What the Cyber Criminals are Doing on Your Website (Right Now)

Front Range OWASP Conference
March 22, 2012

Laz
Director of Strategy, Silver Tail Systems
laz@silvertailsystems.com
Twitter: iamlaz
Agenda

• Introductions
• Some IT Security Trends/Statistics
• Use Cases
• Lessons Learned
• Staying Ahead
• Questions
Some IT Security Trends

2012 Security Spending To Hold Strong

Compliance, mobile devices, and data loss prevention top the list of trends driving 37% of businesses to increase IT security spending.

By Mathew J. Schwartz  InformationWeek
November 17, 2011 02:40 PM

For 2012, 37% of information security spending, while only 16% expect their spend to address compliance, mobile device

Report: Android malware up 3,325% in 2011

By Adrian Kingsley-Hughes | February 23, 2012, 8:36am PST

Summary: Android malware samples had increased from 400 to 13,302 in six months.

Popularity comes at a price.

During 2011 there was an ‘unprecedented growth’ of mobile malware attacks, with Android up a stratospheric 3.325 percent, according to a report by the Juniper Networks Mobile Threat Center.

The report makes depressing reading. Across all platforms, mobile malware attacks are up 155 percent, with mobile malware samples increasing from 11,138 in 2010 to 28,472 in 2011. BlackBerry malware grew by 8 percent, and Java ME saw a 49 percent increase. But the platform hit hardest was Android, with malware increasing by an incredible 3,325 percent in a year. During the last six months of 2011, Android malware samples had increased from 400 to 13,302.

Source: Juniper Networks Mobile Threat Center
Data theft: Hacktivists 'steal more than criminals'

Hacktivists stole more data from large corporations than cybercriminals in 2011, according to a study of significant security incidents.

The annual analysis of data breaches by Verizon uncovered a huge rise in politically motivated attacks.

Verizon found that 58% of all the data stolen during breaches in 2011 was purloined by these groups.

Hacktivists are proving hard to combat, suggests a study of data breaches

Source: Verizon 2011 Data Breach Investigations Report and BBC
Some Statistics

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Method</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>50%</td>
<td>utilized some form of hacking</td>
<td>+10%</td>
</tr>
<tr>
<td>49%</td>
<td>incorporated malware</td>
<td>+11%</td>
</tr>
<tr>
<td>29%</td>
<td>involved physical attacks</td>
<td>+14%</td>
</tr>
<tr>
<td>17%</td>
<td>resulted from privilege misuse</td>
<td>-31%</td>
</tr>
<tr>
<td>11%</td>
<td>employed social tactics</td>
<td>-17%</td>
</tr>
</tbody>
</table>

Source: Verizon 2011 Data Breach Investigations Report
Some Statistics

Who is behind data breaches?

- 92% stemmed from external agents (+22%)
- 17% implicated insiders (-31%)
- <1% resulted from business partners (-10%)
- 9% involved multiple parties (-18%)

Source: Verizon 2011 Data Breach Investigations Report
Identifying Known Issues

• Identifying the issues through:
  – Pen testing
  – Application/Network/OS Scans
  – Internal testing
  – Monitoring/SIEM
What About Unknown Issues?

• Some indicators that things were going bad
  – Always started with a phone call
  – Site performance degrading over time, which resulted in a decline of sales due to bad performance
  – Increase in Customer Service phone calls

• Research is time consuming!
  – How can you justify pulling revenue generating resources off of projects to investigate something?

How will this type of behavior hurt the company brand?
These are Still Well Known Issues

• Man in the Middle
• Man in the Browser
• Man in the Mobile

Criminal behavior looks much different than normal behavior
Some Unknown Issues

• People gaming the system to abuse marketing, sweepstakes, loyalty, and incentive programs
• Increase to fraudulent activities due to lack of visibility into the Web session – cyber criminals are getting more creative with their approach!
• Manipulating the session with Mobile devices
• Site scraping for content, pricing, or inventory/architecture probing
• DDoS (recon and actual attack) attacks

IDS/IPS/WAF and transaction-based solutions are being by-passed by cyber criminals
People Gaming the System

• Business Drivers
  – Online marketing campaigns, sweepstakes, or incentives to acquire new customers

• Challenges Identified
  – Unique registration patterns over time
  – Registrants signing up from all over the world
  – Random name generator from multiple IP addresses

• Research
  – Cheating Network
  – The Botting Network (TBN)
Cheating Network
Cheating Network

Captcha Built In!
<table>
<thead>
<tr>
<th>Topic</th>
<th>Replies</th>
<th>Views</th>
<th>Last Post</th>
<th>Forum</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Release] Auto URL Refresher</td>
<td>3</td>
<td>14</td>
<td>Today 05</td>
<td>Public Bot / Exploit</td>
</tr>
<tr>
<td>Clixchoice - clixchoice.com</td>
<td>2</td>
<td>363</td>
<td>Today 04</td>
<td>Paid To Click</td>
</tr>
<tr>
<td>Quesion</td>
<td>3</td>
<td>217</td>
<td>Today 04</td>
<td>Chit Chat</td>
</tr>
<tr>
<td>Youtube Partnership</td>
<td>7</td>
<td>364</td>
<td>Today 04</td>
<td>Chit Chat</td>
</tr>
<tr>
<td>Sticky: [Release] Make your own bots</td>
<td>126</td>
<td>26,592</td>
<td>Today 03</td>
<td>Public Bot / Exploit</td>
</tr>
<tr>
<td>GemBucks - <em><strong>Brand New</strong></em> - GPT</td>
<td>3</td>
<td>374</td>
<td>Today 03</td>
<td>Get Paid To</td>
</tr>
<tr>
<td>Easy Guide to a Gaming Partnership on</td>
<td>4</td>
<td>503</td>
<td>Today 03</td>
<td>Public Bot / Exploit</td>
</tr>
<tr>
<td>$25 BestBuy gift card</td>
<td>27</td>
<td>989</td>
<td>Today 03</td>
<td>Received In The</td>
</tr>
<tr>
<td>$50 from JunoWallet Giftcards</td>
<td>10</td>
<td>378</td>
<td>Today 03</td>
<td>Received In The</td>
</tr>
</tbody>
</table>
### Notices

Why hello there, welcome to thebotnet.com.
You’re viewing our boards as a guest which limits your access. By joining our free community, you can post topics, pm members, download & upload stuff, read exclusive threads, and many more special features. You’ll also be able to vote inside of every thread as this guest notice.

Registration is free & takes only a few seconds! Click here & join our community today!

### Lobby

<table>
<thead>
<tr>
<th>Forum</th>
<th>Last Post</th>
<th>Threads</th>
<th>Posts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Announcements</strong></td>
<td>Youtube Forum by mixermax0</td>
<td>141</td>
<td>5,176</td>
</tr>
<tr>
<td><strong>General / Off Topic</strong></td>
<td>Ebay &amp; paypal problem by FlyCoyotee</td>
<td>18,278</td>
<td>145,344</td>
</tr>
<tr>
<td><strong>Our Community</strong></td>
<td>Post Your Desktop by enchy</td>
<td>2,973</td>
<td>37,604</td>
</tr>
<tr>
<td><strong>Check It Out</strong></td>
<td>$20 Center of Prizes Winner! by mantalcore</td>
<td>2,494</td>
<td>33,208</td>
</tr>
</tbody>
</table>

### Cake

<table>
<thead>
<tr>
<th>Forum</th>
<th>Last Post</th>
<th>Threads</th>
<th>Posts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Make Money</strong></td>
<td>best GPT site of all time!...</td>
<td>6,823</td>
<td>87,853</td>
</tr>
</tbody>
</table>
TBN – The Botting Network
Increase in Fraud/Malicious Behavior

- Who’s paying for fraud?
- Is this type of behavior violating the Terms of Use of your website agreement?
- Traditional fraudulent behavior is changing – not just hard dollars anymore
- Moving to other parts of the site to compromise the system and/or business logic

Engage Fraud and Legal to Discuss the Emerging Threats
Mobile Issues

• Business Drivers
  – We want to have a multi channel solution to acquire and retain customers through the use of email updates, instant coupons, rebates, and other promotions to our customers
  – We want to communicate with all of our customers in near-realtime

• Challenges Identified
  – User login using IE 7 running Windows OS
  – User continues the session, but the session switches to Firefox on Linux

• Research
  – Compromised phones are accessing the Web site
  – Mobile emulation programs are probing the Web site
Slow Site Scraping for Content, Pricing, Inventory, or just Probing

• Different velocity scans hitting the Web site to find out:
  – How many items are in inventory
  – How much items cost
  – What type of systems/services are running to support the site
  – Moving through the site to understand if there were any translation to other languages

• Research
  – Items were being held in shopping carts and never purchased
  – What is the relationship between Women’s shoes and Women’s clothing searches and page views?
DDoS

• Repeated behavior indicated something was going to happen
• Trending data allowed the team to be prepared
• Preparation included:
  – Simulated DDoS testing
  – Enhancements to the SOPs
  – Understanding where revenue was being generated – which countries and locations were high revenue areas

There is no silver bullet for a DDoS attack
Lessons Learned

• It’s about the data
• Quantify your research
• There are tools out there to solve this complex issue – evaluate the solutions now
• Disk is cheap/creative with storage solutions to trend data over longer periods of time
• Research events and tie the patterns/trends together
• Collaborate, collaborate, collaborate
Staying Ahead – Where to Go

• OWASP Meetings
• ISSA Meetings
• US Secret Service Briefings
• FBI InfraGard
• E-crime Congress
• Financial Services - Information Sharing and Analysis Center (FS-ISAC) (Finance / Financial Services)
• Merchant Risk Council (MRC) (Online / Retail)

Build Your Network of Subject Matter Experts!
Resources

• www.cheatingnetwork.net
• www.cybercrime.gov
• www.datalossdb.org
• www.darkreading.com
• www.e-crimecongress.org
• www.fsisac.com
• www.merchantriskcouncil.org
• www.owasp.org
• www.thebotnet.com
Questions?

Thank You!

Laz
Director of Strategy, Silver Tail Systems
laz@silvertailsystems.com
Twitter: iamlaz