Hacking: Industry Analysis

Hacking has become industrialized.

Attack techniques and vectors keep changing with an ever rapid pace.

Attack tools and platforms keep evolving.
Hack Fact #1:
Hackers Know the Value of Data Better Than the Good Guys
Data is hacker currency

<table>
<thead>
<tr>
<th>Overall Rank 2009</th>
<th>Item</th>
<th>Percentage 2009</th>
<th>Percentage 2008</th>
<th>Range of Prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Credit card information</td>
<td>19%</td>
<td>32%</td>
<td>$0.85-$30</td>
</tr>
<tr>
<td>2</td>
<td>Bank account credentials</td>
<td>19%</td>
<td>19%</td>
<td>$15-$850</td>
</tr>
<tr>
<td>3</td>
<td>Email accounts</td>
<td>7%</td>
<td>5%</td>
<td>$1-$20</td>
</tr>
<tr>
<td>4</td>
<td>Email addresses</td>
<td>7%</td>
<td>5%</td>
<td>$1.70/Million</td>
</tr>
<tr>
<td>5</td>
<td>Shell scripts</td>
<td>6%</td>
<td>3%</td>
<td>$2-$5</td>
</tr>
<tr>
<td>6</td>
<td>Full identities</td>
<td>5%</td>
<td>4%</td>
<td>$0.70-$20</td>
</tr>
<tr>
<td>7</td>
<td>Credit card dumps</td>
<td>5%</td>
<td>2%</td>
<td>$4-$1500</td>
</tr>
<tr>
<td>8</td>
<td>Mailers</td>
<td>4%</td>
<td>3%</td>
<td>$4-$10</td>
</tr>
<tr>
<td>9</td>
<td>Cash-out services</td>
<td>4%</td>
<td>3%</td>
<td>$0-$600</td>
</tr>
<tr>
<td>10</td>
<td>Website administration credentials</td>
<td>4%</td>
<td>3%</td>
<td>$2-$30</td>
</tr>
</tbody>
</table>

Table 5. Goods and services advertised on underground economy servers
Source: Symantec
# Website Access up for Sale

<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://gs.mil/al/">http://gs.mil/al/</a></td>
<td>ARMY Forces of republic of albania</td>
<td>Full SiteAdmin 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://cecom.army.mil/">http://cecom.army.mil/</a></td>
<td>The United States Army</td>
<td>CECOM</td>
<td>Full SiteAdmin Control/SSH Root access</td>
<td>unknown</td>
</tr>
<tr>
<td><a href="http://pec.he.osd.mil/">http://pec.he.osd.mil/</a></td>
<td>The Department of defense pharmacoeconomic Center</td>
<td>Full SiteAdmin Control/Root access, High value informations</td>
<td>unknown</td>
<td>$399</td>
</tr>
<tr>
<td><a href="http://www.woodwards.edu/uy/">http://www.woodwards.edu/uy/</a></td>
<td>Woodwards School Uruguay</td>
<td>Full SiteAdmin Control</td>
<td>5200</td>
<td>$333</td>
</tr>
<tr>
<td><a href="http://s-u.edu.in/">http://s-u.edu.in/</a></td>
<td>Singhania University</td>
<td>Full SiteAdmin Control</td>
<td>unknown</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>Students/Exams user/pass and full admin access</td>
<td>56003</td>
<td>$90</td>
</tr>
<tr>
<td><a href="http://www.tsrc.tp.edu.tw/">http://www.tsrc.tp.edu.tw/</a></td>
<td>Taipei City East Special Education Resource Center</td>
<td>Full SiteAdmin Control</td>
<td>74198</td>
<td>$88</td>
</tr>
<tr>
<td><a href="http://tcpanteleo.gov.it/">http://tcpanteleo.gov.it/</a></td>
<td>Italian Official Government Website</td>
<td>Full SiteAdmin Control</td>
<td>292942</td>
<td>$99</td>
</tr>
<tr>
<td><a href="http://donmilerinapoli.gov.it/">http://donmilerinapoli.gov.it/</a></td>
<td>Istituto Statale Don Lorenzo Milano</td>
<td>Full SiteAdmin Control</td>
<td>292942</td>
<td>$99</td>
</tr>
<tr>
<td><a href="http://itogesseo.gov.it/">http://itogesseo.gov.it/</a></td>
<td>Italian gov website</td>
<td>Full SiteAdmin Control</td>
<td>292942</td>
<td>$99</td>
</tr>
<tr>
<td><a href="http://itmarconi.gov.it/">http://itmarconi.gov.it/</a></td>
<td>Official Italian gov website</td>
<td>Full SiteAdmin Control</td>
<td>292942</td>
<td>$99</td>
</tr>
<tr>
<td><a href="http://pnmodircivico.gov.it/">http://pnmodircivico.gov.it/</a></td>
<td>Official Italian gov website</td>
<td>Full SiteAdmin Control</td>
<td>292942</td>
<td>$99</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 SiteAdmin Control</td>
<td>1123</td>
<td>$88</td>
</tr>
<tr>
<td><a href="http://michigan.gov/">http://michigan.gov/</a></td>
<td>American State of Michigan Official Website</td>
<td>MySQL root access/Valueable information</td>
<td>205070</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 john123@gmail.com
<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://gs.mil.al/">http://gs.mil.al/</a></td>
<td>ARMY Forces of republic of albania</td>
<td>Full Site Admin Control + High value informations</td>
<td>unknown</td>
<td>$499</td>
</tr>
<tr>
<td><a href="http://www.cecom.army.mil/">http://www.cecom.army.mil/</a></td>
<td>South Carolina National</td>
<td>MySQL root access + High</td>
<td>unknown</td>
<td>$1400</td>
</tr>
<tr>
<td><a href="http://cecom.army.mil/">http://cecom.army.mil/</a></td>
<td>The United States Army</td>
<td>Full Site Admin Control/SSH Root access</td>
<td>unknown</td>
<td>$499</td>
</tr>
<tr>
<td><a href="http://www.woodlands.edu.gov/">http://www.woodlands.edu.gov/</a></td>
<td>Woodlands School Uruguay, Singhania University</td>
<td>Full Site Admin Control</td>
<td>5200</td>
<td>$33</td>
</tr>
<tr>
<td><a href="http://www.nccu.edu.tw/">http://www.nccu.edu.tw/</a></td>
<td>National Chengchi University.</td>
<td>Students/Exams user/pass and full admin access!</td>
<td>56003</td>
<td>$90</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>74138</td>
<td>$88</td>
</tr>
<tr>
<td><a href="http://donmillerinapoli.gov.it/">http://donmillerinapoli.gov.it/</a></td>
<td>Istituto Statale Con Lorenzo Milano</td>
<td>Full Site Admin Control</td>
<td>292942</td>
<td>$99</td>
</tr>
<tr>
<td><a href="http://tgcesaro.gov.it/">http://tgcesaro.gov.it/</a></td>
<td>Official Italian gov website.</td>
<td>Full Site Admin Control</td>
<td>292942</td>
<td>$99</td>
</tr>
<tr>
<td><a href="http://pmocircolovicco.gov.it/">http://pmocircolovicco.gov.it/</a></td>
<td>Official Italian gov website</td>
<td>Full Site Admin Control</td>
<td>292942</td>
<td>$99</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>$88</td>
</tr>
</tbody>
</table>

- Daily updated - 

[Click here to check for proof of the hacked sites.](#)

Email me or add me in MSN at [email protected]
Hack Fact #2: Hackers—By Definition—Are Early Adopters
Example: Mobile (In)Security

Growth of Discussion of Mobile Platforms by year

Source: Imperva’s Application Defense Center Research
Hack Fact #3:
The Good Guys Have More Vulnerabilities Than Time, Resourcing Can Manage
Situation Today

# of websites : 357,292,065 (estimated: July 2011)
# of vulnerabilities : 230

821,771,600 vulnerabilities in active circulation

Vulnerabilities by Industry

Top Vulnerabilities by Industry (2010)

Source: WhiteHat 2011
Hack Fact #4:

Attack Automation is Prevailing
Automation is Prevailing

- In one hacker forum, it was boasted that one hacker had found 5012 websites vulnerable to SQLi through automation.

Things to note:

- Due to automation, for only a few dollars, hackers can be effective in small groups – i.e. Lulzsec.

- Automation also means that attacks are equal opportunity offenders. They don’t discriminate between well-known and unknown sites.
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

- Focus on actual threats
- Devise new defenses based on real data and 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
Hacker Forum Analysis #1: General Topics
Jan-June 2011

Source: Imperva
Hacker Forum Analysis #2: Tech Discussions
Jan-June 2011

Top 7 Attacks Discussed
(# Threads with keyword)

- dos/ddos: 22%
- SQL Injection: 19%
- spam: 16%
- shell code: 12%
- brute-force: 12%
- zero-day: 10%
- HTML Injection: 9%
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?
Approach #3: Technical Attack Analysis
US charges 60 people in connection with the Zeus Trojan

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
And You Can Monitor Trendy Attacks

CNN EXCLUSIVE VIDEO OF THE DEATH OF OSAMA BIN LADEN BY U.S.

Original text:
EL TERRORISTA MAS BUSCADO DE TODO EL MUNDO POR AÑOS POR FIN HA SIDO CAPTURADO Y ASESIADO POR EL EJERCITO DE ESTADOS UNIDOS QUIENES TOMARON FOTOS Y VIDEOS COMO TROFEO PERSONAL DE TAN GRANDIOSA ASANA LA CUAL CONTARAN A SUS NIETOS

The most wanted terrorist WORLDWIDE AT LAST FOR YEARS HAS BEEN CAUGHT AND KILLED BY THE UNITED STATES ARMY WHO TOOK PHOTOS AND VIDEOS AS GREAT AS PERSONAL TROPHY WHICH ASANA tell their grandchildren
And You Can Monitor Trendy Attacks
Approach #4:
Traffic Analysis Via Honeypots
Automated Attacks

- **Botnets**
- **Mass SQL Injection attacks**
- **Google dorks**
Finding#1: Automation is Prevailing

On Average:
27 attacks per hour
≈ 1 probe every two minutes

Apps under automated attack:
25,000 attacks per hour.
≈ 7 per second
The Unfab Four

- Directory traversal: 37%
- SQLi: 23%
- XSS: 36%
- RFI: 4%
29 percent of the attack events originated from the 10 most active attack sources
Research Compared to Lulzsec Activity

Lulzsec was a team of hackers focused on breaking applications and databases.

Our observations have a striking similarity to the attacks employed by Lulzsec during their campaign.

Lulzsec used: SQL Injection, Cross-site Scripting and Remote File Inclusion.
Addressing the public on Thursday, LulzSec said that a single SQL Injection flaw led them to more than one million clear text passwords, 3.5 million “music coupon” codes, and 75,000 “music codes”.

Tool #1: Remote File Include

The relevant snippet from the chat log (emphasis ours):

lol - storm would you also like the RFI/LFI bot with google bypass i was talking about while i have this plugged in?

lol - i used to load about 8,000 RFI with usp flooder crushed most server :D

- 1 infected server ≈ 3000 bot infected PC power
- 8000 infected servers ≈ 24 million bot infected PC power

In 2009, a XSS vulnerability was found on the Sun website. A LulzSec member found an old server still online and running an old version of the newspaper website being still vulnerable to the same attack! Once pwned, this server was used as a jump-host to go deeper into the infrastructure. Finally the content management system used to publish the breaking news was also pwned: A simple line of JavaScript code injected in all published news was enough to redirect all the visitors to the fake page hosted somewhere else.
Conclusions
Get Proactive

- 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.
Fight Automation

Adjusted blocking
- Black-list IPs
- Keep lists reflective of real-time malicious sources

CAPTCHA
- Image
- Other methods exist (solving a riddle, watching a video, audio, etc.)

Adaptive authentication
- Alert the user
- Repeat password or answer previously recorded question

Client-side computational challenges
- Slow on the client, quick on the server

Disinformation
- Bogus links
- Hidden Links
Conclusion

The top five security providers—led by Symantec and McAfee—accounted for 44 percent of the $16.5 billion worldwide security software market in 2010, according to Gartner. That’s down from 60 percent in 2006.

“The security industry may need to reconsider some of its fundamental assumptions, including 'Are we really protecting users and companies?'”

Important Details

✔️ If you want slides, send: your credit card number, mother’s maiden name and an email to:

rob.rachwald@imperva.com
Thank You