Cyber Vigilantes

April 2011
Hacking has become industrialized.

Attack techniques and attack vectors keep evolving with an ever rapid pace.

Attack tools and platforms keep evolving.
Reality Check #1:
Hackers Know the Value of Data Better Than the Good Guys
Data is hacker currency
<table>
<thead>
<tr>
<th>Site</th>
<th>Details</th>
<th>Level of Control</th>
<th>Traffic</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://osmil.ai/">http://osmil.ai/</a></td>
<td>ARMY Forces of republic of alliance</td>
<td>Full Site/Admin Control + High value informations</td>
<td>unknown</td>
<td>$499</td>
</tr>
<tr>
<td><a href="http://www.scguard.army.mil/">http://www.scguard.army.mil/</a></td>
<td>South Carolina National Guard</td>
<td>MySQL root access + High value informations</td>
<td>unknown</td>
<td>$499</td>
</tr>
<tr>
<td><a href="http://cescom.army.mil/">http://cescom.army.mil/</a></td>
<td>The United States Army</td>
<td>CECOM</td>
<td>Full Site/Admin Control/SSH Root access</td>
<td>unknown</td>
</tr>
<tr>
<td><a href="http://pec.ha.osd.mil/">http://pec.ha.osd.mil/</a></td>
<td>The Department of defense pharmacoeconomic Center</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.woodlands.edu/uruguay">http://www.woodlands.edu/uruguay</a></td>
<td>Woodlalnds School Uruguay</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://e-u.edu.in">http://e-u.edu.in</a></td>
<td>Singhania University</td>
<td>Full Site/Admin Control</td>
<td>5200</td>
<td>$55</td>
</tr>
<tr>
<td><a href="http://www.nccu.edu.tw">http://www.nccu.edu.tw</a></td>
<td>National Chengchi University</td>
<td></td>
<td>56093</td>
<td>$55</td>
</tr>
<tr>
<td><a href="http://www.terc.tp.edu.tw">http://www.terc.tp.edu.tw</a></td>
<td>Taipei City East Special Education Resource Center</td>
<td>Full Site/Admin Control</td>
<td>74188</td>
<td>$55</td>
</tr>
<tr>
<td><a href="http://itcparlamento.gov.it">http://itcparlamento.gov.it</a></td>
<td>Italian Official Government Website</td>
<td>Full Site/Admin Control</td>
<td>292942</td>
<td>$55</td>
</tr>
<tr>
<td><a href="http://donmilaninapoli.gov.it">http://donmilaninapoli.gov.it</a></td>
<td>Institute Statale Don Lorenzo Milani</td>
<td>Full Site/Admin Control</td>
<td>292942</td>
<td>$55</td>
</tr>
<tr>
<td><a href="http://kopcesaro.gov.it">http://kopcesaro.gov.it</a></td>
<td>Official Italian gov website</td>
<td>Full Site/Admin Control</td>
<td>292942</td>
<td>$55</td>
</tr>
<tr>
<td><a href="http://rimarconi.gov.it">http://rimarconi.gov.it</a></td>
<td>Official Italian gov website</td>
<td>Full Site/Admin Control</td>
<td>292942</td>
<td>$55</td>
</tr>
<tr>
<td><a href="http://primocircovicco.gov.it">http://primocircovicco.gov.it</a></td>
<td>Official Italian gov website</td>
<td>Full Site/Admin Control</td>
<td>292942</td>
<td>$55</td>
</tr>
<tr>
<td><a href="http://www.uteh.gov">http://www.uteh.gov</a></td>
<td>American State of Utah Official Website</td>
<td>Full Site/Admin Control</td>
<td>173146</td>
<td>$55</td>
</tr>
<tr>
<td><a href="http://www.uscb.edu">http://www.uscb.edu</a></td>
<td>University of South Carolina Beaufort</td>
<td>Full Site/Admin Control</td>
<td>1123</td>
<td>$55</td>
</tr>
</tbody>
</table>

*Daily updated - Click here to check for proof of the hacked sites.*

Email me or add me in MSN at: e@e.com
Website Access up for Sale

http://cecom.army.mil/
- The United States Army | CECOM
- Full SiteAdmin Control/SSH Root access
- unknown $499

- Daily updated -
Click here to check for proof of the hacked sites.

Email me or add me in MSN at: imperva@gmail.com
Reality Check #2:
Hackers, By Definition, Are Early Adopters
Reality Check #3:
The Good Guys Have More Vulnerabilities Than Time, Resourcing Can Manage
WhiteHat Security Top Ten—2010

Percentage likelihood of a website having **at least one** vulnerability sorted by class

- **Information Leakage**: 64%
- **Cross-Site Scripting**: 64%
- **Content Spoofing**: 43%
- **Cross-Site Request Forgery**: 24%
- **Brute Force**: 17%
- **Insufficient Authorization**: 15%
- **Predictable Resource Location**: 14%
- **SQL Injection**: 14%
- **Session Fixation**: 14%
- **Abuse of Functionality**: 10%
Feeling Overwhelmed?
“Natural pesticide carcinogens have been shown to be present in the following foods: anise, apples, bananas, basil, broccoli, brussel sprouts, cabbage, cantaloupe, carrots, cauliflower, celery, cinnamon, cloves, cocoa, coffee, comfrey tea, fennel, grapefruit juice, honeydew melon, horseradish, kale, mushrooms, mustard, nutmeg, orange juice, parsley, parsnips, peaches, black pepper, pineapples, radishes, raspberries, tarragon, and turnips.”

- Bruce Ames

Professor of Biochemistry and Molecular Biology at the University of California, Berkeley
“Thus, it is probable that almost every plant product in the supermarket contains natural carcinogens. The levels of the known natural carcinogens in the above plants are almost always much higher than the levels of man-made pesticides, and many are in the range of thousands to millions of parts per billion.”

- Bruce Ames

Professor of Biochemistry and Molecular Biology at the University of California, Berkeley
Studying Hackers

- Why this helps
  - Focus on what hackers want, helping good guys prioritize
  - Technical insight into hacker activity
  - Business trends of hacker activity
  - Future directions of hacker activity

- Eliminate uncertainties
  - Active attack sources
  - Explicit attack vectors
  - Spam content

- Focus on actual threats

- Devise new defenses based on real data
  - Reduce guess work
Approach #1:
Monitoring Communications
Method: Hacker Forums

- Tap into the neighborhood pub

Analysis activity
  + Quantitative analysis of topics
  + Qualitative analysis of information being disclosed
  + Follow up on specific interesting issues
SQL Injection = Most Popular Topic

Topic Breakdown

- SQL Injection: 29%
- Non-tech Related: 26%
- Passwords: 12%
- Credit Cards: 6%
- Spam & Phishing: 6%
- Other Exploits: 21%

Source: Imperva
Hacker interest in mobile has increased. In the last half of the year there were 2383 keywords compared to only 264 on the previous half.

Source: Imperva’s Application Defense Center Research
Approach #2:
Knowing Hacker Business Models
Rustock Takedown Cut Spam By 33%

Bagel and other botnets seem to be picking up the slack, according to Symantec.

By Mathew J. Schwartz, InformationWeek
March 29, 2011 14:13 PM

All hail the Rustock botnet takedown. Between March 15 and 17, during which time Rustock was taken down, global spam volumes fell by 33.6%, according to a Symantec MessageLabs Intelligence report. Compared to the week before the takedown, the number of daily spam emails decreased from 52 billion to 33 billion.

At its height, the Rustock botnet pumped out 13.82 billion emails per day, comprising 29% of the world's daily spam diet. But will the Rustock respite last?
 Spy Eye vs Zeus

- When installing SpyEye there is even the “Kill Zeus” capability which if chosen, checks whether there are any installations of the Zeus Trojan, and uninstalls it before installing SpyEye.

- Towards the end of October, the bot code developers of SpyEye and Zeus bots were showing signs of a merger.
Approach #3:

Technical Attack Analysis
US charges 60 in connection with the Zeus Trojan

Zeus operators have made more than $200 million from the scam, authorities say

By Robert McMillan, IDG News Service
September 30, 2010 11:52 AM ET

U.S. authorities have charged more than 60 people in connection with the money-stealing Zeus Trojan program, according to the U.S. Department of Justice.

Zeus botnet bank thieves were careless with own security

The arrests follow a Tuesday U.K. sweep that led to 11 charges against Eastern European citizens thought to be involved in moving stolen funds out of the country.

Zeus has been a major problem for computer users and financial institutions over the past few years. Once installed on the victim’s PC, the malware can be used to log into a victim’s bank account and transfer funds to another account controlled by the criminals.
No Honor Among Thieves
Automated Attacks

- Botnets
- Mass SQL Injection attacks
- Google dorks
And You Can Monitor Trendy Attacks
Approach #4:
Traffic Analysis Via Honeypots
Example: DDoS 2.0
HTTP Request Caught A ToR Honeypot

+ POST /.dos/function.php HTTP/1.1
+ User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.3) Gecko/20100409 Gentoo Firefox/3.6.3
+ Parameters
  - ip=82.98.255.161&time=100&port=80
Google shows hundreds

Probably only the tip of the iceberg
Impact: Who was Brought Down?

- Only saw it launched against one server
  - IP was Dutch hosting provider
- But there is likely more
  - We only see a fraction of the general traffic on our honey pot
  - This is only one implementation of DoS
- Impact?
  - Depends on the hosting web server bandwidth
  - A cable modem user typically has a 384Kbs upstream
  - Web host in data center can have 1Gbps pipe
- 1 server = 3000 bots
Conclusions
Conclusions

- **Time to get proactive**
  - Scan Google for Dorks with respect to your application
    - Dorks and tools are available on the net
  - Search Google for Honey Tokens
    - Distinguishable credentials or credential sets
    - Specific distinguishable character strings
  - Watch out for name popping in the wrong forums…

- **Fighting automation**
  - CAPTCHA
  - Adaptive authentication
  - Access rate control
  - Click rate control
Conclusions

- Application Security Meets Proactive Security
  + Quickly identify and block source of recent malicious activity
  + Enhance attack signatures with content from recent attacks
  + Identify sustainable attack platforms
    - Anonymous proxies
    - TOR relays
    - Active bots
  + Identify references from compromised servers
  + Introduce reputation based controls
Imperva in 60 Seconds

- Usage
- Audit
- Access
- Control
- Rights Management
- Attack Protection
- Virtual Patching
- Reputation Controls
- Databases
- Files
- Web Apps

Data Security Suite
Questions?
Lesson #3: Automation

- Attacks are automated
  - Botnets
  - Mass SQL Injection attacks
  - Google dorks
Lesson #4: Optimization

- Hackers are looking at ways to optimize
  - Examples:
    - Compromise servers rather than PCs (insert pic!)
    - Malware distribution
    - Direct and indirect value

Take-away: Quickly identify and block source of recent malicious activity
Lesson #5: Mobile

- Hackers keep a tab on consumer trends
- Mobile security goes up the stack:
  - Mobile-platform attacks (1st generation threat)
  - Lost devices
  - Applications
  - The return of Web 2.0 vulnerabilities
Lesson #5: Mobile

- Hacker Forums – Mobile Discussions

Take-aways:
1. As an organization: Risk assessment with respect to mobile
2. As an application provider: Incorporation of new authentication/authorization channels
Lesson #6: Remember Old Threats

- Old threats do not die out! (Pic of Karl Marx)
  - Familiar
  - Succeeds

Take-away:
Drive forward but don’t forget to look into your rear-view
Summary

- Introduce proactive detection into your security environment
- Assess what is sensitive data and apply the necessary controls on that data
- Stop attacks before they even enter your application
- Ensure guards are updated in real-time
- Follow-up on trending attack techniques and models
- Irrelevant controls are not necessarily old controls
Did you feel that the session was both informative & useful?

A. Not very informative or useful
B. Somewhat informative and useful
C. Very informative and useful
Do you feel you know more about the issues & challenges posed to your organisation following this session?

A. No
B. Somewhat
C. Yes
Has the session *answered your questions* about the issues & challenges of the discussion topic?

A. No
B. Somewhat
C. Yes
Did the speakers present the topic well?

A. No
B. Somewhat
C. Yes
Using a scale of 1-5, how would you rate the session overall?

1. Poor
2. Met some of my expectations
3. Met my expectations
4. Good
5. Excellent

![Bar Chart]
Will you be attending any further sessions in the *Technical Theatre* during your visit to this year’s show?

A. Yes
B. Maybe
C. No
Will you be attending any other presentations in the other theatres during your visit to the show?

A. Yes
B. Maybe
C. No