The Proliferation of High Profile Cyberattacks: Is There an End in Sight?

Dr. Eugene Schultz, CISSP, CISM
Chief Technology Officer
Emagined Security
EugeneSchultz@emagined.com

SSA Summit
National Harbor, MD
September 12, 2011

Computer incidents: They happen and they occur often

EMAGINED SECURITY

- The 2010/11 FBI Computer Crime Survey indicated the percentage of respondents that experienced each of the following
  - Malicious code infection - 87%
  - Successful phishing - 39%
  - Theft of laptop or mobile device - 34%
  - Bot infestation - 29%
  - Insider attack - 25%
  - Denial of service - 17%
  - Passwords captured via sniffing - 11%
  - Financial fraud - 9%
  - Wireless network attack - 7%

A big spike in hacking (1)

EMAGINED SECURITY

The Security Skeptic

The Security Skeptic blogs about all matters related to Internet Security, from domain name and network security to phishing and malware.

Home | Archives | Profile | Subscribe

« A Frank Conversation About Known and Zero-day Vulnerabilities | Main | Phishing for domain name accounts »

07/25/2011

My $.02 on the spike in hacking

Freakonomics recently held a security forum and asked Why Has There Been So Much Hacking Lately? Or Is It Just Reported More?

Bruce Schneier, a panel member, and Mike Rothman a sad panda who deserved to be invited but wasn't, don't see the hacking "spike" as a spike at all. Both agree that it's being reported more. And both agree that neither the attacks nor the attackers are more sophisticated but that they are being given more exposure and notoriety opportunities through social and traditional media.

Mike calls this a time of "mainstreaming of hacking" in his blog article. I agree. Attacks today are like a cable network's steady stream of *Law & Order* reruns: a single (perhaps not even clever) exploit of a badly written piece of commonly deployed software is re-used over and over again by a range of actors: bad, misguided or criminal. In the majority of incidents, there is little sophistication or skill involved.

Reporters who don't take the time to understand what they are reporting beyond the need to make things newsworthy in Internet time are prone to making every incident or breach a headline event.Mike makes the sobering

Search

Search

A big spike in hacking (2)

EMAGINED SECURITY

COMMENTARY

Battle damage increases from widespread cyberattacks

Policy needed that supports continual change, adapts to evolution of threats

By Kevin Coleman | Aug 01, 2011

Management consulting firm Deloitte said that in 2010, "security and privacy had graduated from just an IT department concern." The company is right.

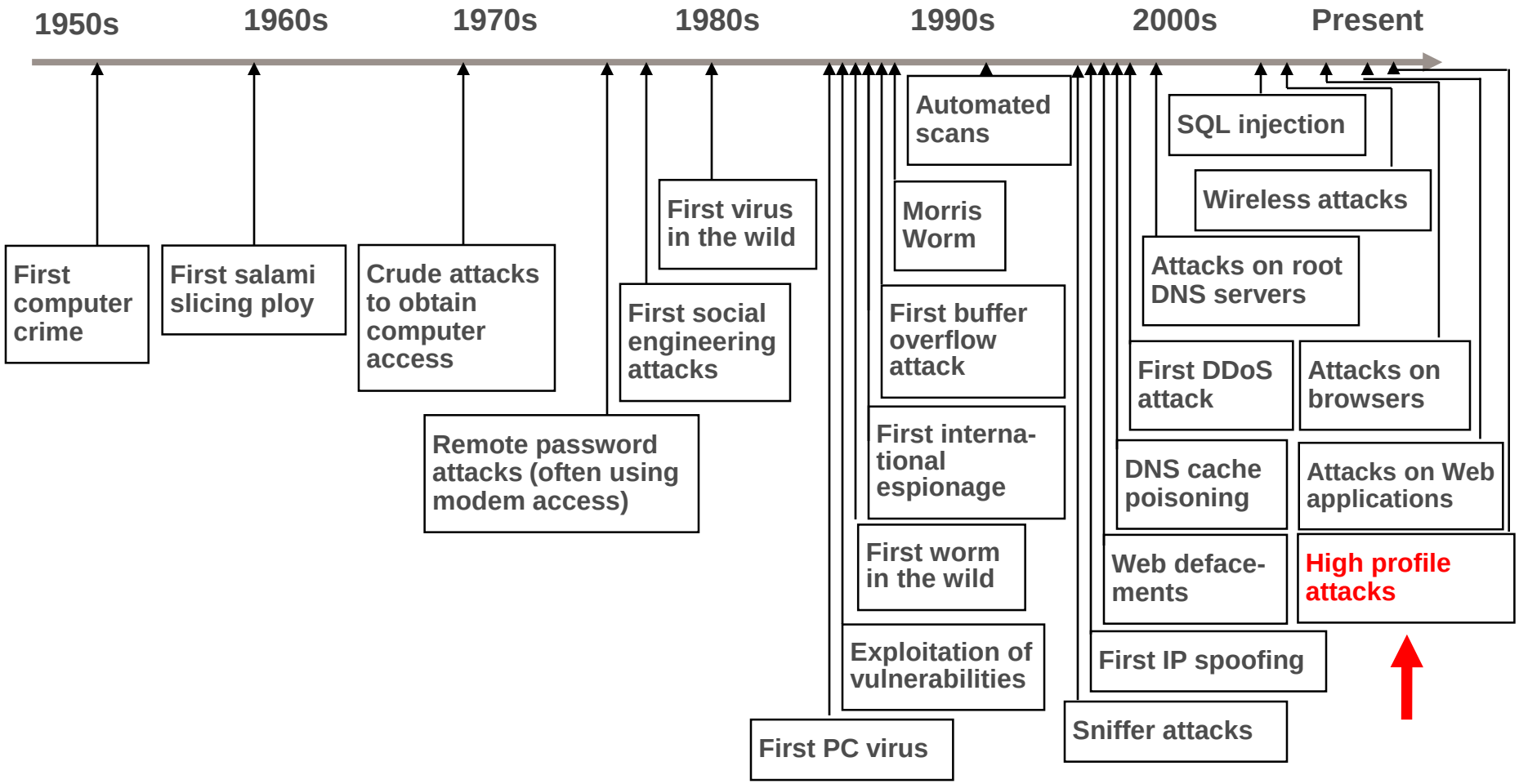
Cybersecurity is now addressed at the CEO and board of directors level and for good reason. The frequency and complexity of cyberattacks, added to high-profile successes of the attacks, have executives concerned about the business impact resulting from these assaults. Customer losses, an attack's cost, and stock price declines that often accompany the news of successful cyberattacks all combine to create a headache for C-level executives.

Deloitte points out that "the vast majority of businesses in 2011 have only limited capabilities to detect and react to point-in-time breaches." You don't have to look very far to find an example of what they are talking about. The businesses that have had their systems breached or compromised often experience high costs that impact their stock price. The organization's incident investigation and added cybersecurity efforts impact the brand's image. These costs hit the balance sheets and affect profitability and stock price.

For example, look at Sony's breach that took place in April. Sony's public disclosure of the attack and intrusion might cost the company $173 million or more. Many believe that it will exceed that number. There is another key indicator that few have recognized or even publicized. When the company

A threat timeline

EMAGINED SECURITY



Sony: Victim of a high-profile attack

EMAGINED SECURITY

Sony PlayStation suffers massive breach

Recommend 3166 recommendations. Sign Up to see what your friends recommend.

By Liana B. Baker and Jim Finkle
NEW YORK/BOSTON | Tue Apr 26, 2011 7:36pm EDT

(Reuters) - Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts in what is one of the largest-ever Internet security break-ins.

Sony learned that user information had been stolen from its PlayStation Network seven days ago, prompting it to shut down the network immediately. But Sony did not tell the public until Tuesday.

Once is not enough (at least with Sony)

EMAGINED SECURITY

Sony suffers second data breach with theft of 25m more user details

Hacker attack on security of Sony Online Entertainment network preceded PlayStation Network breach but was only discovered on Monday, electronics company says

Sony has suffered a second enormous data breach with nearly 25m customers' details from its SOE network stolen. Photograph: Nick Rowe/Getty Images

The crisis at Sony deepened on Tuesday as it admitted that an extra 25 million customers who played games on its Sony Online Entertainment (SOE) PC games network have had their personal details stolen – and that they were taken before the theft of 77 million peoples' details on the PlayStation Network (PSN).

The electronics giant said the names, addresses, emails, birth dates, phone numbers and other information from PC games customers were stolen from its servers as well as an "outdated database" from 2007 which contained details of around 23,400 people outside the US. That includes 10,700 direct debit records for customers in Austria, Germany, the Netherlands and Spain, Sony said.

Sony: Will the attacks ever end?

EMAGINED SECURITY

"Anonymous" attacks Sony to protest PS3 hacker lawsuit

By Nate Anderson | Published 4 months ago

The hacker hordes of Anonymous have transferred their fickle attention to Sony. They are currently attacking the company's online Playstation store in retribution for Sony's lawsuit against PS3 hacker George Hotz (aka "GeoHot"). A denial of service attack has temporarily taken down playstation.com.

In a manifesto announcing the new operation, Anonymous railed against Sony for going after coders who seek to modify hardware that they own. The lawsuits are an "unforgivable offense against free speech and internet freedom, primary sources of free lulz (and you know how we feel about lulz)."

"Your corrupt business practices are indicative of a corporate philosophy that would deny consumers the right to use products they have paid for and rightfully own, in the manner of their choosing," continues the pronouncement. "Perhaps you should alert your customers to the fact that they are apparently only renting your products? In light of this assault on both rights and free expression, Anonymous, the notoriously handsome rulers of the internet, would like to inform you that you have only been 'renting' your web domains. Having trodden upon Anonymous' rights, you must now be trodden on."

Anonymous is rallying participants to voluntarily contribute to the denial of service attack on Sony. That attack is continuing, and it appears to be far more successful than recent hits on Angel Soft toilet paper. In Anonymous chat rooms, participants bash Sony but worry about how their actions will be perceived. "Guys, you need to talk to the gamers and explain to them that this does not affect their gameplay," wrote one.

Some even hope to take credit for a small drop in Sony's stock price: "We're already causing sony stock to drop!!!"

But the CIA is invincible, isn't it?

EMAGINED SECURITY

CIA website brought down by DDoS attack, LulzSec hackers claim responsibility

Hi there! If you're new here, you might want to subscribe to the RSS feed for updates.

by Graham Cluley on June 15, 2011 | Comments (21)

FILED UNDER: Law & order, Vulnerability

The CIA website at cia.gov is currently inaccessible, having apparently fallen foul of a distributed denial-of-service (DDoS) attack by hackers.

Almost inevitably, fingers are pointing towards the notorious LulzSec hacktivist group who have made a name for themselves recently with a

How about the U.S. Senate?

EMAGINED SECURITY

LulzSec hacks US Senate

Bethesda also bashed in latest attack

By **John Leyden** • **Get more from this author**

Posted in Enterprise Security, 14th June 2011 09:26 GMT

Hacker tricksters LulzSec is baiting US lawmakers with its latest attack on the US Senate.

The hacking group posted what security experts Sophos characterised as "basic information on the filesystems, user logins and the Apache web server config files" of the Senate website on Wednesday morning.

The group also posted a directory listing in a post that ends with a brazen taunt to US authorities, referencing proposals by the Obama administration to make hacking critical infrastructure systems an act of war.

> **This is a small, just-for-kicks release of some internal data from Senate.gov - is this an act of war, gentlemen? Problem?**

Under existing US computer crime law (specifically the Computer Fraud and Abuse Act) the hack might be punishable upon indictment and conviction by up to five years' imprisonment.

Lulz Security (LulzSec) has emerged from obscurity over recent weeks with attacks against PBS (over its documentary on Wikileaks), Sony and FBI-affiliated security organisations

Certainly InfraGard is invincible, right?

EMAGINED SECURITY

LulzSec Attacks FBI Affiliate InfraGard

By Stefanie Hoffman, CRN

June 06, 2011 8:22 PM ET

Page 1 of 2

LulzSec, the hacker group behind the recent attacks against Sony Pictures and PBS, said that it had struck again, this time at a small affiliate of the Federal Bureau of Investigation.

The FBI affiliate targeted in LulzSec's latest cyber attack, InfraGard, is an Atlanta, Ga.-based non-profit organization that serves as an information liaison between the private sector and law enforcement, with a mission to protect against hostile threats to the U.S.

LulzSec said that the attack was in response to the U.S. government's recent declaration that it would treat hacking as an act of war.

"It has come to our unfortunate attention that NATO and our good friend Barrack Osama-Llama 24th-century Obama have recently upped the stakes with regard to hacking. They now treat hacking as an act of war. So, we just hacked an FBI affiliated Web site and leaked its user base," LulzSec said in a Pastebin.org blog.

As in its previous attacks, LulzSec exposed InfraGard e-mail, login credentials and other personally identifying information for about 180 employees, all of which were connected to the FBI in some way, the group said in the Pastebin blogpost.

Data security breaches: The statistics are alarming

EMAGINED SECURITY

- A recent 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, well over 600 million pieces of PII have been exposed in the U.S. alone since this organization started counting data security breaches in 2005

We are leaking data all over the place!

EMAGINED SECURITY

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

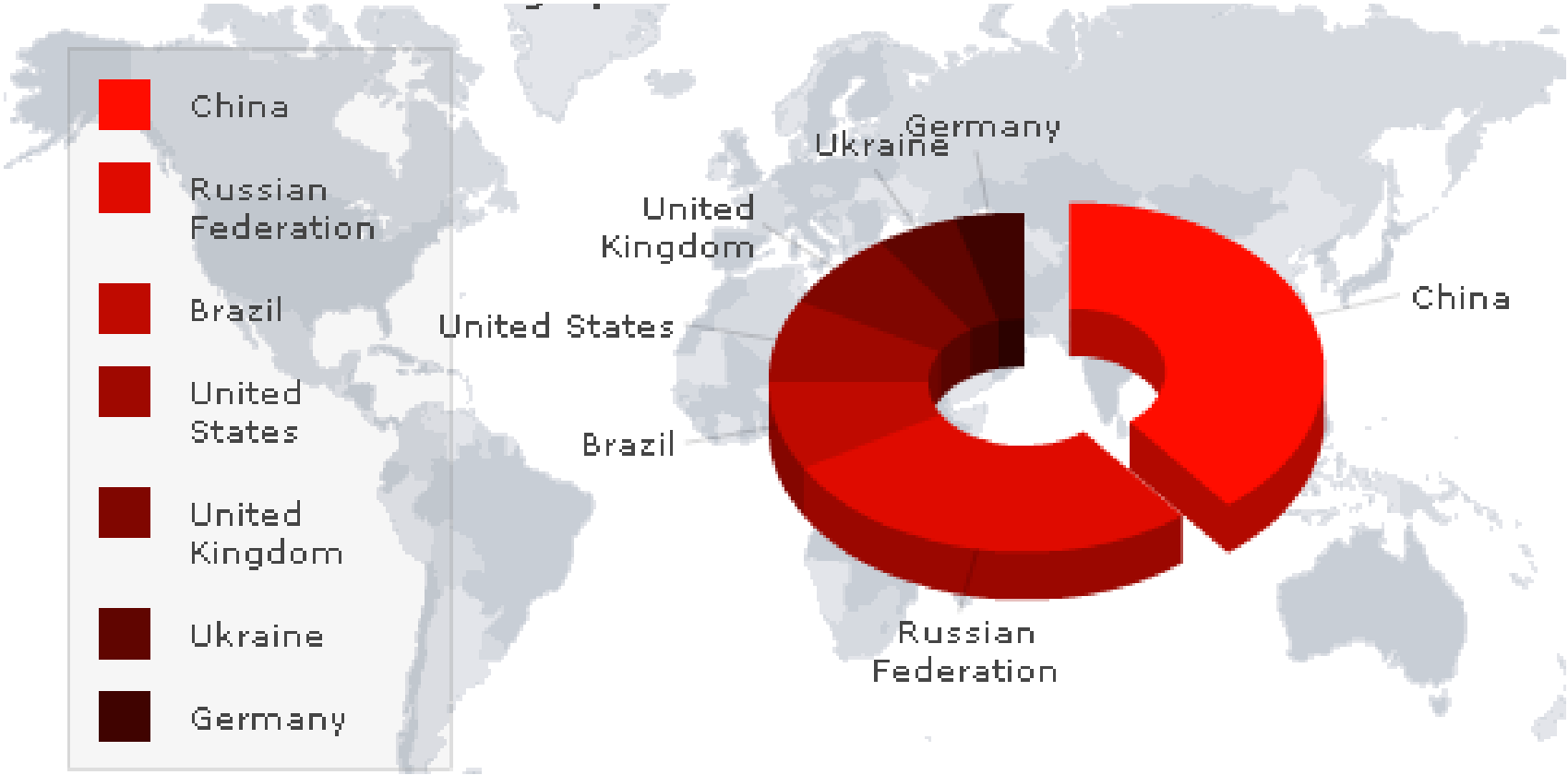
Who causes the trouble?

EMAGINED SECURITY

- State-sponsored attackers
- Organized crime
- The Black Hat community
- Disgruntled or greedy employees
- Hactivists seeking justice
- Industrial espionage agents

Geographic distribution of threats

EMAGINED SECURITY



Unstoppable attacks?

EMAGINED SECURITY

Security industry faces attacks it cannot stop

Analysis: Today's security products not much help for advanced persistent threat attacks

By Robert McMillan

March 11, 2010 04:18 PM ET

8 Comments Like +1 0

IDG News Service - At the RSA Conference in San Francisco last week, security vendors pitched their next-generation of security products, promising to protect customers from security threats in the cloud and on mobile devices. But what went largely unsaid was that the industry has failed to protect paying customers from some of today's most pernicious threats.

The big news at the show had to do with the takedown of the Mairposa botnet -- a massive network of hacked computers that has infected half of the Fortune 100 companies. So-called advanced persistent threat (APT) attacks, such as the one that compromised Google systems in early December, were another hot topic.

Both Mariposa and the Google attacks illustrate the same thing, however. Despite billions of dollars in security spending, it's still surprisingly hard to keep corporate networks safe.

That's because for these advanced attacks to work, the bad guys need to find only one vulnerability to sneak their malicious software onto the target network. Once they get a foothold, they can break into other computers, steal data, and then move it offshore. The good guys have to be perfect -- or at least very quick about spotting intrusions -- to keep APT threats at bay.

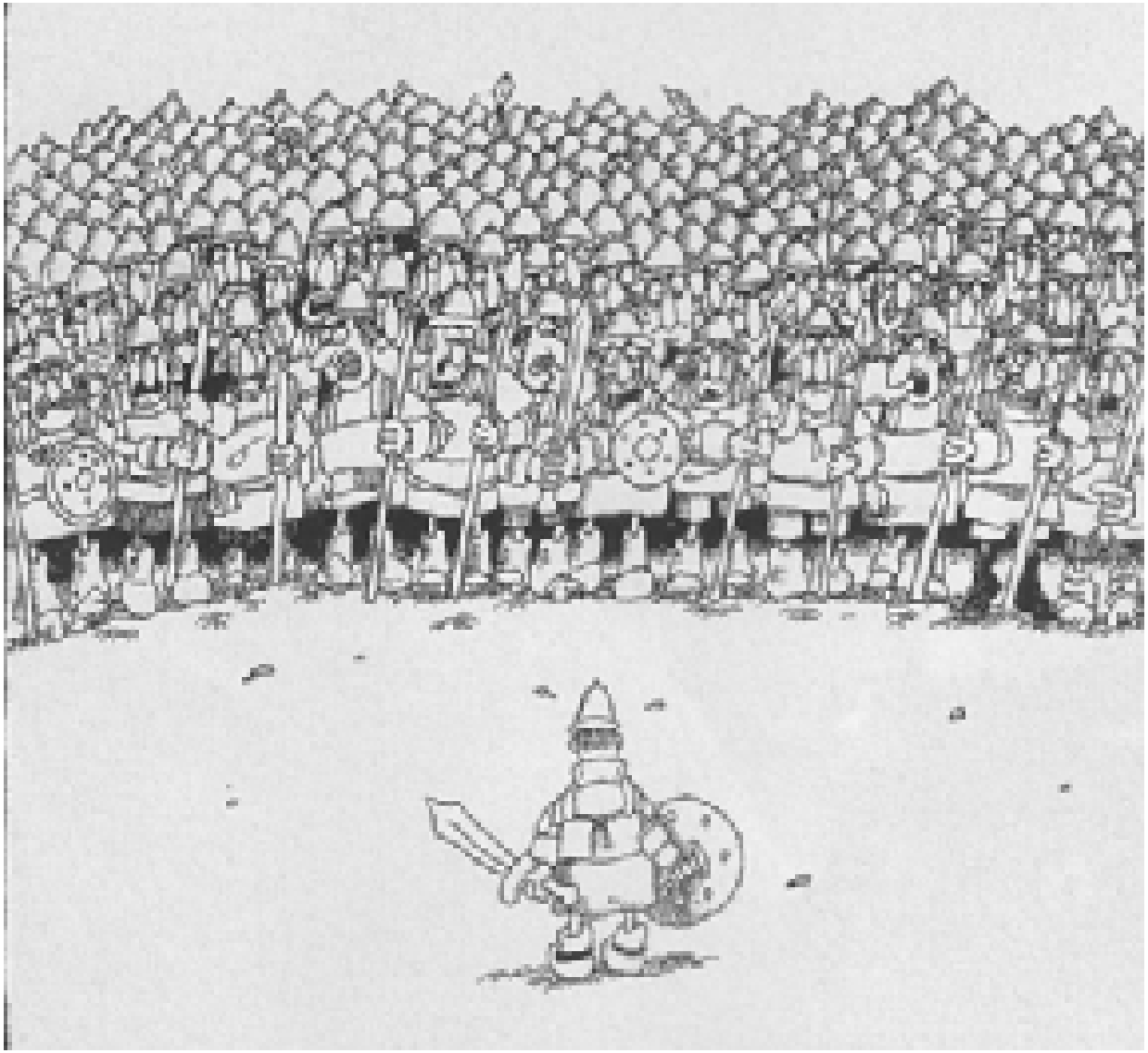
The “unstoppability” factor

EMAGINED SECURITY

- Today’s attacks are
  - Financially motivated
  - Launched by teams of experts who have financial backing
  - Perpetrated by deviants
  - Incredibly persistent

Bad odds!

EMAGINED SECURITY



Why are we hearing about so many more attacks?

EMAGINED SECURITY

- Statistics indicate the number of attacks is increasing year-by-year
- If an attack occurs, it is more difficult for victim organizations to hide what has happened
- Laws and regulations that mandate reporting certain kinds of incidents have been passed

What damage really occurs?

EMAGINED SECURITY

- Financial loss through fraud
- Compromise of intellectual property
- Lawsuits
- Fines/penalties
- Loss of customers
- Reduced value of stock shares
- Harm to people because of reduced safety
- Damaged reputation

Web applications: The number one target of attacks (1)

EMAGINED SECURITY

- Primary goal—to glean data that have monetary value
- Main focus of attackers—exploitable software bugs
  - Buffer overflow conditions
  - Errors that result in a privileged state
  - Ability to escape to a shell that allows command entry
  - Allowing database queries that bypass normal access restrictions
  - Failure to revoke privileges at the end of privileged routines
  - More
- We've been forewarned many, many times
  - DHS threat advisories
  - MITRE's Common Vulnerabilities and Exposures
  - The SANS Top 25 vulnerabilities

Web applications: The number one target of attacks (2)

EMAGINED SECURITY

- Programmers keep making the same mistakes over and over again
- Quality assurance efforts are for the most part not up to par
- Solutions are available
  - OWASP publishes guidelines for secure coding of Web applications
  - Tools that identify software bugs so that they can be eliminated are readily available

The situation is not hopeless

EMAGINED SECURITY

Ongoing storm of cyberattacks is preventable, experts say

By William Jackson · Jun 16, 2011

The CIA has become a member of a less-than-exclusive club of high-profile targets hit by online attacks, falling victim to a denial-of-service attack that temporarily took down its website.

The outage was reported June 15 and the LulzSec hacker group claimed credit. Other recent victims of a variety of attacks include defense contractors Lockheed Martin and L-3 Communications, the website of the Atlanta InfraGard chapter, the International Monetary Fund and the U.S. Senate.

Some of the attacks were targeted, using data stolen earlier this year from EMC's RSA security division, some involved webpage defacements and others were simple denial-of-service attacks.

"They all have one common denominator," said Eric Giesa, vice president of product management for F5 Networks. "All of them are preventable."

What can stop the acceleration of incidents? (1)

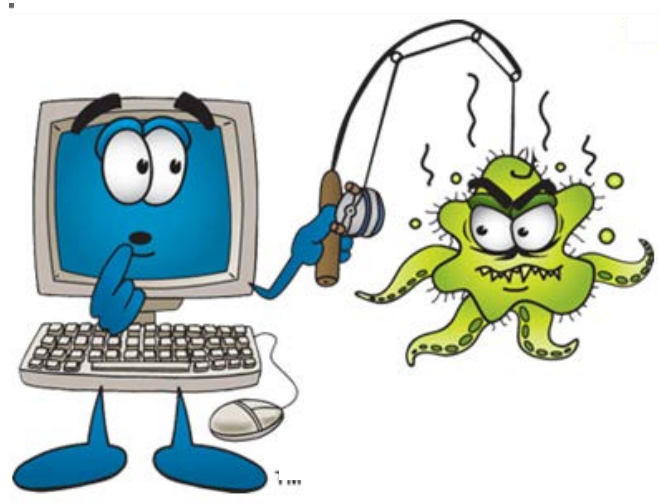
EMAGINED SECURITY

- Stephen Northcutt of the SANS Institute has predicted that unless there is a turnabout in the practice of cyber security, up to 40% of small and medium businesses will be forced out of business within five years
- The first step in dealing with security risk is to have a realistic understanding of just how serious the problem is
  - Fortunately, the catastrophic incidents that organizations are experiencing are providing a major wake-up call to executive management regarding the criticality of cyber security
- Many solutions (some draconian) have been proposed

What can stop the acceleration of incidents? (2)

EMAGINED SECURITY

- Proven, cost-effective security controls such as tools that identify vulnerabilities in programs before they can be exploited are available
- Patching bugs in systems and applications is also critical



Conclusion

EMAGINED SECURITY

- There are no quick, easy and cheap solutions to the problem
- Taking steps towards producing more bug-free software could go a long way
- The worst approach is to do nothing