EBK
 - Troj/RKProc-Fam
 - VirTool:WinNT/Rootkitdrv.DH
 - Generic Rootkit.d
 - Win-Trojan/Agent.11904.C

Symantec bot statistics



Botnet composition



A resurgence in worms

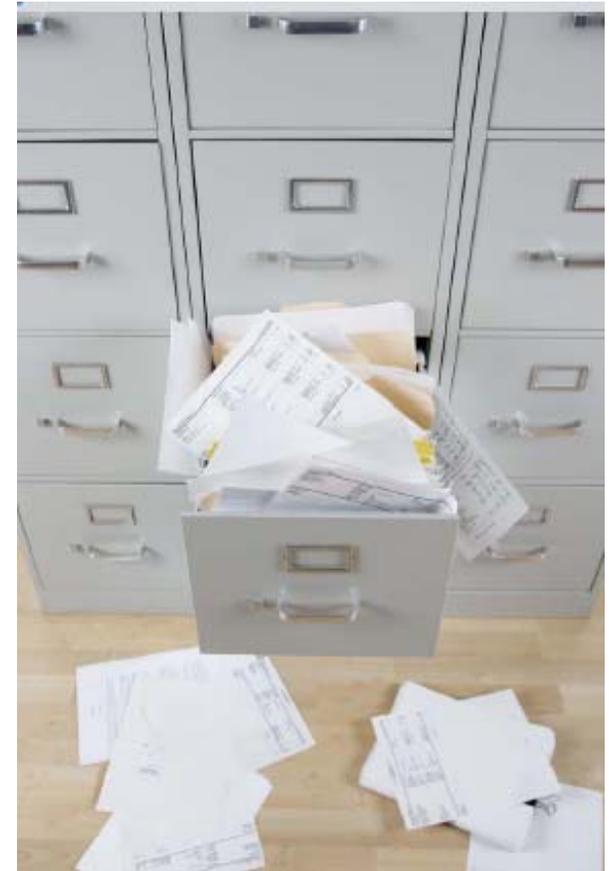


- The Conficker (also called Downup, Downadup and Kido) worm is the most prolific computer worm the world has ever seen
 - Five variants so far—Conficker A, B, C, D, and E
 - Since surfacing in November 2008, Conficker and its variants have according to numerous estimates infected more than 15 million Windows systems worldwide
 - An estimated 90,000 new infections occur every day
- Clampi worm
 - Gets and uses domain-administrator credentials to login to Windows domain controllers,
 - Copies itself to all computers on the domain
 - Serves as a proxy server to anonymize attackers' activity when they log into stolen accounts."
 - Tries to obtain information from commercial Web sites
 - Has resulted in widespread financial loss

We are leaking data all over the place!



- Personally identifiable information (PII)
- HIPAA-protected information
- Proprietary data
- Credit card numbers
- Account information
- Critical infrastructure information
- National security data
- More...

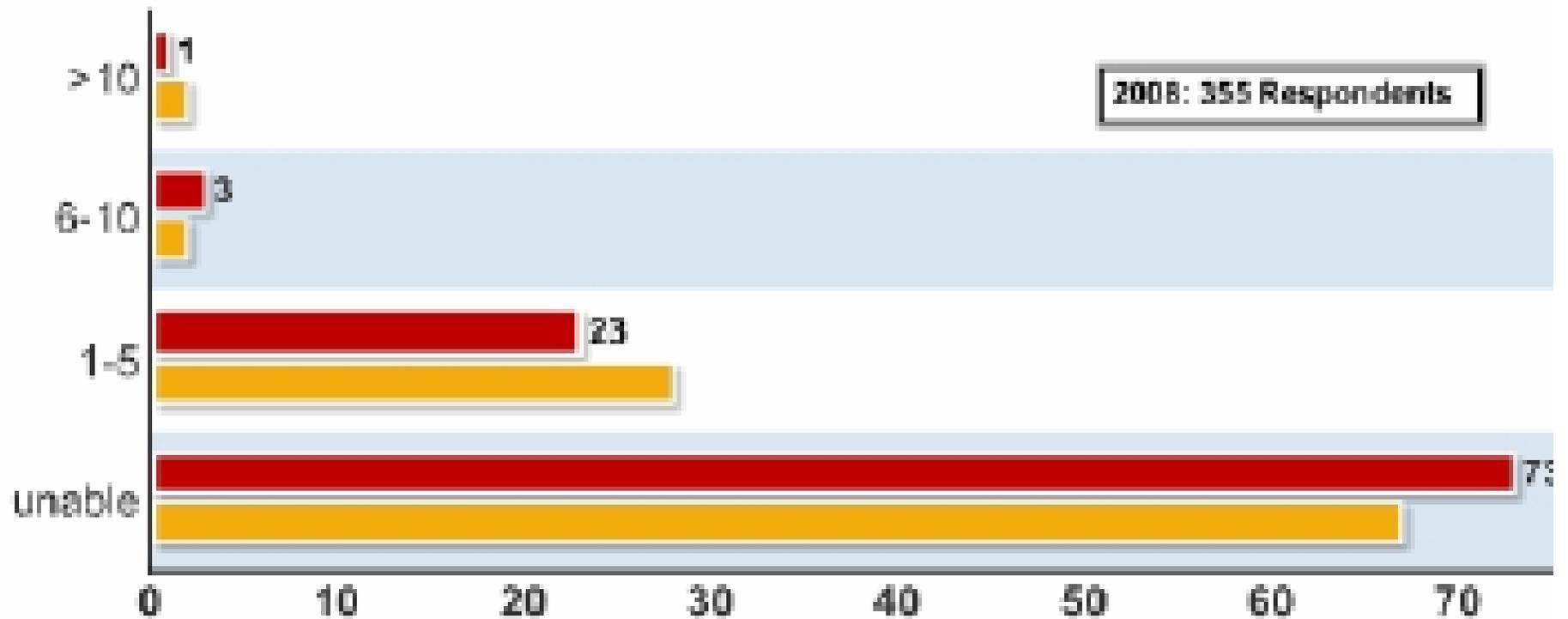


The statistics are alarming

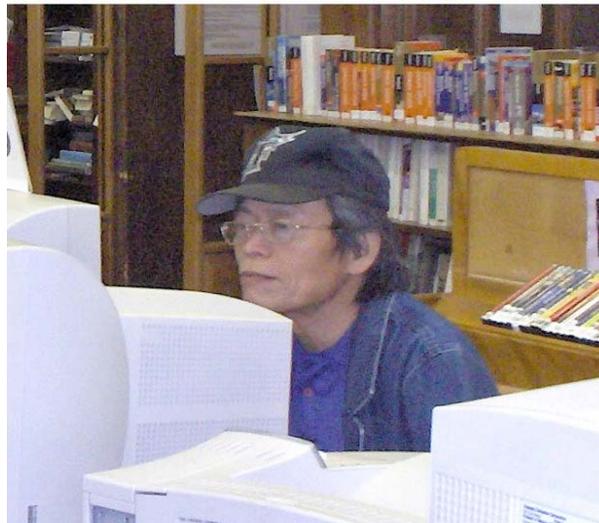
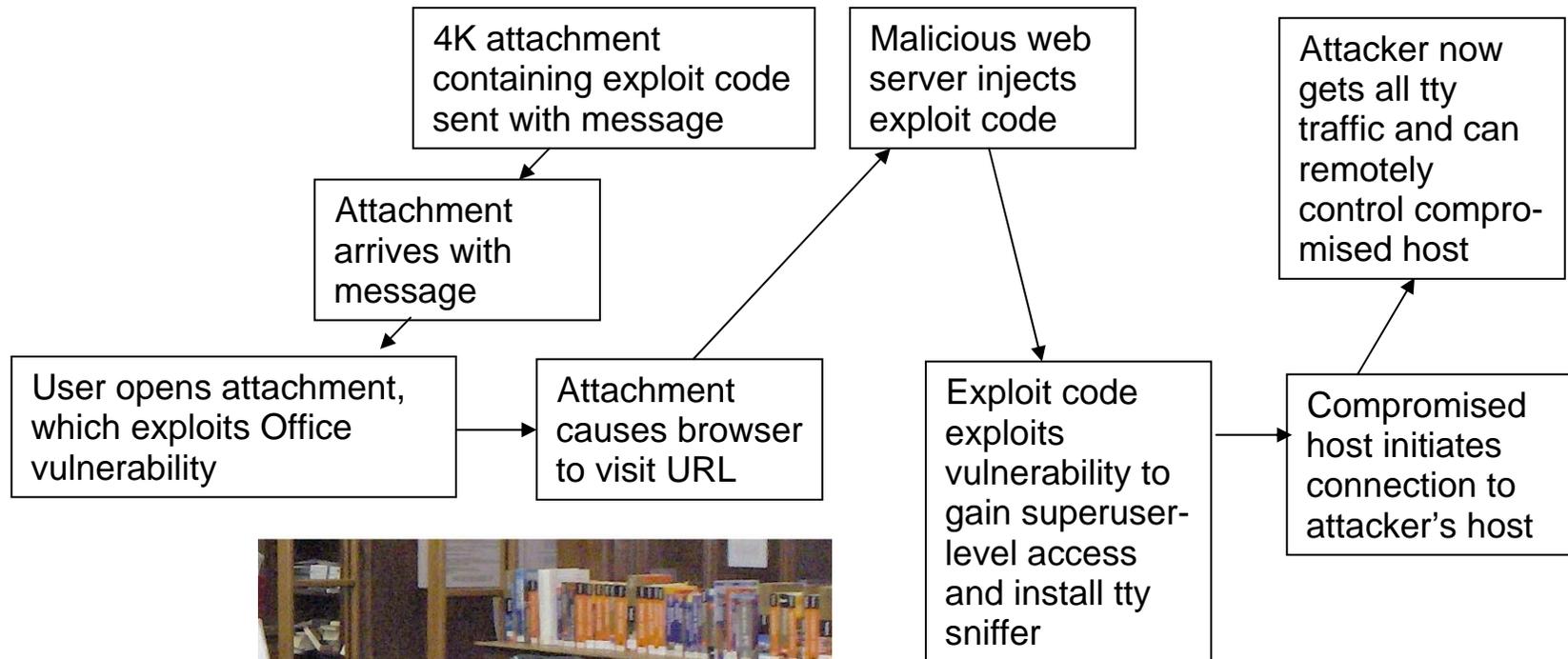


- A study commissioned by Scott & Scott LLP and conducted by the Ponemon Institute indicates that
 - Almost 85 percent of businesses have reported a data security breach
 - 45 percent of the companies have not stemmed the breach or have not implemented security measures that would prevent a similar attack
- According to the Privacy Rights Clearinghouse, 263,247,891 pieces of PII have been exposed since this organization started counting data security breaches in 2005

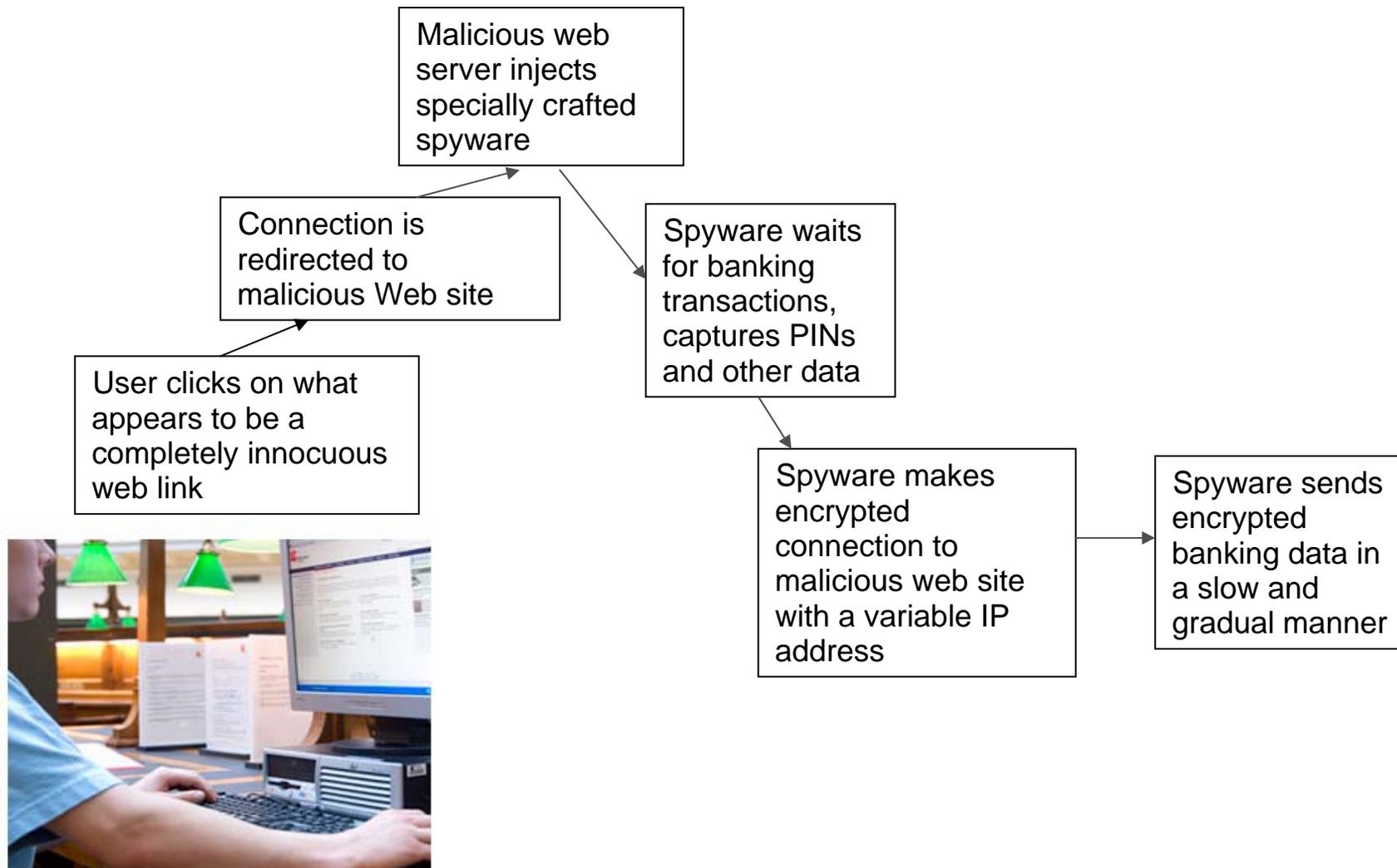
Number of targeted attacks



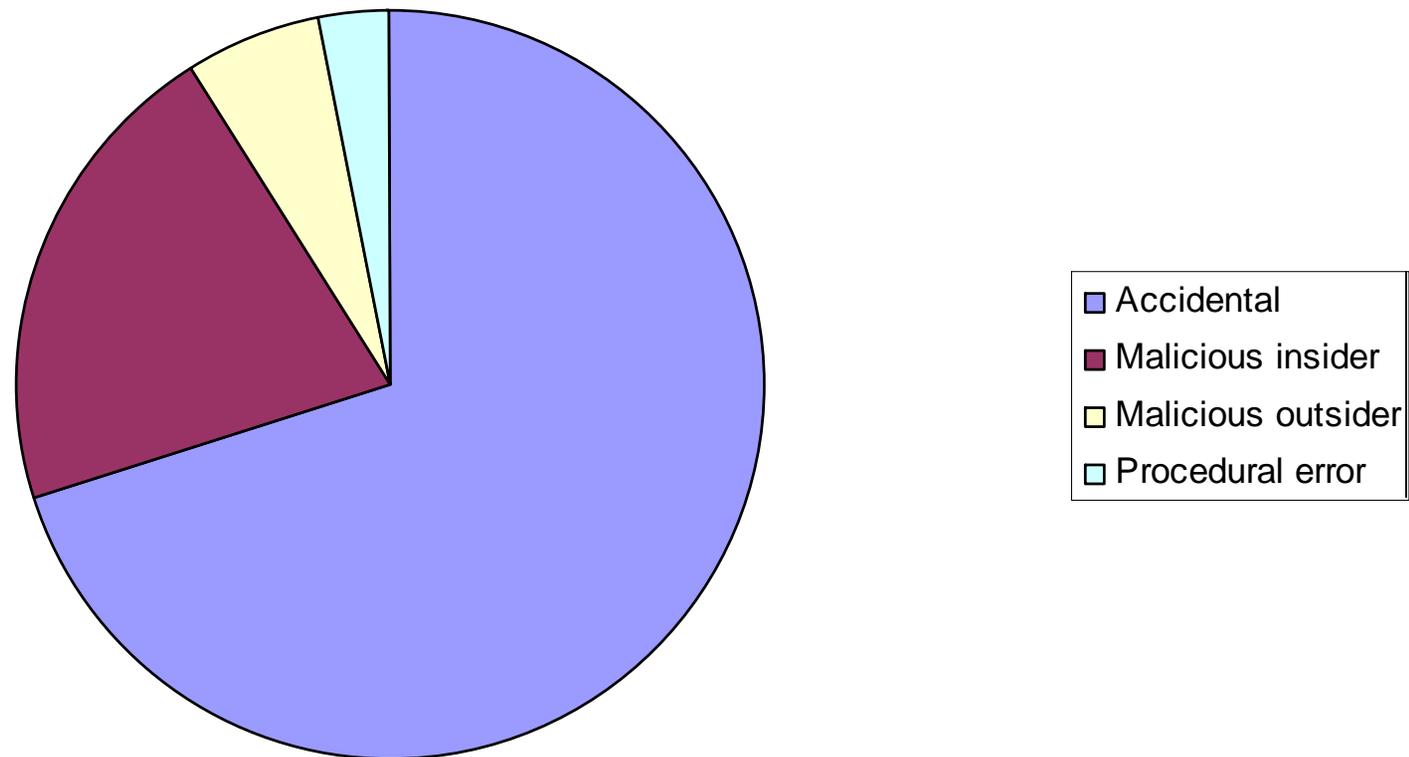
Today's targeted attacks (1)



Today's targeted attacks (2)



Insider attacks—the undisputed major cause of financial loss (1)



Insider attacks—the undisputed major cause of financial loss (2)



- One study showed that 70 percent of all successful (but not attempted) attacks are by insiders
- Another study showed that 81 percent of organizations have experienced financial loss (often major) after an insider attack
- 75 percent of organizations that were attacked by an insider experienced negative impact on their business operations
- 28 percent of organizations that experienced an insider attack suffered a loss in reputation

Crooked insiders: A bigger threat than many people realize



Many Users Say They'd Sell Company Data For The Right Price

In subway survey, 37 percent of workers say they could be bought

By Tim Wilson, [DarkReading](#)

April 24, 2009

URL: <http://www.darkreading.com/story/showArticle.jhtml?articleID=217100330>

Would you sell your company's secrets to a stranger for \$1.5 million? More than one-third of employees surveyed last week said they would -- and some of them said they'd do it for less.

In their annual visit to London's railway stations, researchers from the InfoSecurity Europe conference asked 600 commuters whether they'd sell their company's sensitive data in exchange for various forms of compensation. Last year, the researchers got many railway riders to give up their passwords for a chocolate bar.

This year, the researchers offered the workers an escalating range of theoretical bribes, ranging from a good meal to 1 million pounds (about \$1.5 million). An admirable 63 percent said they wouldn't give out their company's data at any price. Of the 37% of workers who could be corrupted, nearly two-thirds said they would have to get at least \$1.5 million to sell out. Ten percent said they would do it if their mortgages were paid off, 5 percent would do it for a vacation or new job, and 4 percent would do it to pay off their credit card debts.

Two percent of the employees said they'd sell the company's crown jewels for a "slap-up meal" -- that's British slang for a hearty meal.

And the employees weren't all working in the mailroom. In fact, 83 percent of them said they have access to customer databases, 72 percent have access to business plans, 53 percent can get into accounting systems, and 37 percent have IT administrative passwords. Two-thirds (68 percent) of the employees think it's "easy" to sneak information out of their organization; 88 percent of employees think the information they can access is valuable.

Web defacement—here to stay



Spam volume keeps growing



Computer crimes against children occur all the time



- According to current statistics, more than 77 million children regularly use the Internet.
- In the US one in seven children between the ages of 10 and 17 were solicited online by a sexual predator last year
- In 15% of those incidents, the solicitor attempted to contact the youth in person, via telephone, or by mail
- Less than 30 percent of on-line solicitations were reported to parents or authorities

Major trends in types of attacks



GROWING

- Data security breaches
- Financial fraud
- Virus and worm incidents
- DNS-related incidents
- Targeted attacks

DIMINISHING

- Phishing
- Denial of service attacks
- Bots and botnets

Major threat vectors (1)

- Espionage agents
- Organized crime
- The Black Hat community
- Stolen or lost
 - Laptops
 - USB drives
 - Hard drives
 - Mobile devices such as smart phones and PDAs
- Viruses and worms
- Spyware
- Conversations
- email, IM, chat, and social networking sites
- Phishing and vishing

Major threat vectors (2)



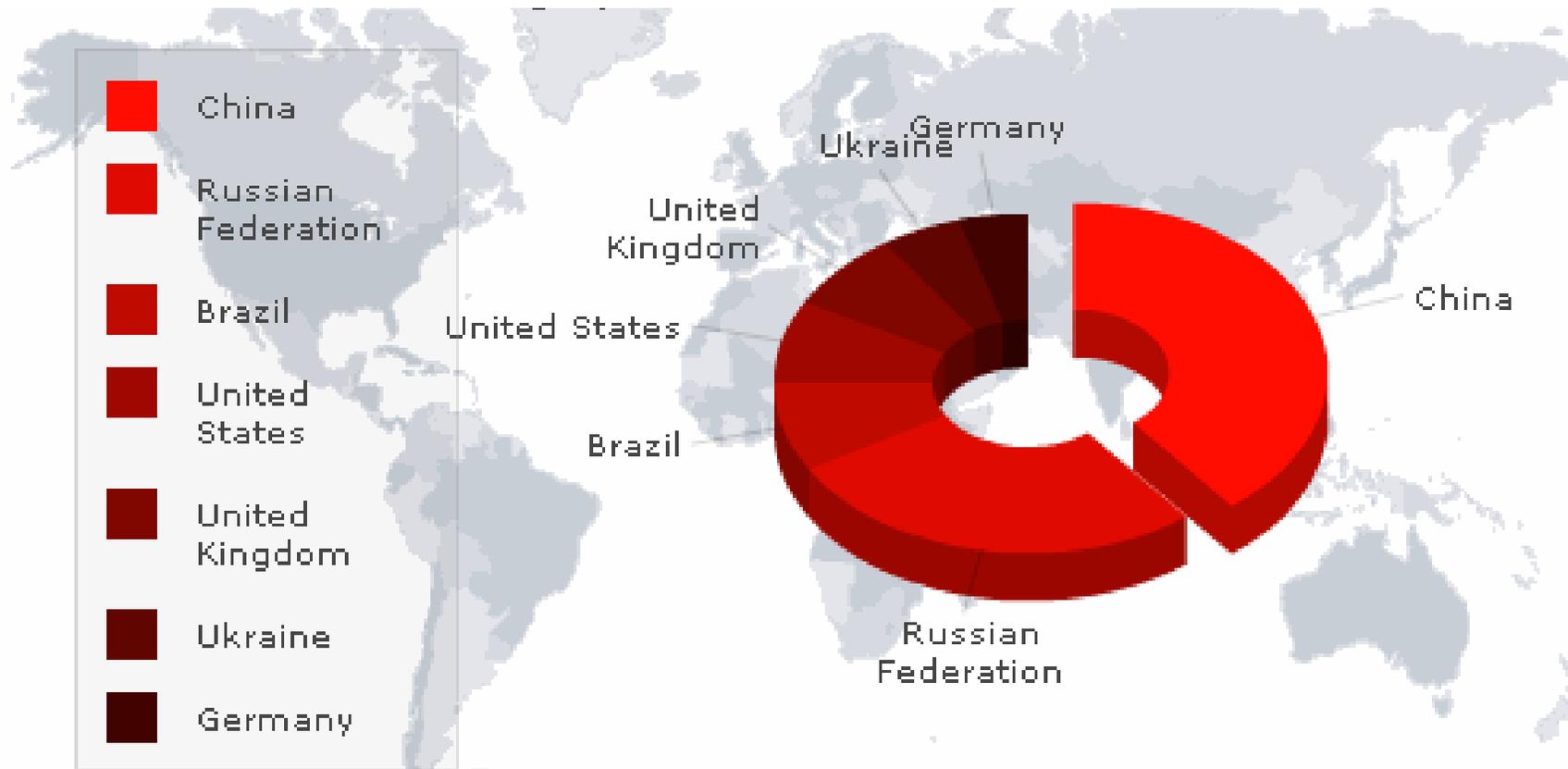
- Disgruntled or greedy employees and contractors
- Poorly configured Web servers
- Poorly designed databases
- Bugs in systems and applications
- Unencrypted network transmissions
- User error
- Much more...

The “unstoppability” factor

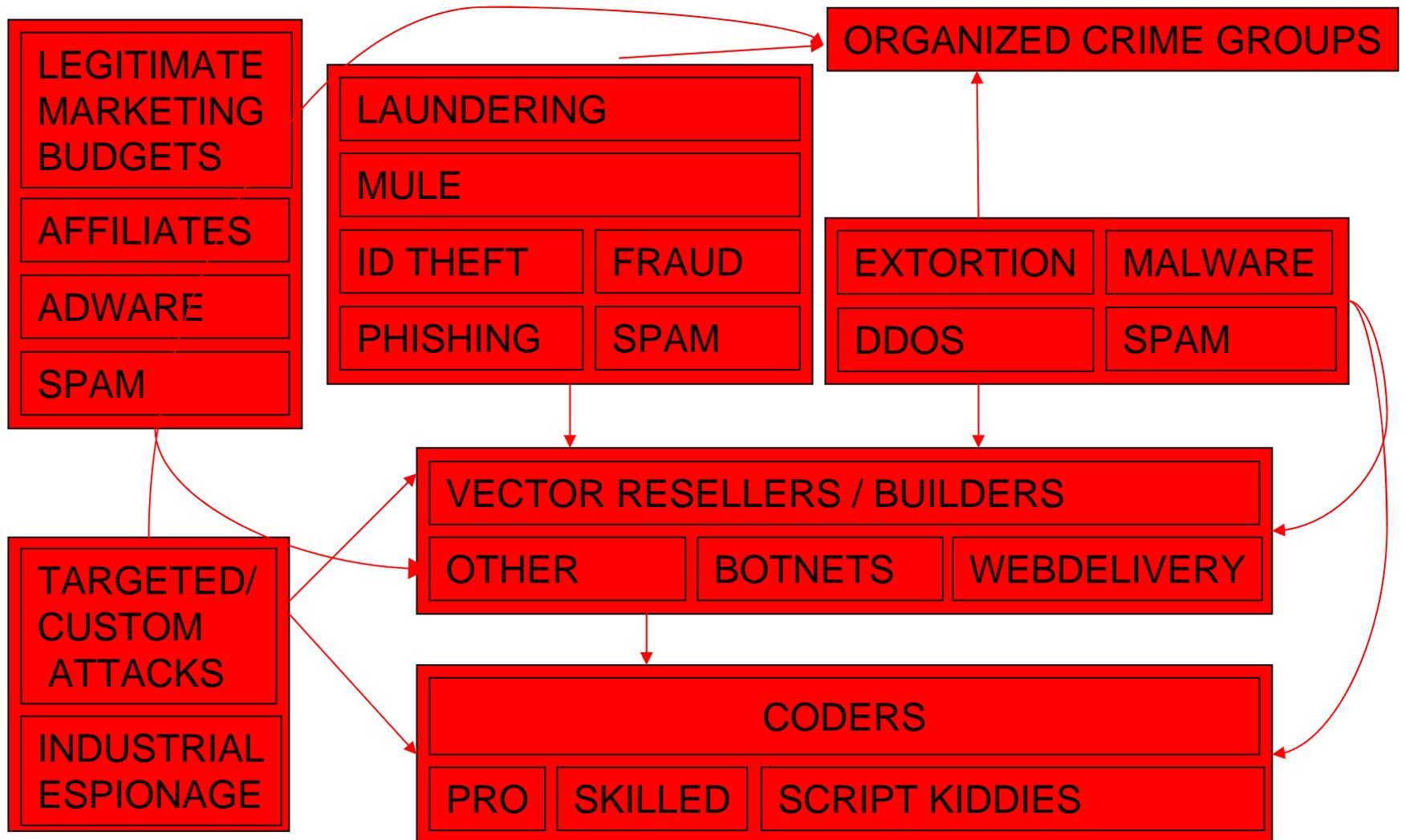


- Today's attacks are
 - Financially motivated
 - Launched by teams of experts who have financial backing
 - Often incredibly persistent

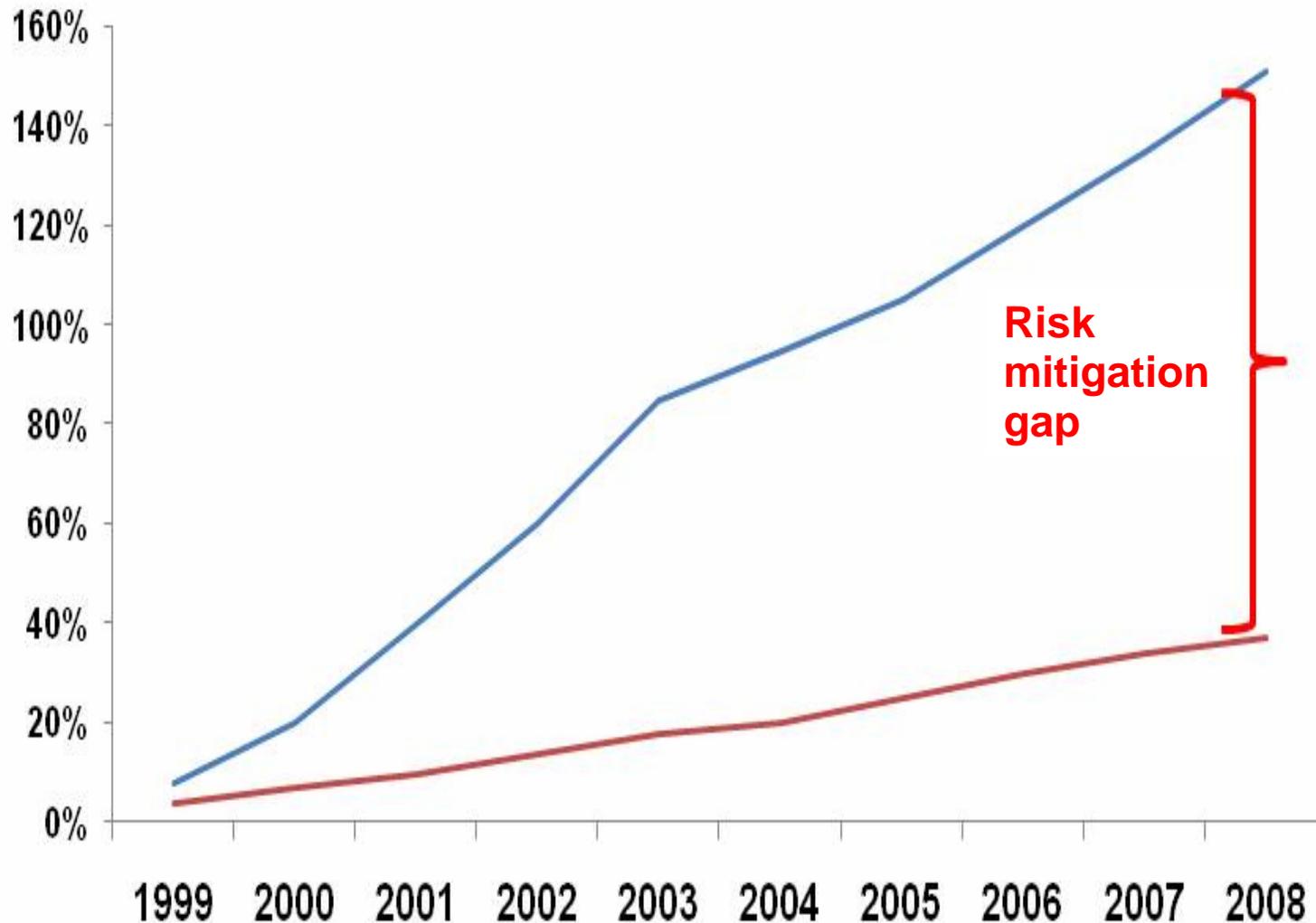
Geographic distribution of threats



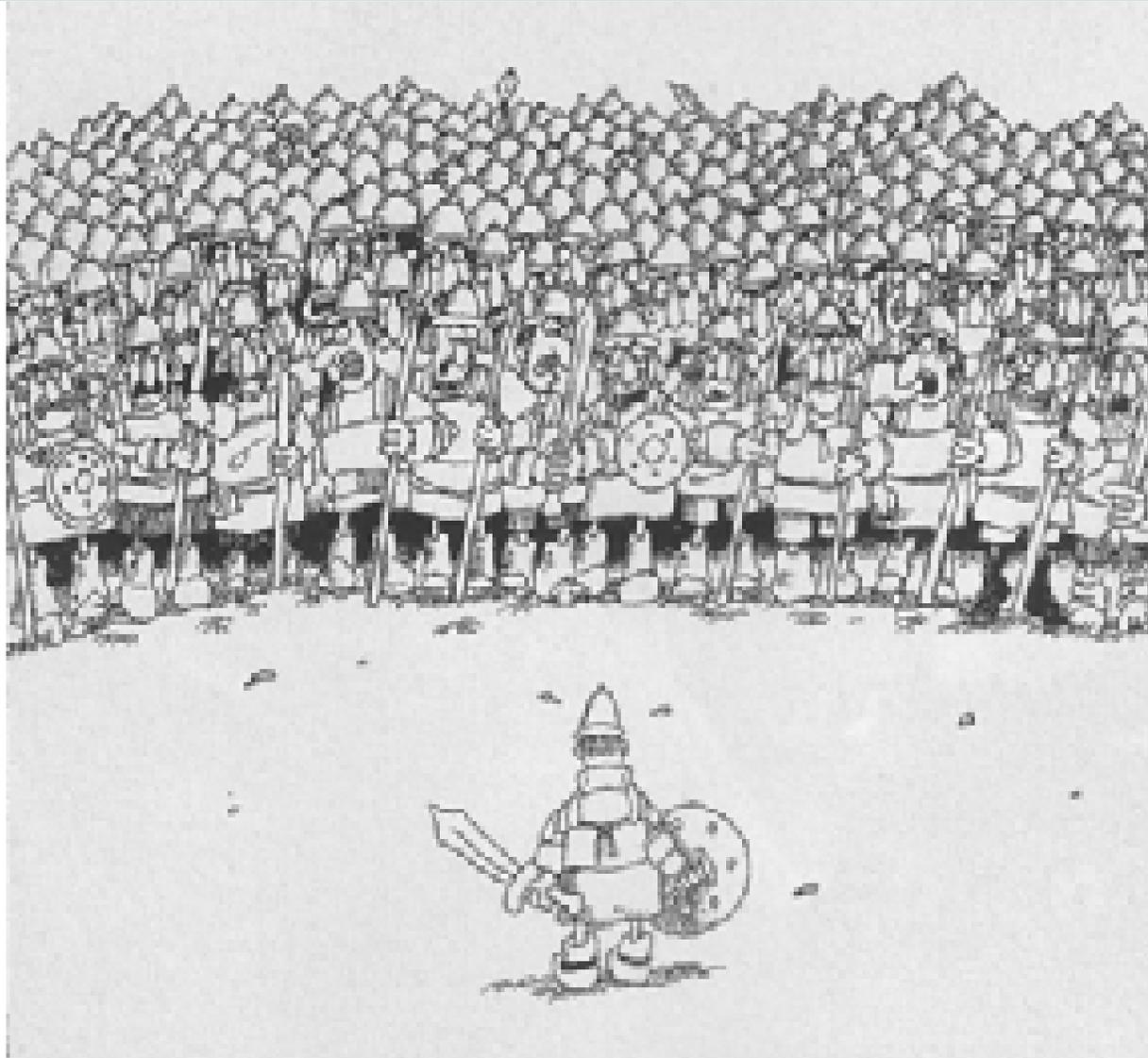
Organized crime money flow



The growing gap between risk and risk mitigation



Bad odds!



Outline



- The problem
- The nature of the threats
- **Conclusion**

Conclusion



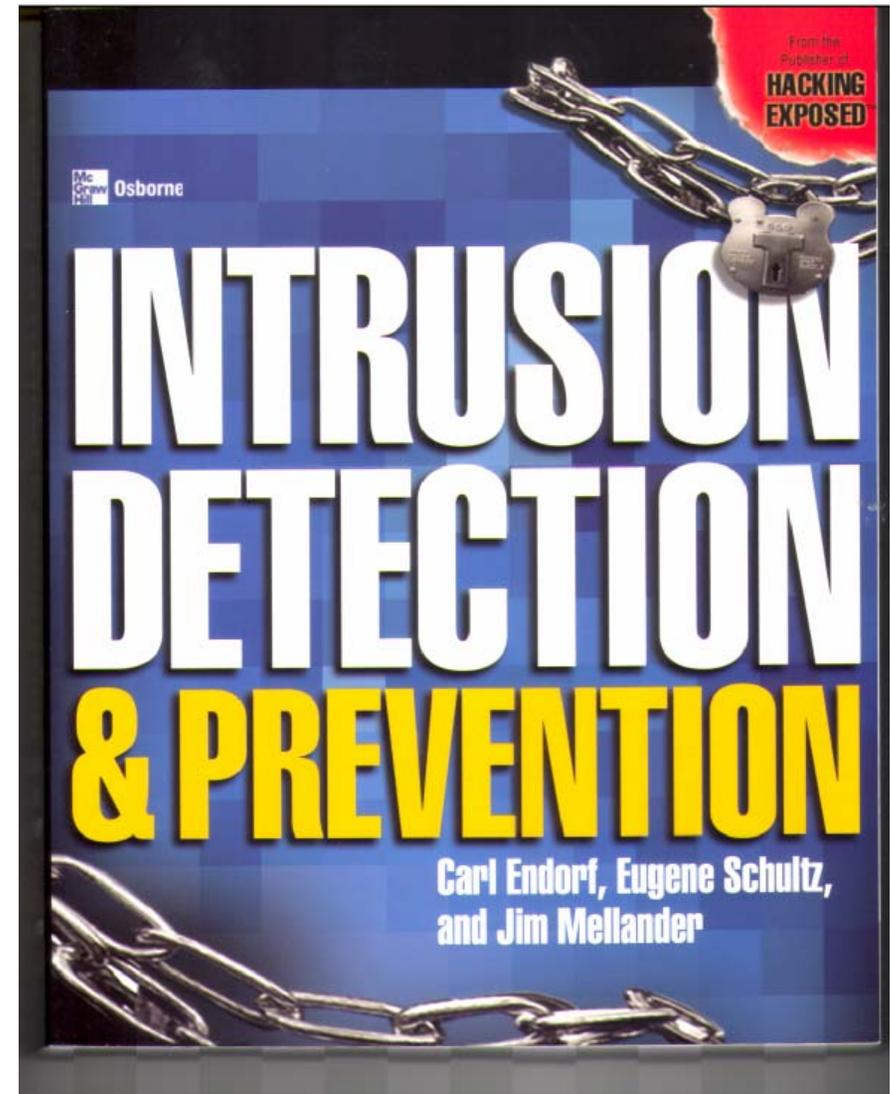
- There are no quick, easy and cheap solutions to the problem
- The first step in dealing with security risk is to have a realistic understanding of just how serious the problem is
 - A silver lining—the catastrophic incidents that organizations are experiencing are providing a major wake-up call to executive management regarding the criticality of information security
- Next develop and implement a comprehensive risk management strategy
 - Defense in depth is the right way to go
- The worst approach is to do nothing

Questions?



Emagined Security
2816 San Simeon Way
San Carlos, CA 94070
USA
+1 (650) 593-9829
eugeneschultz@emagined.com
Web: www.emagined.com
Blog: blog.emagined.com
Dashboard: dashboard.emagined.com

For a PDF copy of these slides send
email to:
YvonneVega@emagined.com





EMAGINED SECURITY