Exploring Three Modern Threat Vectors
Malicious Insiders, Industrialized Hacking and APTs

Brian Contos, Director Global Security Strategy and Risk Management, McAfee

November 2010
Motives

Why do you rob banks?

NOW
Money AND Politics

THEN
Curiosity AND Excitement

Willie "The Actor" Sutton
(1901–1980)
Consequences

Revenue, Penalties, National Security

Economic

Regulatory

Defense
Position

Sharing: Education, Awareness, Perspectives

Not a Product Pitch

Not a Company Pitch
Insiders

Anything done unintentionally can also be done intentionally – with greater impact

Low-tech Trumps Hi-tech

Trust & Access
“It is very important to concentrate on hitting the U.S. economy through all possible means.”
– Osama Bin Laden
Insiders Convicted of Espionage

Aldrich H. Ames – began working for the CIA in 1962. He is currently serving life without parole.

Robert P. Hansen – began working for the FBI in 1976. He is now serving life without parole.

Ronald W. Pelton – began working for the NSA in the early 1960s. He is serving three consecutive life sentences.
Espionage Motivations

69%  Money is the primary motivator
56%  Money is the only motivator
27%  Disgruntlement or revenge
22%  Ideology
17%  Desire to please
12%  Excitement
05%  Coerced
04%  Importance
### Espionage Dollars

More than 50% < $100k
- 11% received < $1,000
- 17% received $1,000 to $9,999
- 26% received $10,000 to $99,999
- 12% received $100,000 to $999,999
- 04% received > $1,000,000

---

Johnny Depp’s Character, Agent Sands in the movie *Once Upon a Time in Mexico*

“I couldn't find a briefcase small enough for 10,000 dollars in cash…so I put it in this lunchbox.”
Industrial Revolution

19th century
Mass Production

Automation, Efficiency, Scalability
Old School

1997 EarthLink & AOL

2002 eBay

2003 Amazon, Banks, ISPs (Grammar)
Organized & Improved
- Tools
- Services
- Communities
- More underground
- Less sharing with public
- Drive-by-downloads
- Steal contacts & propagate
- Social engineering
- Candy drops

2007 –ish
“If crime didn’t pay there’d be no crime.” – G. Gordon Liddy

350,000+ Apps

100,000+ Apps
### How Big Are Applications

#### If Facebook Was a Country…

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>Population</th>
<th>Date of Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>China</td>
<td>1,340,110,000</td>
<td>October 18th 2010</td>
</tr>
<tr>
<td>2</td>
<td>India</td>
<td>1,189,030,000</td>
<td>October 18th 2010</td>
</tr>
<tr>
<td>3</td>
<td>Facebook</td>
<td>500,000,000</td>
<td>October 18th 2010</td>
</tr>
<tr>
<td>4</td>
<td>USA</td>
<td>310,504,000</td>
<td>October 18th 2010</td>
</tr>
<tr>
<td>5</td>
<td>Indonesia</td>
<td>237,556,363</td>
<td>October 18th 2010</td>
</tr>
<tr>
<td>6</td>
<td>Brazil</td>
<td>193,670,000</td>
<td>October 18th 2010</td>
</tr>
</tbody>
</table>
Malware Continues to Be the Biggest Threat to Enterprises and Consumers

Number of malware samples in our database

New pieces of malware per day:
2007: 16,000
2008: 29,000
2009: 46,000
2010 so far: 60,000
We have seen new botnet infections hold steady at around six million per month.
Carbon Footprint of Spam

• Over **62 trillion** email spam messages a year
• **33 billion** kilo-watt-hours per year (2.4 million homes in the U.S.)
• Greenhouse gases equivalent to **3.1 million** passenger cars
Botnets By The Numbers

- Number of Systems: 160,000
- Number of CPUs: 320,000
- Bandwidth: 500 Gbps

- Number of Systems: 500,000
- Number of CPUs: 1,000,000
- Bandwidth: 1,500 Gbps

- Number of Systems: 6,400,000
- Number of CPUs: 18,000,000+
- Bandwidth: 28 Terabits
- Facilities: 230 Countries
Research and Destroy

- Virtual machine Detection
- Line-by-line debugger detection
- Re-writes host file
- Multi-packed, one time, encrypted
- Rootkits
- Fuzzing
- Reverse Engineering
- Code Auditing
Industrialized Hacking Maturity Model

Hacking Is a Profitable Industry

- Researching Vulnerabilities
- Developing Exploits
- Growing Botnets
- Exploiting Targets
- Consuming

- Direct Value—i.e. IP, PII, CCN
- Command & Control
- Malware Distribution
- Phishing & spam
- DDoS
- Blackhat SEO

- Growing Botnets and Exploiting Vulnerabilities
- Selecting Targets via Search Engines
- Templates & Kits
- Centralized Management
- Service Model

Roles
Optimization
Automation

It’s not fair and it’s not personal; it’s just business.
Cyber Criminal Family

More than a Decade of Experience, Relationships and Trust Groups

• Carders
• Hackers
  – Targeted intrusion for harvesting data, develop exploits and toolkits, decryption services, anonymity services, consulting
• Spammers
• Bot herders
• Money Launders
• Renegade Hosters
• Malware developers
• Document forgers
• Specialized hardware providers
• Back office services—FW, AV, Test Beds
Black Hat SEO

2010’s Most Dangerous Internet Searches

60% of Popular Google Searches Yield Malicious Sites in First 100 Results

Cameron Diaz  Julia Roberts  Jessica Biel  Gisele Bündchen
Pricing

Price

Circumstances

Competition

Exclusivity

Volume

Quality

CVV2 $1
- Card Number
- Expiration Date
- Cardholder Name
- Address
- CVV2 Security Code

Full (Wallet) $10
- CVV2
- Date of Birth
- Mother’s Maiden Name
- Social Security Number
- Place of Birth

Source: Secret Service
Zeus: An Abbreviated Love Story
aka: Zbot, PRG, Wsnpoem, Gorhax and Kneber

- Discovered July 2007—More recent versions with over 150 variants
- Doesn’t self propagate—requires spam, phishing, drive-by downloads
- C&C 196 countries; 2,400 companies impacted, 3.6M PCs in U.S. alone

- Targeted: email accounts, social networking sites and banking
- Control, steal credentials, transfer funds
- Man in the Browser

- Kit: $700-$4,000 USD plus add-ons & plug-ins $500-$10,000 USD
- Binary generator to evade detection
- Copy protection and license keys

- Money mules in U.S. recruited and paid on commission
- Create bank accounts using fake documents and phony names
- Wire fund to Eastern Europe or smuggle cash

- Stole around $70M USD
- 100+ arrested across U.S., U.K., & Ukraine 2010
- Charges of bank fraud & money laundering
Zeus: Graphical spam

eFax | FedEx | IRS | Social Security Administration | USPS | Western Union

**UNITED STATES POSTAL SERVICE**

Hello!

Unfortunately we failed to deliver the postal package you have sent on the 19th of September in time because the recipient’s address is erroneous.

Please print out the shipment label attached [USPSLabel.doc] and collect the package at our office.

United States Postal Service

**eFax**

The fax message is attached to this e-mail!

**FedEx**

Dear,

Unfortunately we failed to deliver the postal package you have sent on the 27th of July in time because the recipient’s address is erroneous. Please print out the invoice copy attached and collect the package at our office.

* This site is protected by copyright and trademark laws under US and international law. All rights reserved © 1995-2010 FedEx.
Who sends the most Zeus spam?

- **eFax Zeus Campaign**
  - United States: 60%
  - Vietnam: 26%
  - Brazil: 7%
  - India: 7%

- **USPS Zeus Campaign**
  - United States: 90%
  - China: 3%
  - France: 3%
  - United Kingdom: 2%
  - Brazil: 2%

- **SSA Zeus Campaign**
  - Russia: 35%
  - India: 33%
  - Ukraine: 16%
  - Korea: 16%
SMS: Common, Cheap Two-factor Authentication for Financial Institutions

1. User logs on the banking site
2. Starts a money transfer
3. Bank asks for additional code
4. Code is sent to user’s phone via text message (SMS)
5. User enters the code to validate the transaction

Remember Zeus Has Full Access to the Victim’s Computer

1. Inject additional fields into an online banking webpage asking for the user’s phone number and model
2. Zeus then sends that user’s phone a link to download a “security add-on” (currently works on BlackBerry and Symbian-based phones)
3. The code is malware that intercepts/forwards SMS messages
4. Full operational capabilities on the account
The Countermeasures

- Reputation
- Reduce complexity
- Wolverines not mosquitoes
- Damn the whales—save the plankton
- Anti-social engineering

“The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had.”

Eric E. Schmidt, Chairman of the Board and CEO Google
**APT**

**Industrialized Hacking**

**Advanced:** Custom exploits and other mature tools

**Persistent:** Not a crime of opportunity—on a mission

**Threat:** They have money and they are motivated
APT Maturity Model

**Actors**
- Nation-States
- Insiders & Ex-employees
- Unscrupulous Competitors
- Terrorist/Activist/Criminal Organizations

**Motives**
- Political
- Economic

**Targets**
- Large corporations
- Critical infrastructure
- Governments
- Academic & Media

**Goals**
- Stealth intrusion, backdoors
- Sensitive data, Monitoring, Sabotage
- Leave no traces
Operation Aurora in 12 Steps

• Zero-day vulnerability was discovered
  – Microsoft IE DOM Operation Memory Corruption Vulnerability (CVE 2010-0249)
• Malware written (~July 2009)
• Targets acquired (Google, others) mostly in China/Taiwan
• Users received web link via social engineering attack from trusted source
• Users clicked on web link
• Web page had obfuscated Javascript which included shellcode to exploit 0-day vulnerability
• Exploit downloaded additional shellcode from servers (predominantly in TW) disguised as an image (ad.jpg), decrypted it, and executed it—spawning numerous other files (a.exe, b.exe, etc) that were executed, including backdoors (rasmon.dll, securmon.dll, etc.)
Operation Aurora in 12 Steps

• The backdoor phoned home to C&C servers (predominantly in TW) over TCP 443 (non-SSL protocol)
• Attackers then had direct channel into the inside of the corporate networks

Persistent

• Once inside, attackers targeted administrators and cracked SAMs on local/domain controllers
• Attackers targeted repositories of intellectual property and installed additional backdoors
• Attackers pushed the files through traditional means (FTP/HTTP, etc.) back to their own servers

Threat
APT Type: Information Warfare

Using information to achieve a national objective

- Howard Schmitt—Cyber Security Coordinator (No)
- Firm Booz Allen (Yes)
- Over 100 nations have information warfare capabilities (according to FBI ‘08)
- Congress initiated a bill for $16B to combat cyber attacks
- October 2009 Department of Homeland Security said it would hire 1,000 security experts

Not just states; non-state entities can be leveraged
Not a Super Power—Not a Problem

- **December 2008**: Attacks by Mugabe Gov. in Zimbabwe
- **December 2008**: Israeli Defense Forces and Hamas
- **January 2009**: A DDoS attack on several Kyrgyzstan’s
- **June 2009**: Iranian government sites attacked
- **June 2009**: President of Tatarstan has websites attacked
- **July 2009**: Attacks on S. Korean sites
Technology becomes an equalizer...again

- Inexpensive
- Anonymous
- Simple
- Excellent Range
- State & Non-state Participants
- Espionage
- Propaganda
- Attack

“God made man, but Samuel Colt made them equal.”
• Estonia—May 2007: Three weeks of cyber attacks following the removal of a bronze soldier
• Russian mafia and Russian sympathizers in Latvia, Ukraine, and the US (80,000 IP address sources)

• Georgia - August 2008: Kinetic + Non-kinetic attacks where radio station towers were being shot by tanks, as DDoS was taking out online capabilities

• Others attacks
  • 2007 Lithuania, Ukraine
  • 2009 Kyrgyzstan
April 2008
- CNN reports on Tibet

- 5,000 Chinese forums recruit “patriots” antiCNN.exe

- CNN blocks traffic from .CN
- Double win
The best poker players walk a tightrope between their business sense and their passion. As professionals, they seek out the most profitable opportunities and control as many factors as possible to create a positive result. As gamblers, they want the risk and excitement of something important on the line with the outcome in the balance.

—Michael Craig Full Tilt Poker Blog