How Secure Is Your Data? – Let's talk Layer 7

Josh Hogle, Principal Security Engineer

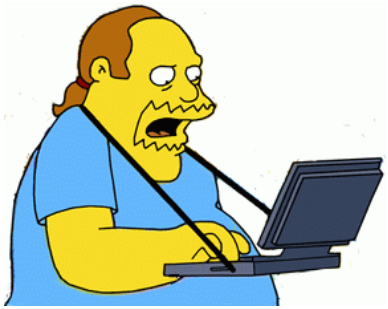
May 3rd, 2013

Reality Check

The Threat Landscape Has Changed

Today's Threat Landscape

Threats have changed…



Script Kiddies and "Digital Graffiti" artists, Backdoors in open source

Code Red Nimda Klez Anna Kournikova

2001

Security Spend

- Anti-virus
- Firewall/VPN
- Content Filtering
- IDS/IPS

Cyber Espionage, Organized Criminals, Hactivists

APT Mobile phone attacks Targeted attacks 232 million identities stolen

2012

Security Spend

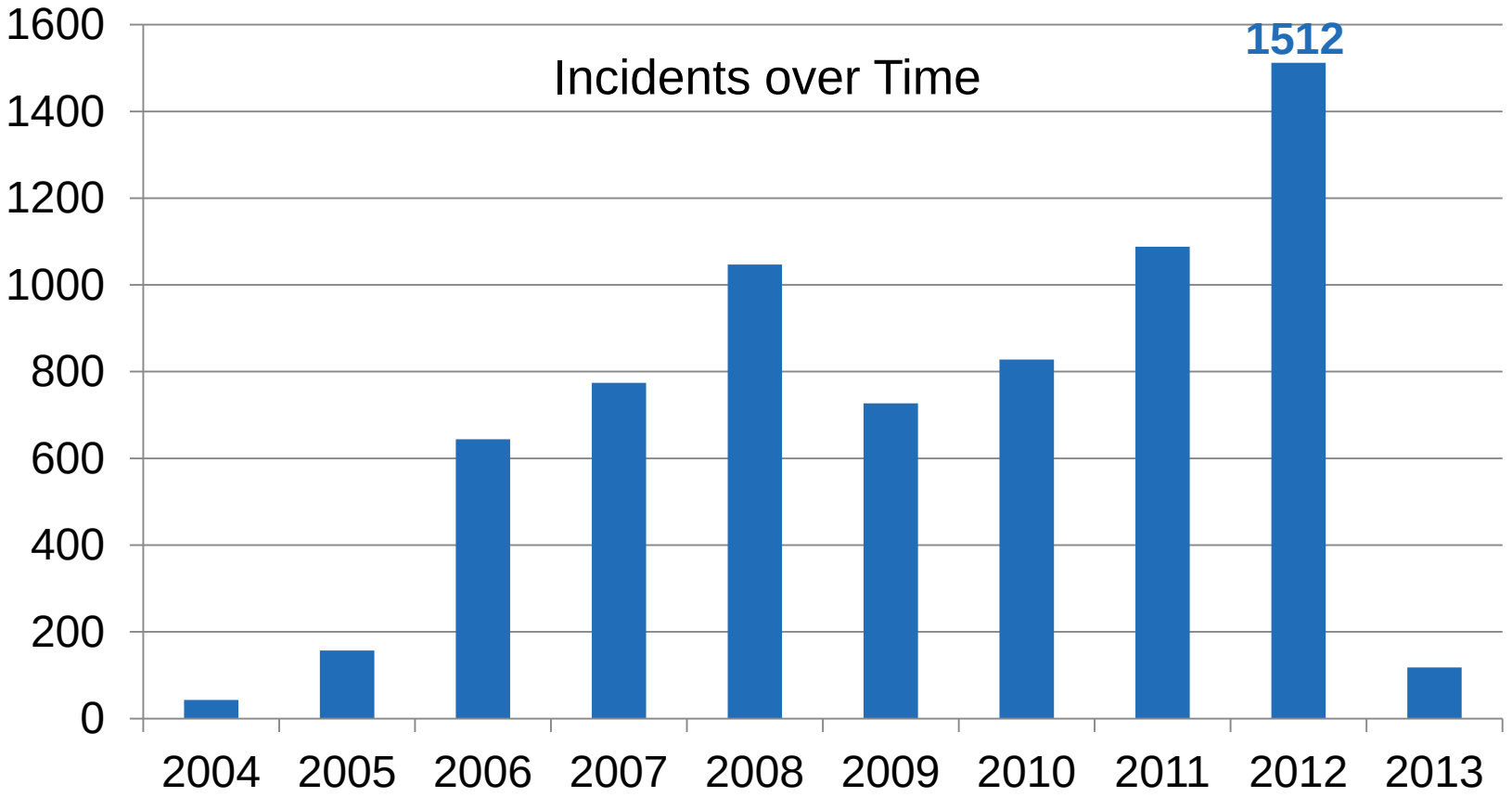
- Anti-virus
- Firewall/VPN
- Secure Email/Web
- IPS

…Security spending hasn't

Sources: Gartner, Imperva analysis

Cyber Attacks Are Getting Worse

2012: the worst year on record for data breaches



Source: DataLossDB.org

Who's Doing It and Why

Governments

- Stealing Intellectual Property (IP) and raw data, and spying
- Motivated by: Policy, Politics and Nationalism

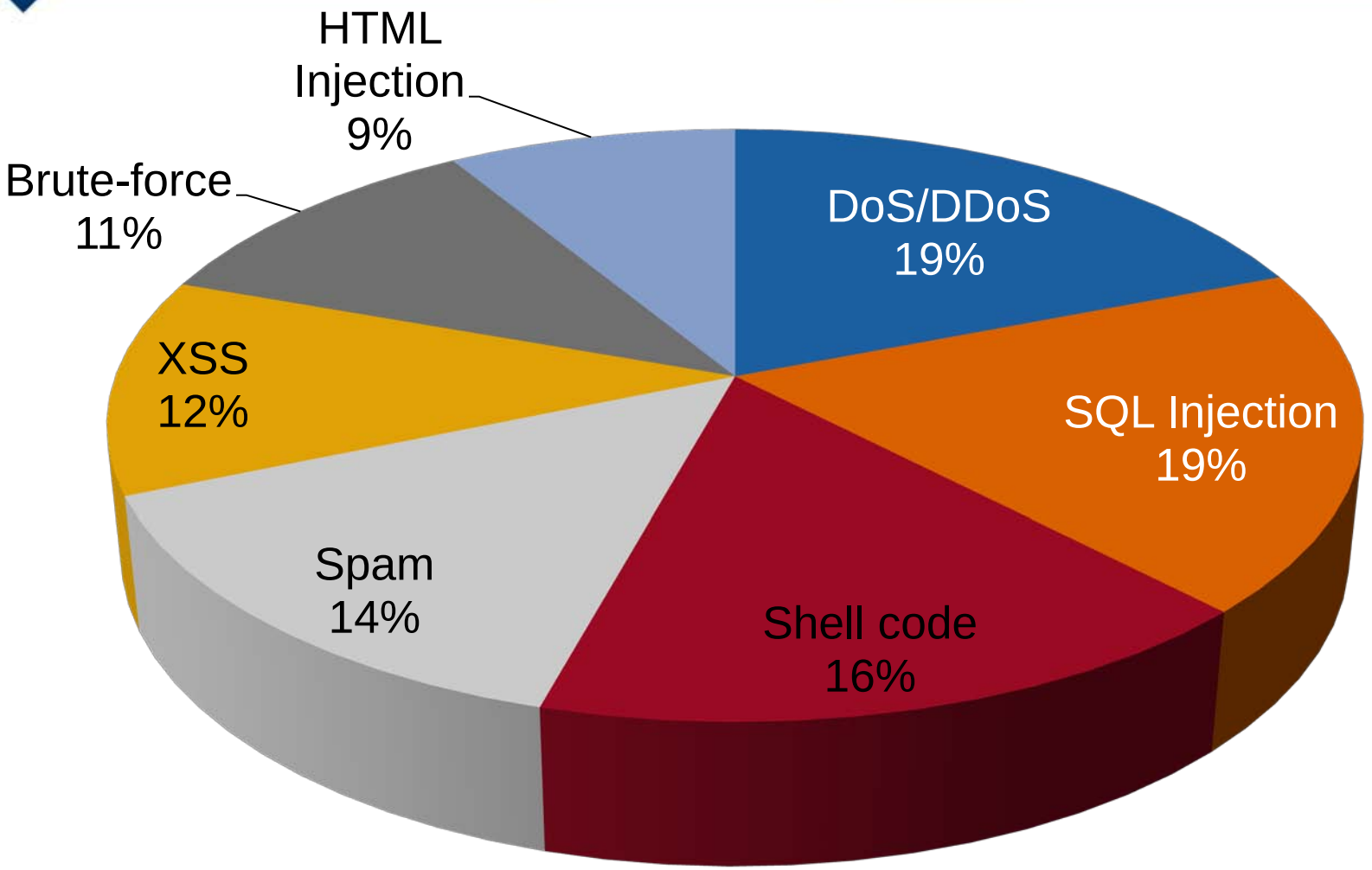
Industrialized hackers

- Stealing IP and data
- Motivated by: Profit

Hacktivists

- Exposing IP and data, and compromising the infrastructure
- Motivated by: Political causes, ideology, personal agendas

Hackers Today Focus on Data and Applications



Source: Imperva. September 2011-September 2012. Sample size was 439,587 total threads.

Where Do They Attack?

Desktop and the user

Multimillion dollar datacenter

Not well protected

Both access the same data

Well protected

Recent Attacker Targets….

- Yahoo Voice
- Linked In
- Last.fm
- Formspring
- eHarmony
- US Department of Justice
- US Copyright Office
- FBI
- MPAA
- Warner Br
- RIAA
- HADOPI
- BMI
- SOHH
- Office of t
- AU House
- AU Depar
- Swiss ban
- Egyptian Government
- Itau
- Banco de Brazil
- US Senate
- Caixa

- Church of Scientology
- Muslim Brotherhood
- Zappos.com
- MilitarySingles.com
- Amazon
- Austria Federal Chancellor
- HBGary Federal
- Mexican Interior Ministry

1. How many of these organizations have AV, IPS and Next Generations Firewalls?

2. Why are the attacks successful when these technologies claim to prevent them?

- PayPal
- MasterCard
- Visa

Industrialization Of Hacking And Automation

Roles

Researching Vulnerabilities

Developing Exploits

Growing Botnets

Exploiting Targets

Consuming

Optimization

Direct Value – i.e. IP, PII, CCN

Command & Control

Malware Distribution

Phishing & spam

DDoS

Automation

Growing Botnets and Exploiting Vulnerabilities

Selecting Targets via Search Engines

Templates & Kits

Centralized Management

Service Model

Automation Is Prevailing

In a hacker forum, it was boasted that one hacker had found 5012 websites vulnerable to SQLi through automation tools

Note:

- Due to **automation**, hackers can be effective in small groups – i.e. Lulzsec
- Automation also means that attacks are equal opportunity offenders. They don't discriminate between well-known and unknown sites

5012 SQL Injectable Websites

Collected by [redacted]

http://www.[redacted]/trainers.php?id='4
http://www.[redacted].com/trainers.php?id='30
http://[redacted].com/trainers.php?id='30
http://www.[redacted].com/article.php?ID='338
http://www.[redacted].com/publications/article.php?ID='51
http://www.[redacted].com/article.php?id='13798
http://www.[redacted].com/news/article.php?Id='0222
http://www.[redacted].com/article.php?id='59
http://www.[redacted].com/press/article.php?id='000073
http://www.[redacted].com/article.php?id='5
http://www.[redacted].net/article.php?id='104
http://[redacted].net/article.php?id='1089
http://www.[redacted].net/news/article.php?id='416
http://[redacted].net/article.php?id='2524
http://www.[redacted].net/article.php?id='11012&lang='th
http://www.[redacted].net/news/article.php?id='48
http://www.[redacted].net/nl/article.php?id='1512&type='col

Distributed Denial Of Service (DDoS) Threats

- DDoS Statistics
  - **74%** of organizations received a DDoS attack in past year[1]
  - **31%** of attacked organizations suffered service disruption[1]

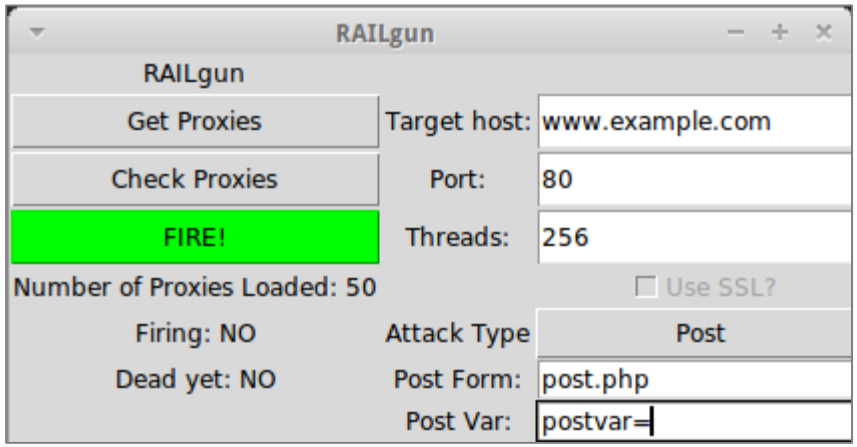
- Most DDoS attacks are launched by botnets, because of scale
  - Toolkits automate DDoS attacks
  - Botnets for rent from $50 - $2K

DDoS Attack Tool

[1] "The Trends and Changing Landscape of DDoS Threats and Protection," Forrester Research

Application DDoS

- Less expensive for hackers because it requires fewer host machines
- Traditional network security cannot block app DDoS
- Common app DDoS attack: exhausting the victim's Web server concurrent requests pool
- App DDoS Tools
  - RAILgun
  - SlowHTTPtest



Web Fraud Costs Businesses Millions

- Fraudulent payment transactions
  - Chargeback fees
- New account fraud
  - Chargeback fees due to ID theft
  - Bots email or post spam
- Account login fraud
  - Logins with stolen credentials erodes brand
- Man-in-the-Browser attacks

Fraud Malware

111,111

Number of unique strains of malware deployed per day

10,000

Malicious new domains deployed per day

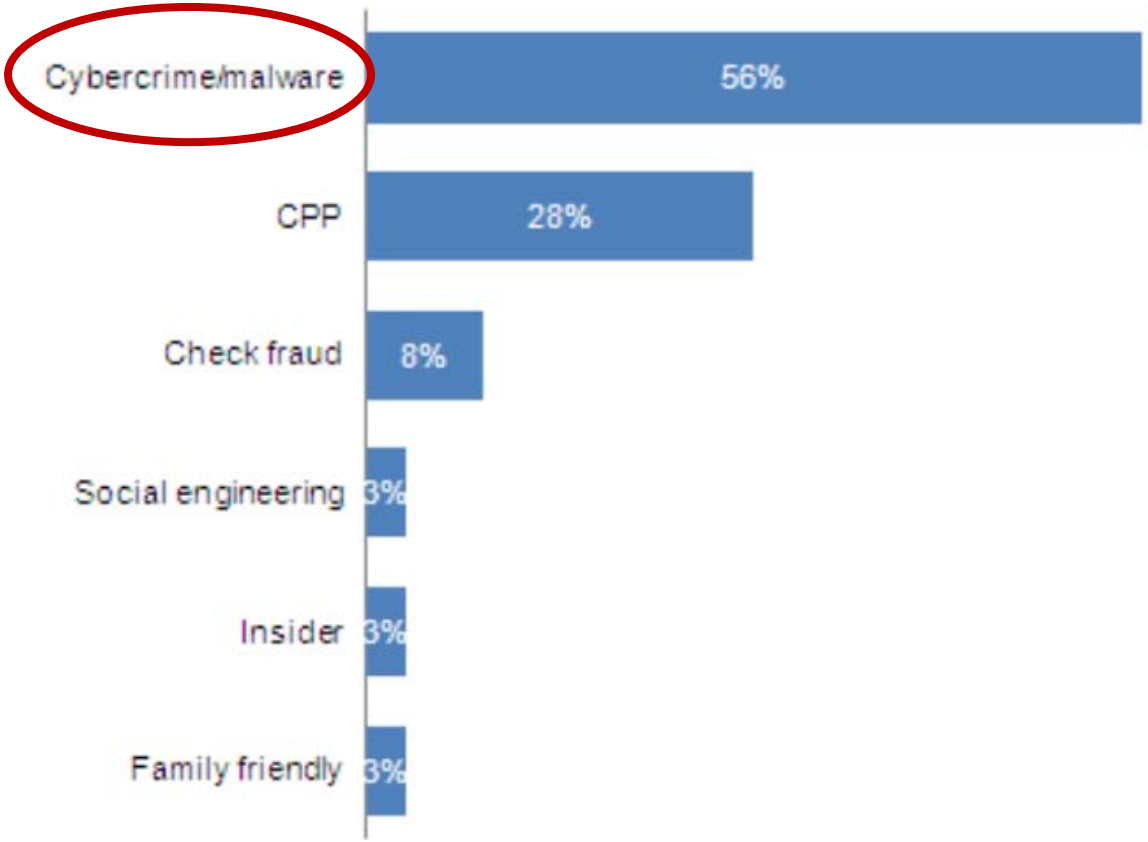
50%

Percent of malware designed to compromise credentials

Source: Aite Group

Online Fraud And Malware Are Greatest Threat

Top Concerns Reported by Financial Institutions



Source: Aite Group interviews with 32 North American FIs

Insider Threat Defined

Insider Threat

Someone who has trust and access and acquires intellectual property and/or data in excess of acceptable business requirements.

They do so:

- Maliciously
- Accidentally
- By being compromised

Employee Attitudes Towards Data

Insiders

- 70% of employees plan to take something with them when they leave the job
  - Intellectual Property: 27%
  - Customer data: 17%
- Over 50% feel they own it

Source: November 2010 London Street Survey of 1026 people, Imperva

Human nature at work?

- 70% of Chinese admit to accessing information they shouldn’t
- 62% took data when they left
- 56% admit internal hacking
- 36% feel they own it

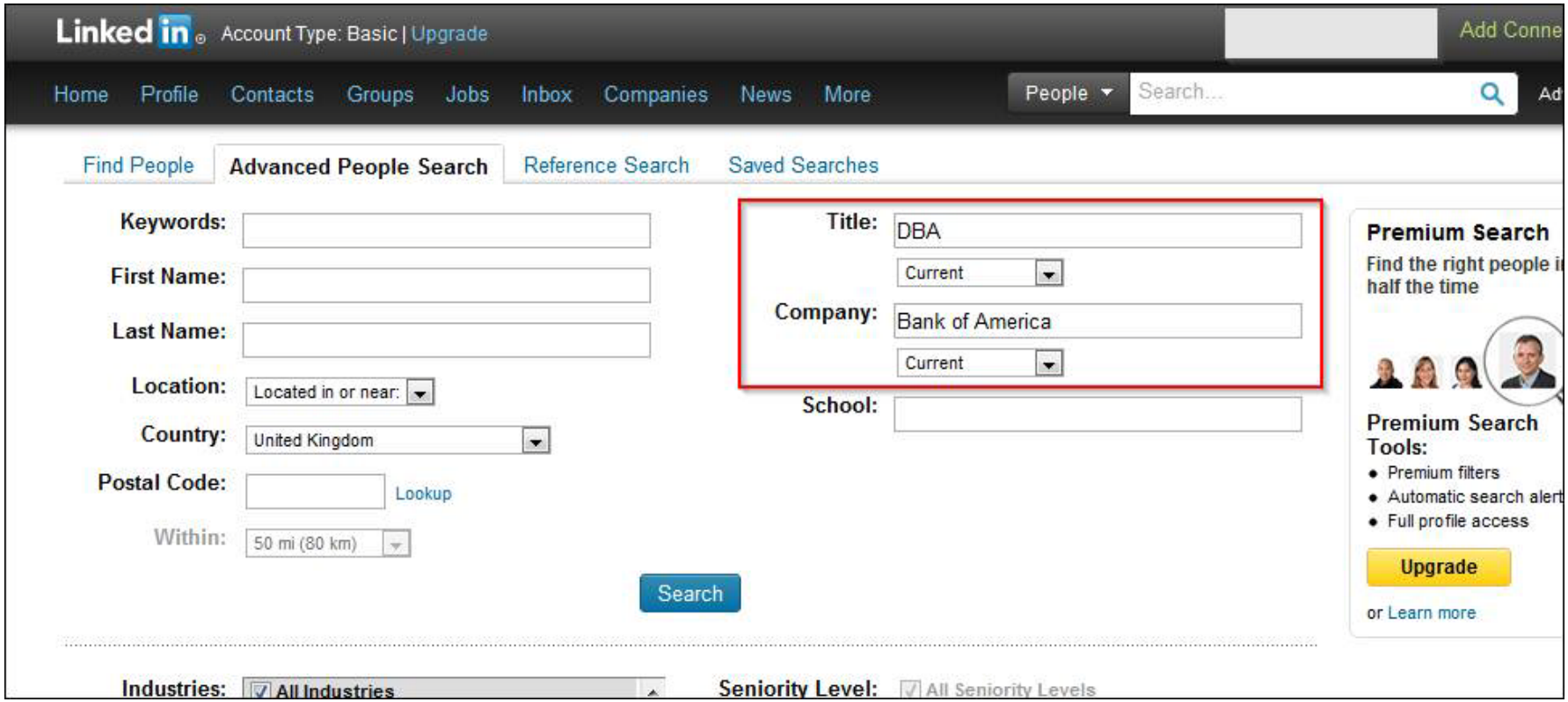
Source: February 2011 Shanghai and Beijing Street Survey of 1012 people, Imperva

Compromised Insider Defined

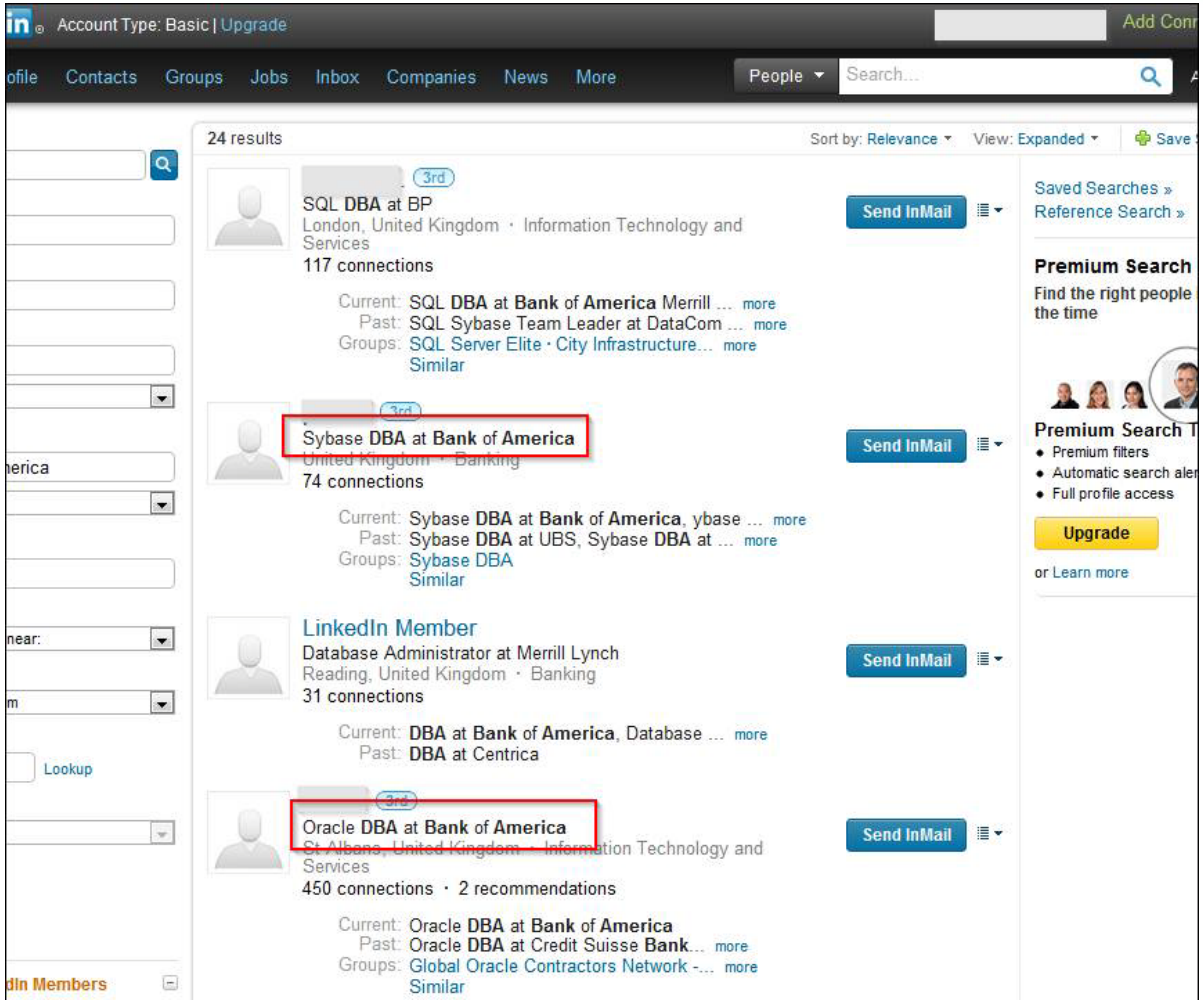
Compromised Insider

A 3rd party who gains access and acquires intellectual property and/or data in excess via client infection. The client, often employees in government, military or private industry, are **unknowing accomplices** and have **no malicious motivation**.

With Social Networks, Smart Bombing Is Not Hard



With Social Networks, Smart Bombing Is Not Hard

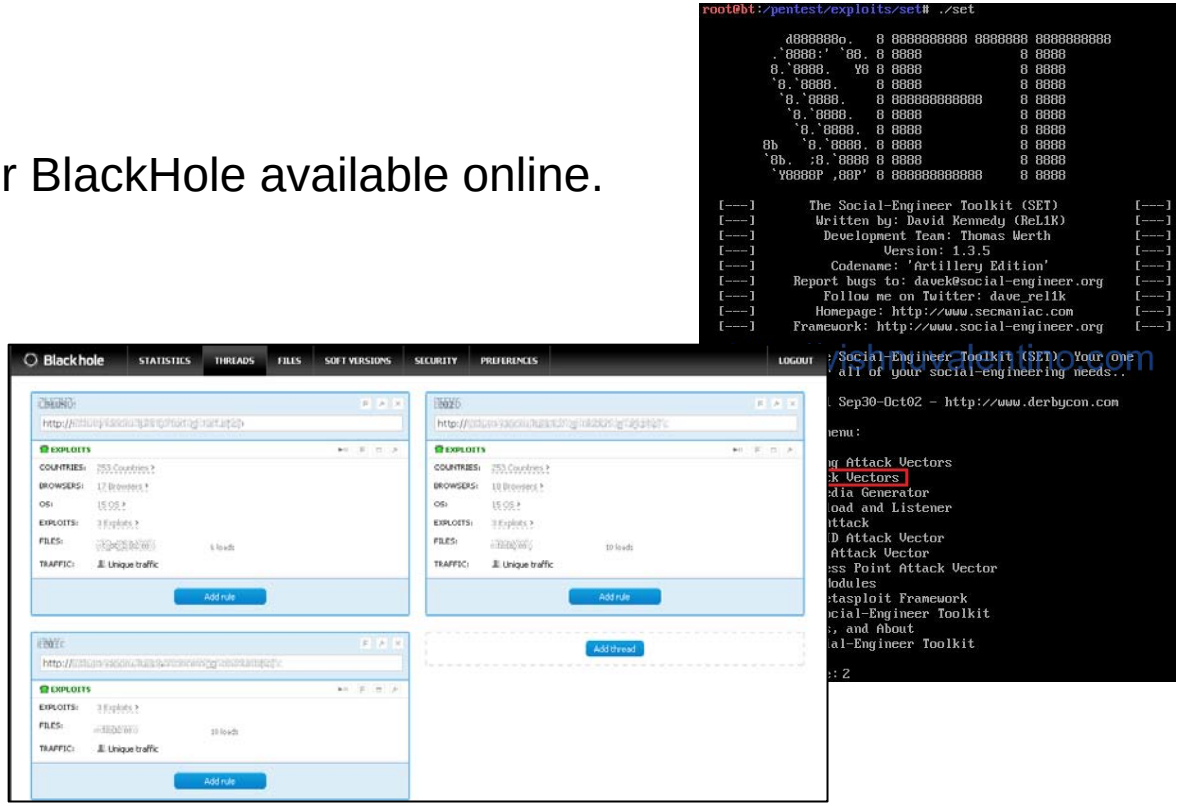


Industrialized Approach

Specialized Frameworks and Hacking tools such as BlackHole 2.0 and others, allow easy setup for Host Hijacking and Phishing.

How easy is it ?

For $700: 3 month license for BlackHole available online. Includes support!



Putting Things in Perspective

"Less than 1% of your employees may be malicious insiders, but 100% of your employees have the potential to be compromised insiders."

Source: http://edocumentsciences.com/defend-against-compromised-insiders

Security is like onions and ogres…

…it has layers.

But today's threats require new layers of security!

Anatomy of an Attack

South Carolina Department of Revenue

Don’t Be the Next Headline

Report: Hacker breached SC database 2 ways

Marshall Heilman of Mandiant said the attacker tricked a user in the Department of Revenue's system into opening a file that then allowed the hacker to access the system, according to a report Wednesday from the Post and Courier of Charleston (http://bit.ly/PXPebX).

South Carolina hired Mandiant last month after learning that more than 3.6 million tax returns going back as far as 1998 had been improperly accessed on a Department of Revenue server. Officials later said that about 657,000 business returns were also hacked, and Revenue officials told the State newspaper (http://bit.ly/QnINP) that the number of hacked returns had risen to 3.8 million.

Jim Etter, director of the Department of Revenue, told state senators in a hearing last month that about 250 employees had credentials to access the database. Nearly 700,000 people have signed up for free credit monitoring because of the hacking incident.

Timeline of the Attack

Report: Hacker breached SC database 2 ways

Records lost: 4M
Population: 5M
= 80%

Targeted, efficient, undetected

Attacker steals login credentials via phishing email & malware

13-Aug-12

Attacker logs in remotely and accesses the database

27-Aug-12

Additional reconnaissance, more credentials stolen

29-Aug-12 - 11-Sept-12

Attacker steals the entire database

12-Sept-12 - 14-Sept-12

What's the Bill?

- $500k – Mandiant's services
- $12M – Experian credit monitoring for citizens
- $800k – Improved security monitoring
- $100k – External legal fees
- $150k – PR campaign to restore image
- $750k – Cost to notify out-of-state taxpayers
- **= $14.3M TOTAL**

How Did This Happen?

Problem: Most organizations chase the mice and don't focus enough on protecting the cheese.

- Much of security budgets spent on:
  - NG-FW, IPS/IDS
  - Virus prevention

- Front-line/end-user defenses must be 100% accurate, since if only 1 mouse gets past them the cheese is gone.

Defending Yourself

Traditional Security Doesn't Stop Today's Threats

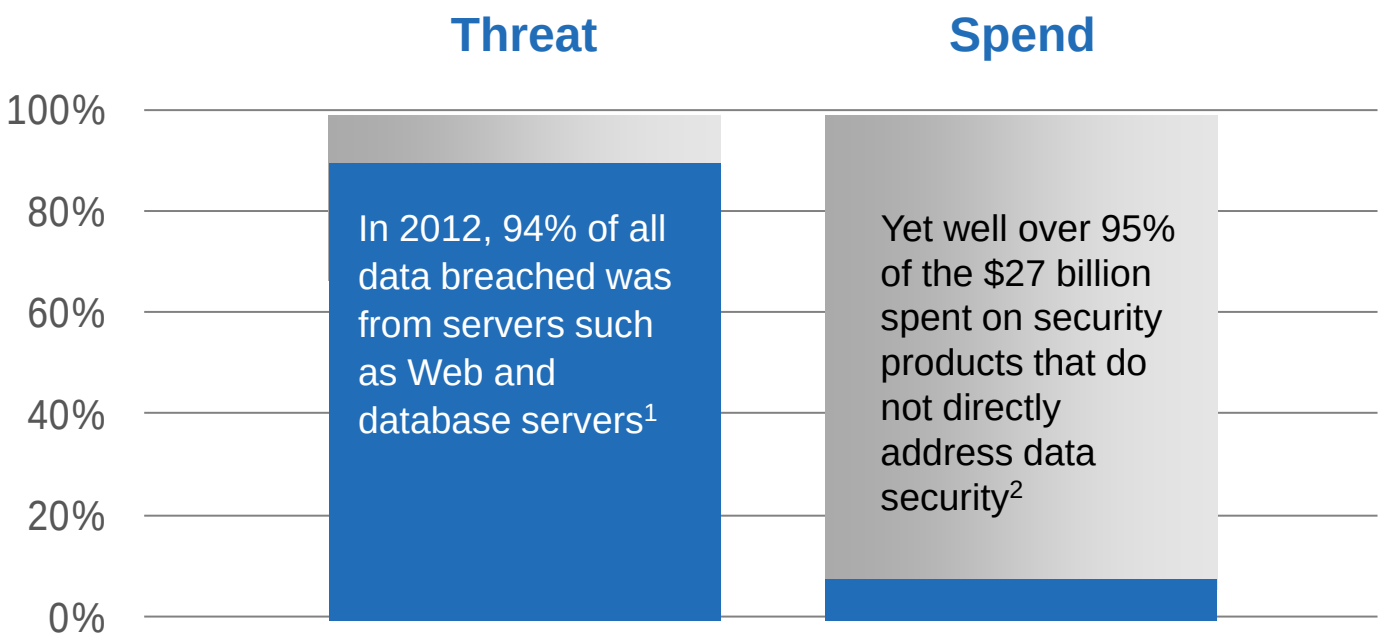
What helped get us secure…

- Router ACLs
- Network Firewalls
- IDS and IPS
- VPNs
- Anti-Virus

Is not keeping us secure

- SQL Injection
- (XSS) Cross-site Scripting
- Remote File Inclusion
- Cross-site Request Forgery
- Business Logic Attacks
- Fraud Malware

Why Haven't We Solved This Problem?



[1] 2012 Data Breach Investigations Report (Verizon RISK Team in conjunction with the US Secret Service & Dutch High Tech Crime Unit)
[2] Worldwide Security Products 2011-2014 Forecast (IDC - February 2011)

How to Stop Hacktivism, Fraud, DDoS

Correlated Attack Validation

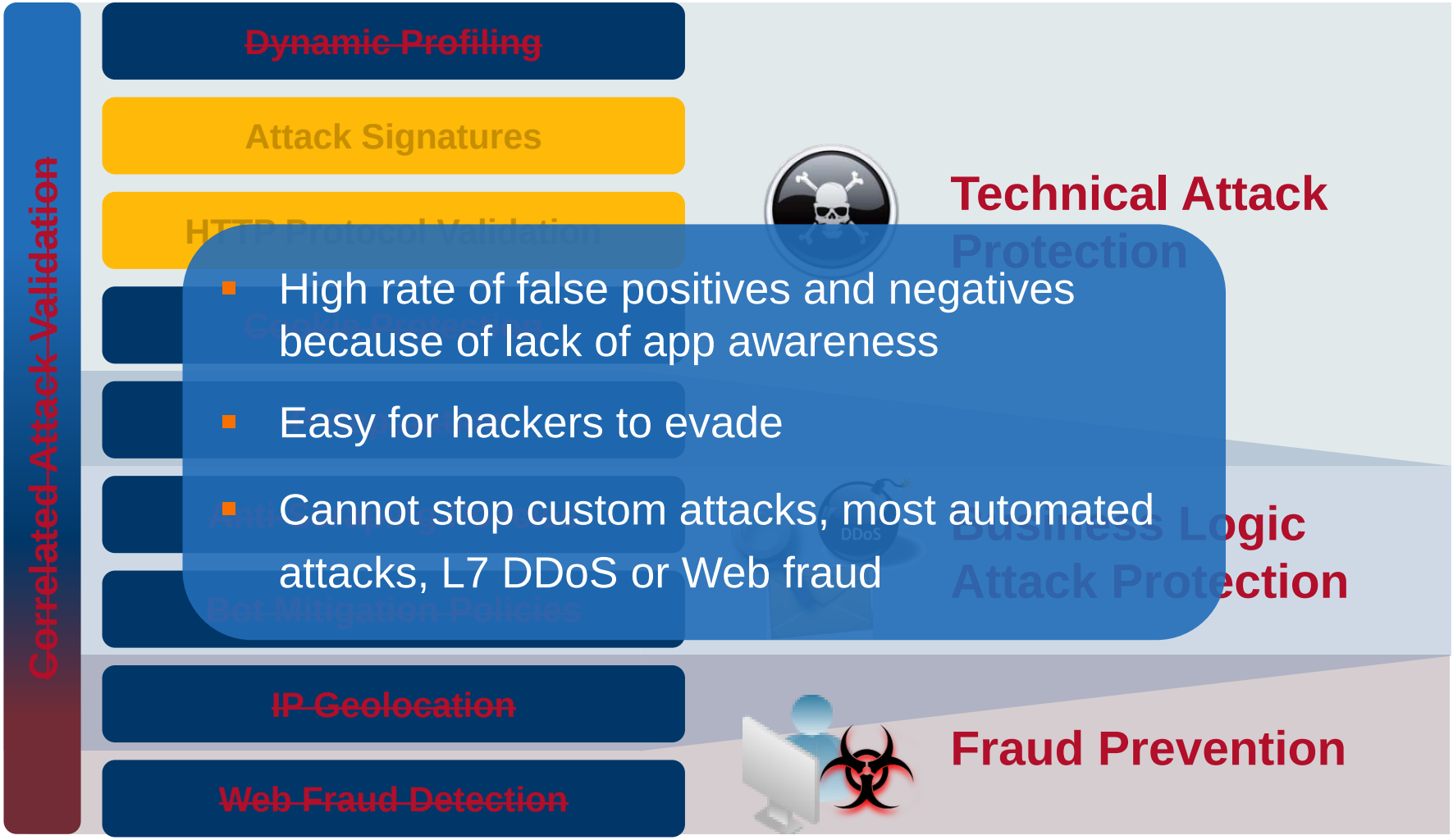
- Dynamic Profiling
- Attack Signatures
- HTTP Protocol Validation
- Cookie Protection
- IP Reputation
- Anti-Scraping Policies
- Bot Mitigation Policies
- IP Geolocation
- Web Fraud Detection

Technical Attack Protection

Business Logic Attack Protection

Fraud Prevention

IPS & NG Firewall Web Security Features



Understand Data and What Users Do With It

Discover and classify sensitive information

Build security policies

Review and rationalize access rights

Audit, analyze, and alert on access activity

Look for unusual behavior

Identify and remediate compromised devices

What's the Lesson?

Threats have evolved – so should your security portfolio!

Thank You

Doug Smith, Region Sales Mgr Canada
doug.smith@imperva.com
416.800.7644