



Roy Wattanasin  
@Boston University Security Camp

August 18, 2011

# INFORMATION SECURITY THREATS FOR 2011




# 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

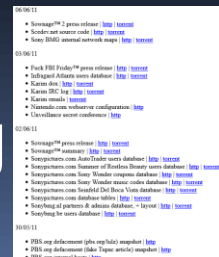
- 2011 Breaches Review
  - How can users protect their data ?
  - What is a threat ?
  - The Threat Landscape (in no particular order)
  - Summary
  - What can we do ?
  - Tools
  - Final Words . . .
- 

# 2011 – A year of + breaches

<http://www.privacyrights.org/data-breach> and <http://datalossdb.org/>

- March – RSA: 25,000 SecurID tokens
- April – Epsilon
  - Amerirprise 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



```
06/06/11
  • Sony PSN press release | http | http://www.sony.com
  • Sony PSN user records | http | http://www.sony.com
  • Sony PSN network maps | http | http://www.sony.com

08/06/11
  • Bank First Future press release | http | http://www.bankfirst.com
  • Dell Inspiron laptop users database | http | http://www.dell.com
  • Euronews press release | http | http://www.euronews.com
  • Euronews press release | http | http://www.euronews.com
  • Nintendo.com webserver configuration | http | http://www.nintendo.com
  • Nintendo.com user database | http | http://www.nintendo.com

09/06/11
  • Sony PSN press release | http | http://www.sony.com
  • Sony PSN press release | http | http://www.sony.com
  • Sony PSN press release | http | http://www.sony.com
  • Sony PSN press release | http | http://www.sony.com
  • Sony PSN press release | http | http://www.sony.com
  • Sony PSN press release | http | http://www.sony.com
  • Sony PSN press release | http | http://www.sony.com
  • Sony PSN press release | http | http://www.sony.com
  • Sony PSN press release | http | http://www.sony.com
  • Sony PSN press release | http | http://www.sony.com


10/06/11
  • PDS.org press release | http | http://www.pds.org
  • PDS.org press release | http | http://www.pds.org
  • PDS.org press release | http | http://www.pds.org
```

# 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 ?

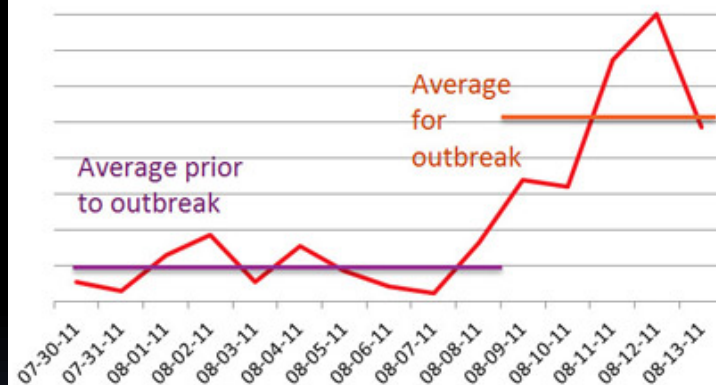
- A potential cause of an unwanted incident, which may result in harm to a system or organization (ISO/IEC 27000).
- 

# 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:



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

(Help Net Security)

## Old Days – Manual New Days – Automation

- Malware automates hacking
  - Banking trojan - Banco do Brasil (TSPY\_BANKER.PHT)

U	0000F038	1100F038	0	javascript:acessaPagina('ted.processa')
U	0000F048	1100F048	0	sltCodigoBanco
U	0000F0CC	1100F0CC	0	frmTedTerceiros
U	0000F100	1100F100	0	txtAgenciaDestino
U	0000F128	1100F128	0	11348
U	0000F138	1100F138	0	txtContaDestino
U	0000F15C	1100F15C	0	txtDvContaDestino
U	0000F184	1100F184	0	sltTipoContaDestino
U	0000F1AC	1100F1AC	0	selectedIndex
U	0000F1CC	1100F1CC	0	[REDACTED]
U	0000F1F0	1100F1F0	0	[REDACTED]
U	0000F20C	1100F20C	0	txtContingDestino
U	0000F234	1100F234	0	5000,00

(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

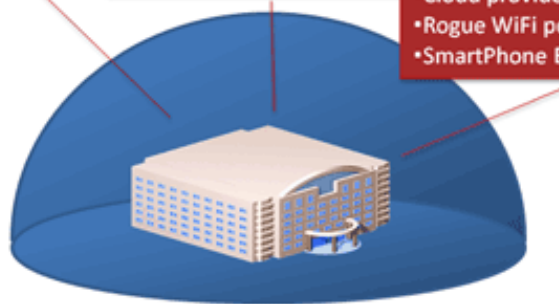
- Drive-by Downloads
- Email Attachments
- File sharing
- Pirated software & keygen
- Spear Phishing
- DNS & Routing Mods

### 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







# 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.

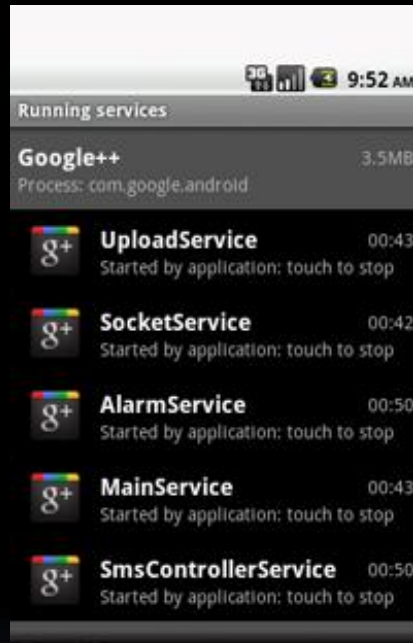


Figure 1. Services used by ANDROIDOS\_NICKISPY.C

(Malware Blog)



Figure 2. The malicious app installed as "Google++"

## Other mobile threats:

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

# Social Networking: Facebook?

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

### Fraudster used Facebook to hack bank accounts

A hacker stole £35,000 from his neighbours' online bank accounts after working out the answers to their security questions from information they posted on Facebook. Friends Reunited.

11:19PM BST 14 Aug 2011

11 Comments

Iain Wood spent up to 18 hours per day online, working out passwords from personal information posted on social networking sites by his acquaintances.



He targeted people living in his block of flats in a complex fraud and used his friends' personal details to get past security checks and hack into their bank accounts - stealing more than £35,000 over two years which he blew on gambling.

His scam only came to an end when he became over-confident and changed his system and the authorities were alerted.

Jailing him for 15 months, Judge Guy Whitburn said at Newcastle Crown Court:

Iain Wood targeted people living in his block

### John Smith, United States

Quick Facts  
Smith is charged in the abduction, rape and killing of Carlie Brucia, in February...  
Smith is currently on the medication Cognex, the first effective treatment for mild-to-moderate Alzheimer's disease...

Contact Details

**John Smith, 2 Park Dr, Alabaster, AL...**  
Search Person Map Address

**John Smith, 616 Park Forest Ln, Alabaster, AL...**  
Search Person Map Address

**John Smith, 100 Wagon Cir, Alabaster, AL...**  
Search Person Map Address

**John Smith, 125 Wagon Trl, Alabaster, AL...**  
Search Person Map Address

Sponsored Tip: Find Out All of John Smith's Juiciest Secrets. ...  
46 additional Contact Details >

Premium Address Reports

**John Wesley Smith, Ardmore, OK (Smith, Mamye Evelyn; Wiggins, Debra Kay; Smith, ... \$\$\$**  
Background Report - PeopleFinders - Sponsored Result

**John A Smith, Metairie, LA (Smith, Deborah K; Smith, Arneker D)... \$\$\$**  
Background Report - PeopleFinders - Sponsored Result

**John Gordon Smith, Deerfield Beach, FL, Miami Lakes, FL (Smith, Pauline)... \$\$\$**  
Background Report - PeopleFinders - Sponsored Result

**John Wilburn Smith, Oklahoma City, OK (Smith, Mary F)... \$\$\$**  
Background Report - PeopleFinders - Sponsored Result

Sponsored Tip: MyLife has access to 200 million profiles. Find what you're looking for on anyone...  
12 additional Premium Address Reports >

Personal Profiles

**cabbie b\*. 41, San Francisco, California...**  
Personal Web Space - MySpace

**JWS. 28, Austin, Texas...**  
Personal Web Space - MySpace

**John. Smith. 29, San Francisco, California...**  
Personal Web Space - MySpace

**THE REAPER. 23, P-Town(806), Texas...**

- 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

<http://research.zscaler.com/2010/07/new-firefox-add-on-to-protect-against.html>

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.

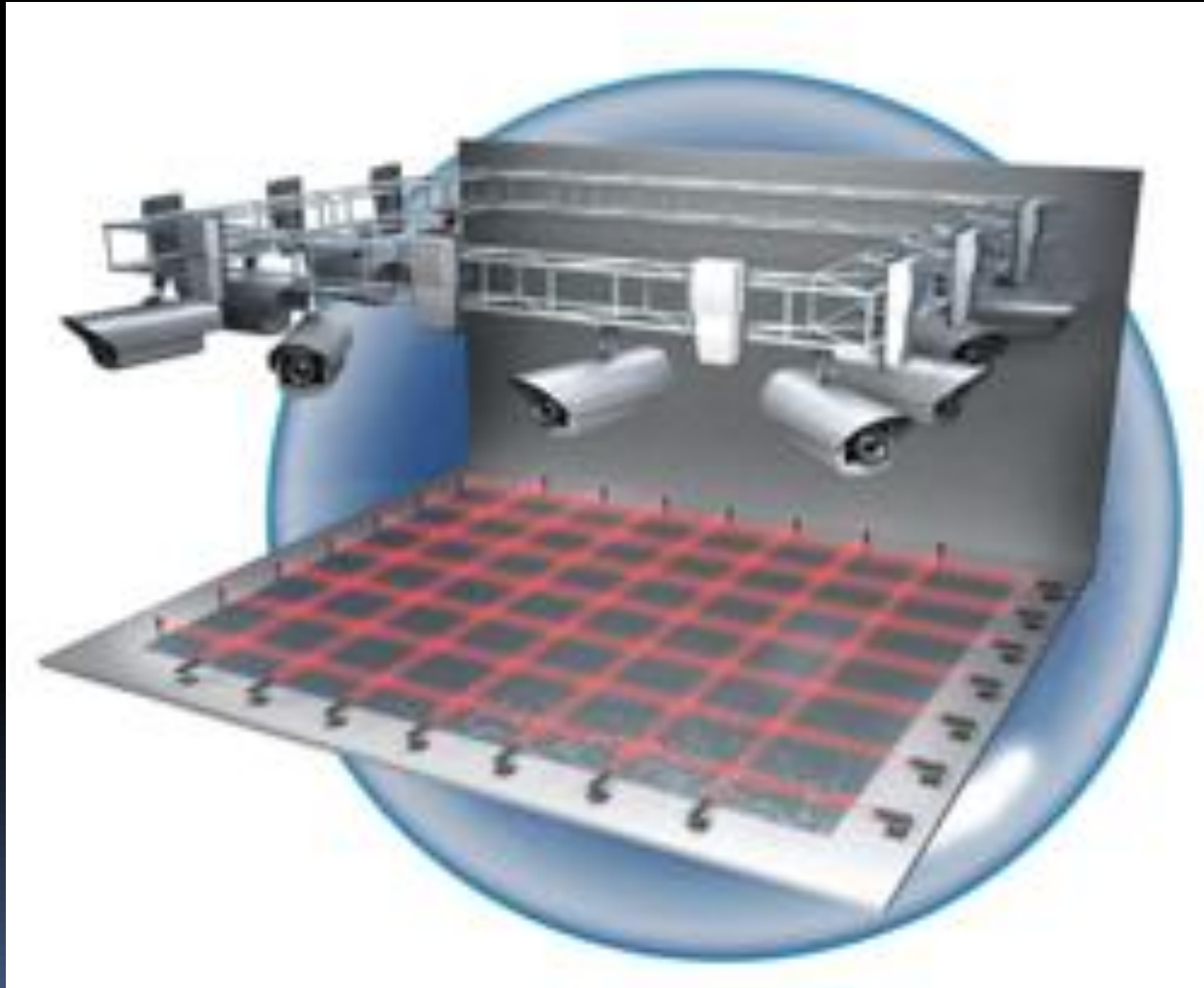
204	www.google.co.uk	/url?sa=T&source=web&ct=res&cd=9&ved=0CCAQFjAI
302	www1.secure.com	/bnr1/catalog/product_info.php/?cdoc=hannah+storm+
302	www1.secure.org	/in.cgi?24&parameter=\$keyword&se=\$se&seoref=http
302	www1.secure.in	?uid=287&pid=3&q=hannah+storm+outfit+picture&ttl
200	www1.secure.in	?p=p52dcWpsb1%2FCj8bYboNuilik12qYVp%2FZatrau4F
200	www1.secure.in	/Images/loading.gif
200	www1.secure.in	/Scripts/Strategies/6a2c4383bf98763d7ea90eaebde1eec50530066
200	www1.secure.in	/service.php?p=p52dcWpsb1%2FCj8bYboNuilik12qYVp%2FZatrau



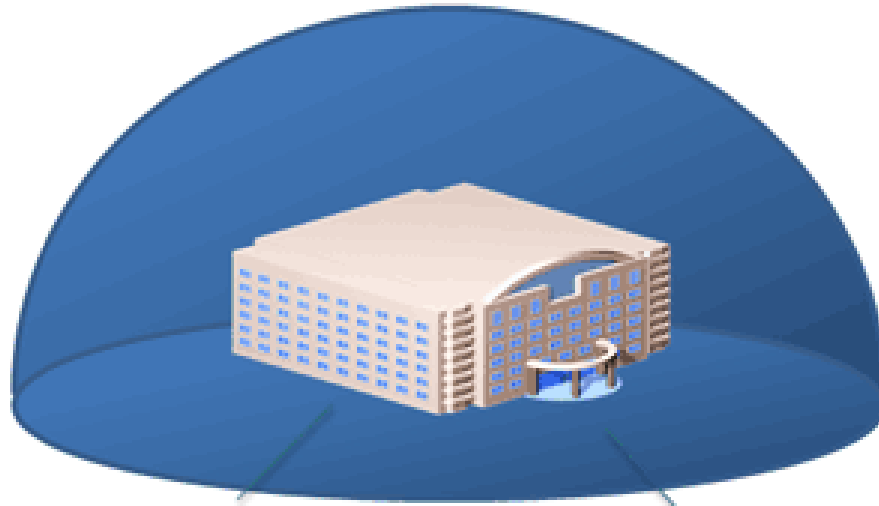
# 3rd Party Software

- 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




# 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)





# 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
  - <http://research.zscaler.com/2010/07/new-firefox-add-on-to-protect-against.html>
- Remember to not trust any tool until it is properly tested

# References

- "Advanced Persistent Threats." <http://www.damballa.com/knowledge/advanced-persistent-threats.php>
- "Black Hat 2011: Attack vectors, vulnerabilities and malware analysis." <http://searchsecurity.techtarget.com/video/Black-Hat-2011-Attack-vectors-vulnerabilities-and-malware-analysis>
- Bradley, Tony. "McAfee: Corporate Espionage Is the Currency of Cybercrime." March 28, 2011. PC World. [http://www.pcworld.com/businesscenter/article/223483/mcafee\\_corporate\\_espionage\\_is\\_the\\_currency\\_of\\_cybercrime.html#tk.hp\\_new](http://www.pcworld.com/businesscenter/article/223483/mcafee_corporate_espionage_is_the_currency_of_cybercrime.html#tk.hp_new)
- Brandeis University Graduate Professional Studies (GPS) <http://www.brandeis.edu/gps/>
- Crecente, Brian. "Don't Blame Sony, You Can't Trust ANY Networks." May 4, 2011. <http://kotaku.com/5797602/dont-blame-sony-you-cant-trust-any-networks>
- "Hacker Intelligence Initiative, Monthly Trend Report #3"  
[http://www.imperva.com/docs/HII\\_The\\_Convergence\\_of\\_Google\\_and\\_Bots\\_-\\_Searching\\_for\\_Security\\_Vulnerabilities\\_using\\_Automated\\_Botnets.pdf](http://www.imperva.com/docs/HII_The_Convergence_of_Google_and_Bots_-_Searching_for_Security_Vulnerabilities_using_Automated_Botnets.pdf)
- "Is mobile malware really a problem?" <http://ctoinsights.trendmicro.com/2011/08/is-mobile-malware-really-a-problem/>
- "Malware Automates Hacking." Malware Blog. <http://blog.trendmicro.com/malware-automates-hacking/>
- OWASP Top 10 Application Security Risks [https://www.owasp.org/index.php/Top\\_10\\_2010-Main](https://www.owasp.org/index.php/Top_10_2010-Main)
- Poremba, Sue. "How to Disappear Almost Completely ... and Protect Yourself from Data Breaches ." May 9, 2011. <http://www.securitynewsdaily.com/protect-yourself-from-data-breaches-0769/>
- Turiel, Avi. "500% increase in email-attached malware." [http://www.net-security.org/malware\\_news.php?id=1802](http://www.net-security.org/malware_news.php?id=1802)
- Verizon 2011 DBIR [http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2011\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf)
- Widman, Jake "10 Massive Security Breaches." March 12, 2011. <http://www.informationweek.com/news/galleries/security/attacks/229300675?pgno=1>
- Zeltzer, Lenny. "Evolving IT security threats: Inside Web-based, social engineering attacks." SearchSecurity. <http://searchsecurity.techtarget.com/tip/Evolving-IT-security-threats-Inside-Web-based-social-engineering-attacks>



# Final Words . . .

- websec at gmail dot com
- twitter: wr0

- 
- Questions