Dissecting the Modern Threatscape
Malicious Insiders, Industrialized Hacking, and
Advanced Persistent Threats

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

October 2010
AGENDA

Insiders

Industrialized Hacking

Advanced Persistent Threats
Motives

Why do you rob banks?

Now
- Money
- Politics

Then
- Curiosity
- 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

Low-tech Trumps Hi-tech

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

Trust & Access
Who Are They

Why hack when you can recruit…

“It is very important to concentrate on hitting the U.S. economy through all possible means.”

– Osama Bin Laden

…or plant?
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.”
Downloaded to McAfee.
Uploading

Malware

Unauthorized Software
Moonlighting

Resource Theft Liability
19th century mass production

Automation, efficiency, scalability
New School

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

350,000+ Apps

100,000+ Apps

Most widely deployed apps in the world
Mature Malware

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

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
- Blackhat SEO

Automation

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

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 Lauunders
- Renegade Hosters
- Malware developers
- Document forgers
- Specialized hardware providers
- Back office services – FW, AV, Test Beds
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
Beyond CCN and PII
User with IE vulnerability visits website infected with Operation Aurora

EXE disguised as JPG, encrypted 3x with different keys, unpacks a dozen different files

Custom protocol behaves like SSL, port 443, evades detection, and gains access to highly valuable corporate IP
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
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
5th Dimension of Warfare?

- Land
- Sea
- Air
- Space
- Cyber
Cyber is an element of, and support for Intelligence Gathering | Operations | Communication
Money or Information
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
1994: The Internet is open to China’s Public Red Hacker Alliance soon follows Chinese Nationalist Hacker Network

1998: Independent cells unite Rioting in Jakarta, Indonesia where the Chinese were being targeted

1999: Taiwan advocated being independent of mainland China

2000: Attack Japan after WWII War crimes case was lost
If accepted there should be increased reconnaissance and intelligence activity…

…and there is - Taiwan, France, Germany, Britain, Australia, New Zealand, India and the US have suffered critical data theft
Espionage

Allen Dulles, “The essence of espionage is access”

2003
Titian Rain

April 2009 - $300 Billion Fighter (F-35)
Equivalent to about **4,600 tanks**
The US has about 8,000
Patriotic DDoS

April 2008
CNN reports on Tibet

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

CNN blocks traffic from .CN
Double win