Cyber Security: Espionage and Social Networking

Presented by

SSA Elvis Chan
San Francisco Division

Federal Bureau of Investigation
Why is Cyber so Important?

<table>
<thead>
<tr>
<th>Year</th>
<th>World Pop.</th>
<th>Internet Users</th>
<th>% Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>6.12 billion</td>
<td>413 million</td>
<td>6.7%</td>
</tr>
<tr>
<td>2005</td>
<td>6.51 billion</td>
<td>1.03 billion</td>
<td>15.8%</td>
</tr>
<tr>
<td>2010</td>
<td>6.91 billion</td>
<td>2.03 billion</td>
<td>29.4%</td>
</tr>
<tr>
<td>2011</td>
<td>6.99 billion</td>
<td>2.27 billion</td>
<td>32.5%</td>
</tr>
<tr>
<td>2012</td>
<td>7.08 billion</td>
<td>2.51 billion</td>
<td>35.5%</td>
</tr>
<tr>
<td>2013</td>
<td>7.16 billion</td>
<td>2.71 billion</td>
<td>37.9%</td>
</tr>
<tr>
<td>2014</td>
<td>7.24 billion</td>
<td>2.92 billion</td>
<td>40.4%</td>
</tr>
</tbody>
</table>

http://www.internetlivestats.com/internet-users/#trend
We Will Discuss…

- Cyber Espionage
- Spear Phishing and Social Networking
- FBI-Private Industry Partnerships
“Our foreign adversaries and competitors are determined to acquire, steal, or transfer a broad range of trade secrets in which the United States maintains a definitive innovation advantage. This technological lead gives our nation a competitive advantage in today’s globalized, knowledge-based economy. Protecting this competitive advantage is vital to our economic security and our national security.”

“Economic Espionage and Theft of Trade Secrets are increasingly linked to the Insider Threat and the growing threat of cyber-enabled trade secret theft… Long gone are the days when a spy needed physical access to a document to steal it, copy it, or photograph it, where modern technology now enables global access and transmission instantaneously.”

Randall C. Coleman
Assistant Director, Counterintelligence Division, Federal Bureau of Investigation
Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, Washington, D.C.
May 13, 2014
**Statutes**

- **Economic Espionage** 18 U.S.C. § 1831
  - Whoever knowingly performs targeting or acquisition of trade secrets to knowingly benefit any foreign government, foreign instrumentality, or foreign agent
  - *must prove link to foreign country’s government*
  - Criminal penalty: 15 years and <$5M (individual) or $10M (corporation)

- **Theft of Trade Secrets** (Industrial Espionage) 18 U.S.C. § 1832
  - Whoever knowingly performs targeting or acquisition of trade secrets or intends to convert a trade secret to knowingly benefit ANYONE other than the owner
  - Criminal penalty: 10 years and <$250K (individual) or $5M (corporation)
Statutes

• Fraud and Related Activity in Connection with Computers 18 U.S.C. § 1030
  - Crime to commit, attempt or conspire to commit computer trespassing (e.g., hacking) in a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce (e.g., a worm, computer virus, Trojan horse, time bomb, a denial of service attack, and other forms of cyber attack, cyber crime, or cyber terrorism); trafficking in passwords for a government computer, or when the trafficking affects interstate or foreign commerce; and accessing a computer to commit espionage.
  - Criminal penalty: up to 10 years first offense and 20 years second offense
What is a Trade Secret?

Can be in all forms, both tangible and intangible, but it must cover these three areas:

1. Have potential or actual economic value
2. Not generally known to public (guarded)
3. Reasonably protected
Examples of Trade Secrets

• Software
• Marketing Plans
• Customer Lists
• Source Codes
• Pricing Information
• Technical Drawings
• Chemical Formulas
Methods for Targeting/Acquiring Trade Secrets

• Most common modalities for egress of data:
  - Portable devices
  - Email
  - Remote Access

• Print and walk

• The purchaser likely needs the information AND implementation
Espionage Indicators and Vulnerabilities

1. Unsolicited requests for information
2. Soliciting or marketing of services
3. Conferences, conventions, and trade shows
4. Official foreign visitors
5. Exploiting joint research
6. Foreign targeting of US visitors overseas
7. Exploiting of open source information
8. Abrupt resignations/unauthorized business activities
9. Suspicious downloading/emailing of data without proper authorization
10. Recruiting individuals from competitor companies
Most Targeted Sectors

- Information/Communications
- Military
- Dual-Use
- Advanced Materials and Manufacturing
- Healthcare, Pharmaceuticals and Related Technologies
- Agriculture
- Business Information
- Energy and Natural Resources
Who is Doing the Targeting?

- Insiders
  - Disgruntled employees
  - Employees looking for their “exit bonus”

- Competitors

- Foreign Intelligence Services
How Are They Targeting?

• Social/Insider Recruitment
  – Implausible coincidences
  – Eager stranger friendships
  – Deep interest in your work

• Online Social Engineering
  – Phishing/Spear Phishing

• Travel vulnerabilities!
  – Honeypots, unsolicited friends
Cyber Espionage Case Study

• May 19, 2014 first ever cyber-espionage case against Chinese military officials
• Indictment against five Shanghai-based officials, who have never set foot in the United States.
• Chinese government not cooperating
Cyber Espionage Case Study

- **Defendants**: All are officers in Unit 61398 of the Third Department of the Chinese People’s Liberation Army (PLA)
  - Wang Dong
  - Sun Kailiang
  - Wen Xinyu
  - Huang Zhenyu
  - Gu Chunhui

- Indictment alleges that Wang, Sun, and Wen, hacked or attempted to hack into U.S. entities, while Huang and Gu supported their conspiracy by, among other things, managing infrastructure (e.g., domain accounts) used for hacking.
Cyber Espionage Case Study

- **Victims:**
  - Westinghouse Electric Co. (Westinghouse)
  - U.S. subsidiaries of SolarWorld AG (SolarWorld)
  - United States Steel Corp. (U.S. Steel)
  - Allegheny Technologies Inc. (ATI)
  - United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union (USW)
  - Alcoa, Inc

- **Time period:** 2006-2014
- **31 counts**
Emerging Threats

• Cyber actors use the latest technology and online marketing

• Examples include: Smartphone malware, tablets…
Mobile Danger

- February 2013, 133.7 million Americans with smartphones, up from 104 million in 2012
- By 2015, est. >2 billion mobile devices worldwide
- Customers choosing banks based on mobile apps
- 5.6 million potentially-malicious files reported on Android…of which 1.3 million confirmed malicious by multiple anti-virus vendors
- Smartphone and tablet/laptop computers are a vector to victimization through data theft or eavesdropping

http://apwg.org/resources/mobile
How the Bad Guys Attack: Spear Phishing

• Impersonating someone trustworthy to try and acquire your information
• Spear-phishing attack uses personal information to make the scam seem real
• Not just emails…
  – Spoofed Websites for technical support, banking, or shopping
  – Phone Calls, Text Messages
  – On-line Gaming
• Phishing casts a wide net to ensure success, Spear Phishing is more personal
• Sending 20 messages provides an almost 100% guarantee that at least one will be successful
How the Bad Guys Attack: Spear Phishing

• One of the most popular and devastating online attacks….you can always clean a virus, but if your banking details are stolen...

• Control over your account login provides not only know the information contained in that account, but the odds are that same login information may be used on various other accounts (personal and professional)

• If they compromise your email account, they can reset all your other passwords...banking, social networking, etc
How the Bad Guys Attack: Spear Phishing

Paypal

Dear Paypal member,

You have added adelaidegerarrd@gmail.com as a new email address for your Paypal account.

If you did not authorize this change, check with family members and others who may have access to your account first. If you still feel that an unauthorized person has changed your email, submit the form attached to your email in order to keep your original email and restore your Paypal account.

If you are using Internet Explorer please allow ActiveX for scripts to perform all data transfers securely.

Thank you for using Paypal!

Please do not reply to this email.
This mailbox is not monitored and you will not receive a response.

Copyright © 1999-2011 PayPal. All rights reserved.

PayPal- Account Update Form.pdf.htm
32K View Download
Profile Update

Please complete the form below to update your Profile information and restore your email address.

Online Access Information Profile
Personal Information Profile

Make sure you enter the information accurately, and according to the formats required. Fill in all the required fields.

*Full Name:
Date of Birth: [month] [day] [year]
Social Security Number:
Home Phone Number: [This number will be used to contact you about Security Measures and/or other issues regarding your PayPal account.]

Home Address Profile

Enter your information as accurately as possible.

*Address Line 1:
Address Line 2:
City:
State:
*Zip Code:
*Country: [Algeria]

Credit/Debit Card Profile

Enter card information as accurately as possible. For card number, enter numbers only please, no dashes or spaces.

*Bank Name:
*Card Number:
Expiration Date: [month] [year]
*Card Verification Number:
*Password 3D Secure Verified By Visa:
CAUTION! Think of SNS more like public record... Don’t put anything on that you wouldn’t want to see on the front page of a newspaper...

• Beware what you post (and what is posted about you—family, friends, coworkers...)
• Privacy settings... check and double check... regularly
• What’s publicly visible even if your profile isn’t?
  • Log out of all social network sites -- then do a search of yourself (Google, Bing, Yahoo!, etc)...
Social Networking Dangers…

• Don’t create groups (i.e. “poker club”, “co-workers”, “family”) – organize based access you want them to have, don’t give potential Phishers too much information about you

• Don’t broadcast your home address, phone number, etc. to strangers on the web, use email, phone, IM…

• Beware connecting social networking sites/sharing information…just because it's marked private on one does not mean it is on another site...

*Use different user names / passwords for all sites (compromise of one does not mean compromise of all…)*

*Be your children’s “friends” and/or “followers” on all sites…*
Identity Theft

EVERYONE is vulnerable... our personal information is EVERYWHERE... bank, school, employer, doctor, merchant, utilities, brokerage, 5k results, social networks...

• Theft of Personal Identifying Information (PII)
  - Commission of other crimes
  - Sold

• Protect yourself!
  • Don’t: carry SSN, unsecure wifi
  • Do: SHRED everything with PII, regular credit checks, firewall, update your systems
What to Do if You’ve Been Hacked

• Report the intrusion
  – Contact your local law enforcement or FBI field office
  – Report intrusions via automated system
  – We’ll work with you and our government partners to respond appropriately and expeditiously

• Get us the malware
  – We’ll examine the malware in our analysis tool, BACSS (the Binary Analysis Characterization and Storage System)
  – Can match digital signatures, help with attribution and mitigation
Victim Reporting

The FBI estimates only one-third of all intrusions into business networks are reported.

Why Don’t Victims Report being victimized?

A: Embarrassment
B: Consumer Confidence
C: Internal Mitigation
D: Concerns about Liability
Intrusion Information Sought

In the area of computer intrusions, the FBI seeks information about the following:

- Malware
- Botnets
- Hacktivists
- Wireless technologies
- Evasive Use of information technology
- Malicious use of mobile technology
- PCS and SCADA (Process Control Systems and Supervisory Control and Data Acquisition systems)
- Cyber threats to U.S. transportation systems
- Electronic payment systems and virtual currencies

If you’re not sure, call us anyway…conversation never hurts…
Typical FBI Response

• Interview key personnel to understand nature, scope, and impact of incident
• Identify & Isolate compromised systems
• On-scene forensic imaging of compromised systems
• Obtain all relevant logs & related evidence
• *Live response on compromised computers with trusted software tools
• *Network traffic monitoring of compromised systems

If possible, we will do all work on site and leave all of your equipment with you

*On-going Intrusion
What the FBI **WILL NOT** Do

- Take over your systems
- Repair your systems
- Share proprietary information with competitors
- Act as a Consultant
- Provide investigation-related information to the media or your shareholders
Parting Thoughts....
Passwords and Encryption are your friends 😊

• Don’t travel with anything that you wouldn’t ‘give away’
• Have ‘travel’ computers
  – “Bare-bones”
  – Beware when plugging that computer back into your network
• Policy for storage during travel
• Beware of ‘freebies’
  – Thumbdrives, software, hardware, etc
• Beware Unencrypted Wi-Fi (coffee shops, airports, hotels, etc)
Protecting Personal Information Online

• Be careful supplying personal information
  • Look for indications that the site uses SSL to encrypt your information (such as the ‘s’ in ‘https’ and the “lock” in the address bar)

• Limit cookies
  • Ensure sites are not collecting personal information about you without your knowledge, choose to only allow cookies for the web site you are visiting and block or limit cookies from a third-party

• Do not use your primary email address in online submissions
  • Consider opening an additional email account for use online

• Avoid using debit cards for online purchases
  • Debit cards are linked DIRECTLY to your bank account…

• Devote one credit card to online purchases
  • Keep a minimum credit line on the account
A Few Basic Steps to Be More Secure…

- Set strong passwords and don’t share them
- Keep a clean machine – update regularly
- Maintain an open dialogue with your family, friends, and community about Internet safety
- Limit the amount of personal information you post online, and use privacy settings to avoid sharing information widely
- Be cautious about what you receive or read online – remember, if it sounds too good to be true, it probably is…
Contacts and Resources


Domestic Security Alliance Council: [http://www.dsac.gov](http://www.dsac.gov)

Center for Responsible Enterprise and Trade: [https://CREATe.org](https://CREATe.org)

Office of the Director of National Intelligence: [www.odni.gov](http://www.odni.gov)

FBI Liaison Alert System (FLASH) reports and Private Industry Notifications (PINs)…received via InfraGard

Internet Crime Complaint Center: [www.ic3.gov](http://www.ic3.gov)
InfraGard

InfraGard is a Partnership between the private sector and the U.S. government represented by the Federal Bureau of Investigation (FBI).

The InfraGard initiative has been developed to encourage the exchange of information by the government and InfraGard members.

The InfraGard San Francisco Bay Area Members Alliance has been established in partnership with the FBI San Francisco Division and is part of the InfraGard National organization.

SF Bay Area InfraGard Members Alliance
San Francisco FBI
Tel: 415-553-7400

http://www.infragard.net or http://www.sfbay-infragard.org
Internet Crime Complaint Center: IC3

Cyber Crime Central Clearinghouse and Repository for Complaints

Types of Fraud Reported:
- Auction
- Auto
- Counterfeit
- Financial Instruments
- Identity Theft
- Financial Fraud
- Hacking
- Spam
- Foreign Lottery
- Charities
- Pharmaceutical
- Romance
- Employment/Business Opportunities
- Impersonation
- Extortion

www.IC3.gov
Any Questions?