

### It Came Out of the Sky....Now


- Mid-December 2009 – 34 networks (including Google, Yahoo, Adobe, Symantec, Northrop Grumman, Dow Chemical, and Juniper Networks) were hit by attacks originating from China
- Gmail accounts of human rights activists were targeted
- 'Operation Aurora' attackers used multiple exploits and multiple, tailor-made Trojans for different targets.
- IP addresses used "were associated with groups that are either directly employed agents of the Chinese state or amateur hackers used as proxies."
- Spear phishing, Zero-day Explorer exploit involved
- *This was news? Its routine, happens all the time. Yawn.*
- What **is** news? *That several of the companies admitted it.*

Attacker Profiles 3

### It Came Out of the Sky....Then

- 'Titan Rain' – U.S. government's name for a series of coordinated attacks on American computer systems going on since 2003. U.K. military networks were also attacked.
- The director of the SANS Institute said that the attacks were "most likely the result of Chinese military hackers attempting to gather information on U.S. systems".
- Systems breached included Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, and NASA. Breaches are not typically reported, however.
- .gov netblocks were heavily scanned. *A lot...*


Attacker Profiles 4



## Vendorspace

- The security vendor community responded with case studies, white papers, and a name: "Advanced Persistent Threat (APT) is a sophisticated and organized cyber attack to access and steal information from compromised computers. APT attacks target the Defense Industrial Base (DIB), financial industry, manufacturing industry, and research industry. The attacks used *are not very different* from any other intruder. The main differentiator is the APT intruder's perseverance and resources."

Attacker Profiles 5



## Firewall logs for July 29, 2005

| Source IP       | Hits    | Target | Port | Time | Source                   | Comment            |
|-----------------|---------|--------|------|------|--------------------------|--------------------|
| 129.93.8.213    | 123,984 | 1      | 1250 | 6m   | Nebraska U               | Trojan fishing     |
| 61.152.93.117   | 91,773  | 2      | many | 11h  | China.net                | (A)                |
| 222.76.230.3    | 71,999  | 1      | 80   | 23h  | China.net                | (B)                |
| 61.54.155.58    | 53,570  | 2      | many | 20h  | China backbone           |                    |
| 131.123.194.174 | 52,401  | 1      | 2100 | 9h   | Kent State               | Oracle FTP exploit |
|                 |         |        | 2727 |      |                          | Oracle exploit     |
| 61.134.43.60    | 36,045  | 1      | many | 18h  | China.net backbone       |                    |
| 61.152.91.33    | 34,935  | 1      | many | 23h  | China.net                |                    |
| 220.194.56.30   | 31,194  | 2      | many | 5h   | China Unicom             |                    |
| 61.156.38.36    | 29,662  | 1      | many | 23h  | China backbone           |                    |
| 61.152.96.197   | 23,998  | 1      | many | 23h  | China.net                |                    |
| 61.128.162.232  | 20,092  | 1      | many | 16h  | China.net backbone       |                    |
| 205.177.72.216  | 16,539  | 1      | many | 4h   | US                       |                    |
| 220.194.56.52   | 15,656  | 2      | many | 7h   | China Unicom (C)         |                    |
| 218.5.76.47     | 15,146  | 2      | many | 15h  | China.net backbone       |                    |
| 67.18.208.148   | 14,726  | 2      | many | 1h   | undetermined             |                    |
| 61.152.96.219   | 14,040  | 2      | many | 13h  | China.net                |                    |
| 192.220.92.92   | 11,439  | 1      | many | 23h  | US                       | Trojan fishing     |
| 218.6.135.47    | 11,142  | 2      | many | 6h   | China.net backbone       |                    |
| 219.138.184.219 | 10,910  | 2      | many | 23h  | China.net backbone       |                    |
| 218.61.33.116   | 10,536  | 2      | many | 3h   | China backbone           |                    |
| 61.152.92.102   | 6,963   | 2      | many | 2h   | China.net                |                    |
| 218.85.132.19   | 4,960   | 1      | many | 6h   | China.net backbone       |                    |
| 219.139.32.243  | 4,806   | 2      | many | 13h  | China.net backbone       |                    |
| 211.115.111.151 | 2,863   | 2      | many | 32m  | DAKOM Korea              |                    |
| 211.84.240.9    | 2,503   | 1      | many | 21h  | China Kaileng University |                    |
| 210.51.192.157  | 2,414   | 2      | many | 11m  | China net.com            |                    |
| 222.77.185.246  | 2,294   | 2      | many | 13m  | China.net backbone       |                    |

Attacker Profiles 6



## China Attacks Rolls-Royce

**Rolls-Royce secrets under attack from China's spies**  
December 3, 2007 <http://www.snp.com/securitynews>


- Rolls-Royce** - Britain's largest engineering company
- Royal Dutch Shell** - World's 2<sup>nd</sup> largest oil multinational fell victim to sustained assaults as part of a Chinese campaign to obtain confidential commercial information. News of the attacks came after a warning by Britain's security services that China is sponsoring espionage against vital parts of the British economy, including breaking into big companies' computer systems. The infiltration of the Rolls network is thought to have **occurred remotely after a specially tailored Trojan was downloaded** into the site.

Attacker Profiles 7




## China Clones Rolls-Royce

April 2009 - Luxury British car maker Rolls-Royce threatens legal action after a Chinese company unveiled a prototype limousine that is a dead ringer for the Rolls-Royce Phantom and which would sell for a fraction of the price


Attacker Profiles 8



## Threat: Operationally Defined


- Long-term pattern of targeted sophisticated hacking attacks aimed at governments and companies.
- It also includes internal sources, whether from a zero-day exploit, misconfigured networked devices [computers, printers, scanners, etc.], one of the many holes punched in the security layers, or some special dufus on the third floor who just doesn't get it.
- Bottom line is: There are people smarter than us, they have more resources than us, and they are coming for us. *It's not anything new.*

Attacker Profiles 9




## Class Outline

- A. The Internet, TCP/IP, and PANs, LANs, CANs, MANs, & WANs
- B. Ping sweeps, port scans, traceroute, & OS fingerprinting
- C. **Attacker Profiles**
- D. Attack Points
  - Human access
  - Physical access
  - LAN (insider) access
  - Remote (Internet) access
  - Wireless access
- E. Anatomy of an Attack
  - Step 1: Target survey
  - Step 2: Vulnerability assessment
  - Step 3: Vulnerability exploitation
  - Step 4: Maintaining access/persistence
  - Step 5: Covering tracks
- F. Physical access attacks
- G. The future: emerging technologies





Attacker Profiles 10



## Potential Attacker Profiles


Identify potential attackers in order to understand motivations and capabilities. Some general types:

- Curious Hacker
- Script Kiddie
- Black Hat
- Disgruntled Employee
- Economic Opportuni\$t - cyber crime
- Government Sanctioned - cyberwar, cyberterrorist



How is cyber any different?  
"Who are those guys?"

Attacker Profiles 11




## Potential Attacker Profiles

### Curious Hacker

- Low to Medium level of expertise
- Possible technical background
- Accesses system from internal LAN/Internet
- Attacks system in order to learn from experimentation with hacking tools & concepts
- Motivation is for disclosure or modification rather than deletion of data, e.g. 'because it's there'
- Level: Target-of Opportunity Attack


Attacker Profiles 12




## Potential Attacker Profiles

### Script Kiddie

- Medium level of expertise
- Copy/use tools developed by others
- Possible technical background
- Accesses system from Internet
- Motivation is defacement and publicity
- Level: Intermediate Attack



Attacker Profiles 13




## Potential Attacker Profiles

### Black Hat

- Medium to High level of technical expertise
- Accesses System: internally or Internet
- Develops tools, finds vulnerabilities
- Primary motivation: disclosure of sensitive information rather than modification or deletion
- Additional motivations include potential disruption and denial of service
- Level: Sophisticated attack

Attacker Profiles 14




## Potential Attacker Profiles

### Disgruntled Employee

- Objective: wreak havoc via data deletion/modification of data, access denial (SF City Network Admin)
- Low to medium level of technical expertise
- High level of experience with system
- User has account and password access to system
- Trusted User able to cause damage to critical systems
- Level: Intermediate Attack
- In 2000, a disgruntled employee rigged a computerized control system at a water-treatment plant in Australia, releasing over 200,000 gallons of sewage into parks, rivers and Hyatt hotel grounds

Attacker Profiles 15




## Potential Attacker Profiles

### Economic Opportunist

- Objective is to steal sensitive information
- Medium level of technical expertise
- Accesses System internally or from Internet
- Primary motivation is disclosure of sensitive information, used to gain financial access
- Range: 419 fraud to Bankcard processing
- Level: Intermediate attack
- Median loss (2008):
  - \$3,000 Check fraud
  - \$2,000 Confidence fraud
  - \$1,650 Nigerian, 419, advance fee letter fraud

Attacker Profiles 16




## Potential Attacker Profiles

### Government Sanctioned


- Objective is to steal sensitive information
- High level of technical expertise
- Accesses System internally or Internet
- Primary motivation is disclosure of sensitive information rather than modification or deletion
- Additional motivation is potential disruption and denial of service – or worse
- Level: Sophisticated attack

**Want a recent example?**

Attacker Profiles 17



## Stuxnet Worm



### Stuxnet targeted Iran's Nuclear program


NY Times Jan 15, 2011

Most sophisticated cyber weapon yet deployed

Targeted Siemens SCADA controllers (P.L.C.) running Step 7


- Recorded normal operations data
- Played it back to fool operators
- Sent centrifuges spinning wildly out of control

984 nuclear centrifuges damaged  
20% of Iran's capacity  
Likely - Israeli & US operation



**Is a missile any different?**  
*How?*

Attacker Profiles




## Outliers

- Former US Cycling star Landis sentenced for Trojan attack
- French court hands down 12-month suspended sentence
- Landis's former coach Arnie Baker given same sentence
- Plot to steal documents from the country's national anti-doping laboratory (LNDD) using Trojan in attempt to clear name. Landis tested positive for testosterone during 2006 Tour de France, became first rider in history to be stripped of a Tour de France winner's title for such an offence.
- Computer consultant Alain Quiros carried out the attack, sentenced to 6 months in prison and 4,000 € fine. Quiros worked for Kargus Consultants, which has been accused of creating malware to hack a variety of organizations in France, including Greenpeace on behalf of energy company EDF.

ITWorld.com 11/11/2011

Attacker Profiles 19




## Outliers

- Energy giant EDF used Trojans to spy on Greenpeace - Prison sentences and huge fine for use of malware
- The head of nuclear security at French energy giant EDF has been given a prison sentence, company fined 1.5 million € - guilty of spying on Greenpeace using Trojan malware.
- EDF runs 58 nuclear power stations in France and 8 in the UK, set out in 2006 to spy on the Greenpeace's then head of campaigns in France, Yannick Jadot. Hired Kargus Consultants, who used Trojans to attack Jadot's computer, stealing 1,400 documents relating to the organization's campaign against nuclear power.
- EDF's former security head, Pascal Durieux, a 3 year jail sentence with one suspended, while his deputy Pierre-Paul François was given 3 years with 30 months suspended.
- The head of Kargus, Thierry Lorho, given 3 years in jail with 2 suspended and a 4,000 € fine, technical expert Alain Quiros given 2 years suspended. TechWorld 11/11/11

Attacker Profiles 20




## Assault on Networks




|   |  |
|---|--|
| <b>Source</b> <ul style="list-style-type: none"> <li>Organized Crime</li> <li>Governments</li> <li>Business</li> <li>Education</li> <li>Hactivists</li> </ul> | <b>Targets</b> <ul style="list-style-type: none"> <li>Government</li> <li>Federal</li> <li>Local</li> <li>Industry</li> <li>Business</li> <li>Education</li> </ul> |
|---|--|

What is Missing?




Attacker Profiles 21

## Assault on Networks




|   |  |
|---|--|
| <b>Source</b> <ul style="list-style-type: none"> <li>Organized Crime</li> <li>Governments</li> <li>Business</li> <li>Education</li> <li>Hactivists</li> </ul> | <b>Targets</b> <ul style="list-style-type: none"> <li>Government</li> <li>Federal</li> <li>Local</li> <li>Industry</li> <li>Business</li> <li>Education</li> </ul> |
|---|--|

People



Attacker Profiles 22

## Context



- Criminal Activity
- Military Intelligence
- Competitive Intelligence
- Political/Social Agenda


Goals

- Information superiority
- Money
- Change

- Data is raw input
- Information is the meaning assigned to data
- Knowledge is an organized body of information

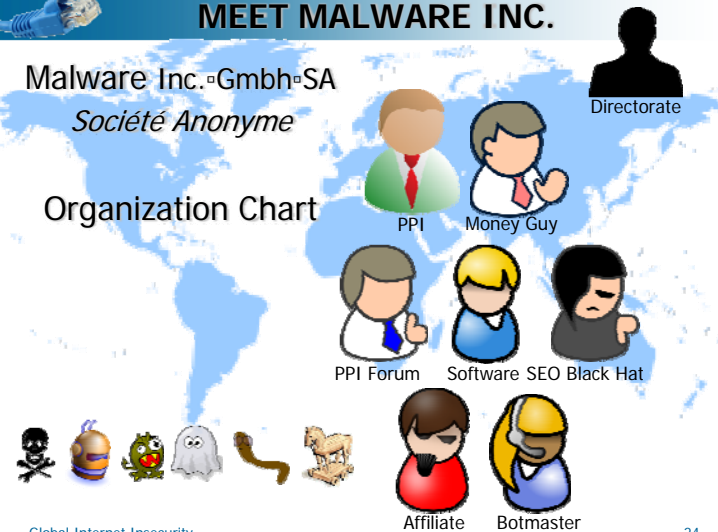
Attacker Profiles 23

## MEET MALWARE INC.




Malware Inc. "GmbH" SA  
*Société Anonyme*

Organization Chart




Global Internet Insecurity 24



## Attack Shift

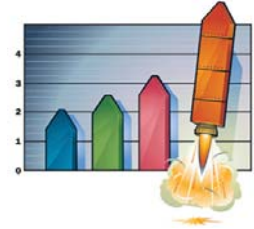
- Legacy goal – own a box, mess with it
- Modern goal – own multiple boxes
  - ♦ Make Money
- Essentially – attacking the enterprise
- Through vulnerable people
- Using the network as a weapon
- Technology can fix technology
- Technology can't fix people
- People are vulnerable (people are exploitive)
- There is no patch for human stupidity, cluelessness, greed, etc.

Attacker Profiles 25



## Focal Shift

- The focal point has changed from having the right technology to having the right people. Today, technology is easy.
- The automated defenses of a network, when implemented properly with best practices, for the most part, works.
- The security job market is



Attacker Profiles 26

