Disclaimer

- You do not hold the presenter liable and accept full responsibility for your actions.

- You will use any tools mentioned in an ethical, professional and legal manner.

- You will always get permission before running any tools on the network.

- The presentation does not endorse or approve and assumes no responsibility for the content, accuracy or completeness of the information presented.

- This presentation does not represent the opinions of any of the organizations that I have worked for.
Agenda

- 2011 Breaches Review
- How can users protect their data?
- What is a threat?
- The Threat Landscape (in no particular order)
- Summary
- What can we do?
- Tools
- Final Words...
2011 – A year of + breaches

- March – RSA: 25,000 SecurID tokens
- April – Epsilon
  - Ameriprise Financial, BestBuy, Capital One Bank, Citi, JP Morgan Chase, Tivo, US Bank and Others
  - Sony Playstation Network (PSN) – 77 million records
  - Sony Online Entertainment – 25 million records
- May – Lockheed Martin – used cloned RSA tokens
- June – Lulzsecurity & Anonymous hacking

Source: Lulz Security
How can users protect their data?

- Minimize information that is put online
- Use disposable email accounts
- Use disposable credit card numbers (if possible)
- Use a new password for every account
- Do not provide any non-essential personal information
- Never give out social security number (SSN) or write it down on checks
What is a threat?

- A potential cause of an unwanted incident, which may result in harm to a system or organization (ISO/IEC 27000).
Malware = Profit

500% increase in email-attached malware
USPS subject line (Your USPS id. 44531036)

The UPS name is once again being used to spread vast amounts of email-attached malware. The last week has seen an extraordinary increase – over 5.5 times the average level before the outbreak.

The attack closely resembles the large outbreak reported on at the end of March. The graph below illustrates the increase:

Old Days – Manual
New Days – Automation

• Malware automates hacking
  • Banking trojan - Banco do Brasil (TSPY_BANKER.PHT)

There are numerous versions of the email text, here’s an example:

Good afternoon!

Dear Client, Recipient’s address is wrong

Please fill in attached file with right address and resend to your personal manager

With best regards, Your USPS.com Customer Services

(Malware Blog)
Targeted Attacks

- Spear Phishing
- Advanced Persistent Threats (APT)

How Advanced Persistent Threats Breach Enterprises:

APTs breach enterprises through a wide variety of vectors, even in the presence of properly designed and maintained defense-in-depth strategies:

- Internet-based malware infection
- Physical malware infection
- External exploitation

Internet Malware Infections
- Drive-by Downloads
- Email Attachments
- File sharing
- Pirated software & keygen
- Spear Phishing
- DNS & Routing Mods

Physical Malware Infections
- Infected USB memory sticks
- Infected CD’s and DVD’s
- Infected memory cards
- Infected appliances
- Backdoored IT equipment

External Exploitation
- Professional Hacking
- Mass vulnerability exploits
- Co-location Host Exploitation
- Cloud provider penetration
- Rogue WiFi penetration
- SmartPhone Bridging

(Damballa)
Vulnerabilities

- Legacy machines or software/hardware are still not being patched
- Old vulnerabilities still exist and are exploited
- Operating System (OS) patching + specific applications patching and more
- Vendor patching is getting better
- Browsers are getting better, but third party software are still a major problem
Mobile Devices – Appstores

Google++ (Android)

- Capable of collecting data such as text messages, call logs, and GPS location from infected devices, which it then uploads to a certain URL through port 2018.
- Also capable of receiving commands via text messages and recording phone calls.

Other mobile threats:

- Love Trap Android Malware Found in 3rd party app stores
- Spying tools
- SMS Relays
- Backdoor Apps
- Zeus, SpyEye etc.
- GPS tools
- Rooting devices

(Malware Blog)
Social Networking: Facebook?

- Review what information is out there
- Do not trust your data to social network sites

**Personal information**

- names, addresses, birth dates, SSN = identity theft
- financial information = credit card numbers, bank account passwords are still big business
- health information
Search Engine Optimization (SEO) – FakeAV


1. Pages using server side kits to fool search engine bots into ranking them high in results are uploaded to legitimate web sites. If all goes to plan, when a user searches for a popular term, high up in the search engine results are links to these pages. In the example below, the malicious SEO page was the 2nd item in the search results (highlighted in blue).

2. When the user arrives on such a page (highlighted in green in the example below), the referrer is typically checked to ensure they came from a search engine. If so, there are redirected (302 redirect) to another site (orange below).

3. There are typically additional levels of redirection from this point. In the example shown below, the user is bounced from the .org to the .in site (purple).

4. Finally, the user will be redirected to the fake AV distribution site (red). This is where the user receives the usual visual trickery, in order to fool them into installing the rogue application.
3rd Party Software

- Lack of complete inventory details
- Patching is often regarded as a secondary security measure
- Third-party programs are not yet perceived as the preferred attack vector by non-security staff
- Security updates are complex to navigate and deploy
Physical Security
Insiders

**Insider Threat**
- Rogue Employee
- Malicious Sub-contractor
- Social engineering expert
- Funded placement
- Criminal break-in
- Dual-use software installation

**Trusted Connections**
- Stolen VPN credentials
- Hijacked roaming hosts
- B2B connection tapping
- Partner system breaches
- Externally hosted system breaches
- Grey market network equipment

(Damballa)
Social Engineering

- We are only as strong as the weakest link in your company.
- Social engineering attacks bypass technical defenses
Disasters

- Prepare for the worst!
- Planning
- Recovery
- Business continuity
Web 2.0 (1 of 2)

- Majority of web applications are insecure
- The web (HTTP) was not designed to be secure
- Security was “bolted-on” rather than “built-in”
- A lot of applications are on the Internet now
- “Our findings show that during an attack, hackers can generate more than 80,000 daily queries to probe the Web for vulnerable Web applications.” (Imperva)
Web 2.0 (2 of 2)

- Application Security!
- Threat Modeling
- Code Changes
- Secure Architecture
- Developer & Architect Awareness
- Common Security Controls
- Software Development Lifecycle

(OWASP)
Summary

- Data breaches will occur
- No networks are really secure
- “Network data breaches happen all the time, quietly affecting millions more people.” (Bruce Schneier)
- Blackhats will always win
- Landscape will keep changing and target what end users use more of.
What can we do? (1 of 4)

- Networking = Awareness
- “More” Education and Training
- Plan for the worst and be ready at all times
- Build “black hat” mindset
- Be proactive instead of reactive
- Take proactive steps to assess risk and implement appropriate security controls and defenses
- Review and monitor activity logs
What can we do? (2 of 4)

- Lock down workstation and limit local privileges
- Limiting the rights employees have to access the network and applications to match their business needs
- Evaluate the effectiveness of browser security software in its ability to restrict access to dangerous content
- Use enterprise management system (EMS) tools
- Assess capabilities of the security tools used to protect Web browsing activities
What can we do? (3 of 4)

- Change the perspective of your security efforts from attempting to prevent breaches to resisting intrusions.
- Understand where your valuable data is located and adjust defensive spending.
- Identify the individuals who are most likely to be targeted and protect them with more training.
- Educate employees about risks of data leaked inadvertently on public forums.
- Establish a practical and comprehensive Web application security program.
What can we do? (4 of 4)

- Incorporate application related steps into your incident response plan
- Break down the wall between infrastructure and application security teams
- Understand the business purpose of the applications
- Include application components in your penetration testing projects
- Include application logs as part of your log management or security information and event management (SIEM) efforts
Tools

- Bin Pack
  - Portable security environment for Windows
    - westcoasthackers.net
- Zscaler Spam SEO for Firefox

- Remember to not trust any tool until it is properly tested
References

- Brandeis University Graduate Professional Studies (GPS) http://www.brandeis.edu/gps/
Final Words . . .

- websecr at gmail dot com
- twitter: wr0

- Questions