



Cyber Vigilantes

Rob Rachwald
Director of Security Strategy

Porto Alegre, October 5, 2011

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

Overall Rank		Item	Percentage		Range of Prices
2009	2008		2009	2008	
1	1	Credit card information	19%	32%	\$0.85-\$30
2	2	Bank account credentials	19%	19%	\$15-\$850
3	3	Email accounts	7%	5%	\$1-\$20
4	4	Email addresses	7%	5%	\$1.70/MB
5	9	Shell scripts	6%	3%	\$2-\$5
6	6	Full Identities	5%	4%	\$0.70-\$2
7	13	Credit card dumps	5%	2%	\$4-\$150
8	7	Mallers	4%	3%	\$4-\$10
9	8	Cash-out services	4%	3%	\$0-\$600
10	12	Website administration credentials	4%	3%	\$2-\$30

Table 5. Goods and services advertised on underground economy servers

Source: Symantec

07-31-2010, 05:42 PM

molodec ▾

Join Date: Jun 2010

Posts: 27

Репутация: -3

Сфера: Stuff, CC, Cashing

Цитата выделенного

Offline !

Yesterday, 09:47 AM

Peks ▾

Sell CC base

Have 2 bases:
EU (1.3k valid)
USA (>2k valid)
Prices and conditions of deal ----> 402860090

Он в блэке на соседних площадках. В частнос

Website Access up for Sale

Website Hacking
LR ID: 3.333

Offers Services Proofs Free Logins Payment method

Site	Details	Level of Control	Traffic	Price
http://gs.mil.al/	ARMY Forces of republic of albania	Full SiteAdmin Control + High value informations	unknown	\$499
http://www.scguard.army.mil/	Souce Carolina National Guard	MySQL root access + High value informations	unknown	\$499
http://cecom.army.mil/	The United States Army CECOM	Full SiteAdmin Control/SSH Root access	unknown	\$499
http://pec.ha.osd.mil/	The Department of defense pharmaco-economic Center	Full SiteAdmin Control/Root access, High value informations!	unknown	\$399
http://www.woodlands.edu.uy/	Woodlands School Uruguay.	Full SiteAdmin Control!	5200	\$33
http://s-u.edu.in/	Singhania University	Full SiteAdmin Control.	unknown	\$55
http://www.nccu.edu.tw/	National Chengchi University.	Students/Exams user/pass and full admin access!	56093	\$99
http://www.terc.tp.edu.tw/	Taipei City East Special Education Resource Center	Full SiteAdmin Control.	74188	\$88
http://itcpantaleo.gov.it/	Italian Official Government Website.	Full SiteAdmin Control.	292942	\$99
http://donmilaninapoli.gov.it/	Istituto Statale Don Lorenzo Milani	Full SiteAdmin Control.	292942	\$99
http://itcgcesaro.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	\$99
http://itimarconi.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	\$99
http://primocircolovico.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	\$99
http://www.utah.gov/	American State of Utah Official Website.	Full SiteAdmin Control.	173146	\$99
http://www.uscb.edu/	University of South Carolina Beaufort.	Full SiteAdmin Control.	1123	\$88
http://michigan.gov/	American State of Michigan Official Website.	MySQL root access/Valuable information.	205070	\$55

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

Email me or add me in MSN at [\[icon\]](#) @gmail.com

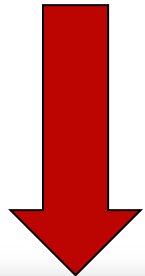


Website Access up for Sale

Website Hacking
LR ID: 3533

Offers Services Proofs Free Logins Payment method

Site	Details	Level of Control	Traffic	Price
http://gs.mil.al/	ARMY Forces of republic of albania	Full SiteAdmin Control + High value informations	unknown	\$499
http://www.squad.army.mil/	Souce Carolina National	MySQL root access + High	unknown	\$499



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

http://pec.ha.osd.mil/	The Department of Defense pharmacoeconomic Center	access, High value informations!	unknown	\$399
http://www.woodlands.edu.uy/	Woodlands School Uruguay.	Full SiteAdmin Control!	5200	\$33
http://s-u.edu.in/	Singhania University	Full SiteAdmin Control.	unknown	\$55
http://www.nccu.edu.tw/	National Chengchi University.	Students/Exams user/pass and full admin access!	56093	\$99
http://www.terc.tp.edu.tw/	Taipei City East Special Education Resource Center	Full SiteAdmin Control.	74188	\$88
http://itcpantaleo.gov.it/	Italian Official Government Website.	Full SiteAdmin Control.	292942	\$99
http://donmilaninapoli.gov.it/	Istituto Statale Don Lorenzo Milani	Full SiteAdmin Control.	292942	\$99
http://itcgcesaro.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	\$99
http://itimarconi.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	\$99
http://primocircolovico.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	\$99
http://www.utah.gov/	American State of Utah Official Website.	Full SiteAdmin Control.	173146	\$99
http://www.uscb.edu/	University of South Carolina Beaufort.	Full SiteAdmin Control.	1123	\$88
http://michigan.gov/	American State of Michigan Official Website.	MySQL root access/Valuable information.	205070	\$55

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

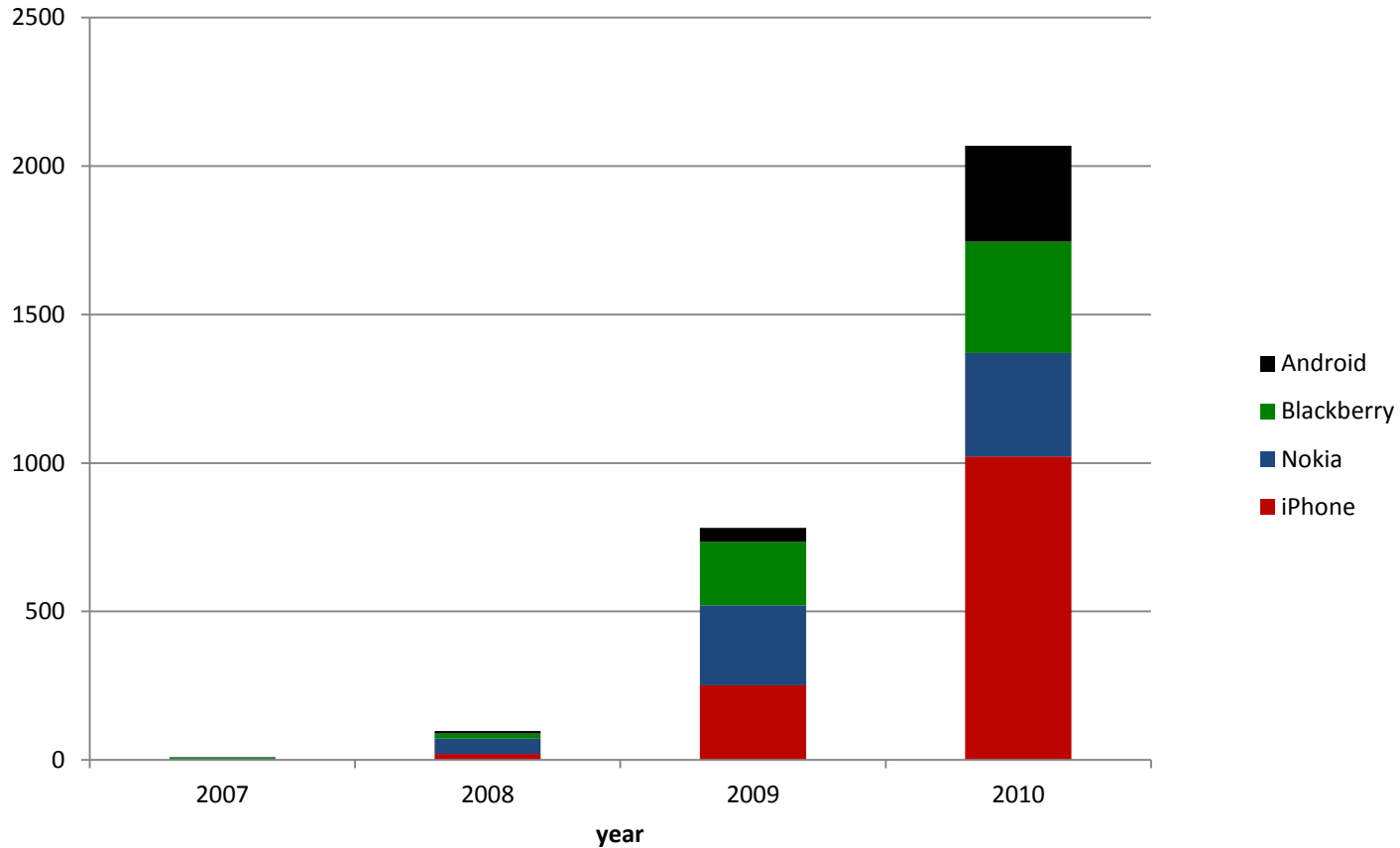
Email me or add me in MSN at [\[Profile\]](#) @gmail.com

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 : X
230

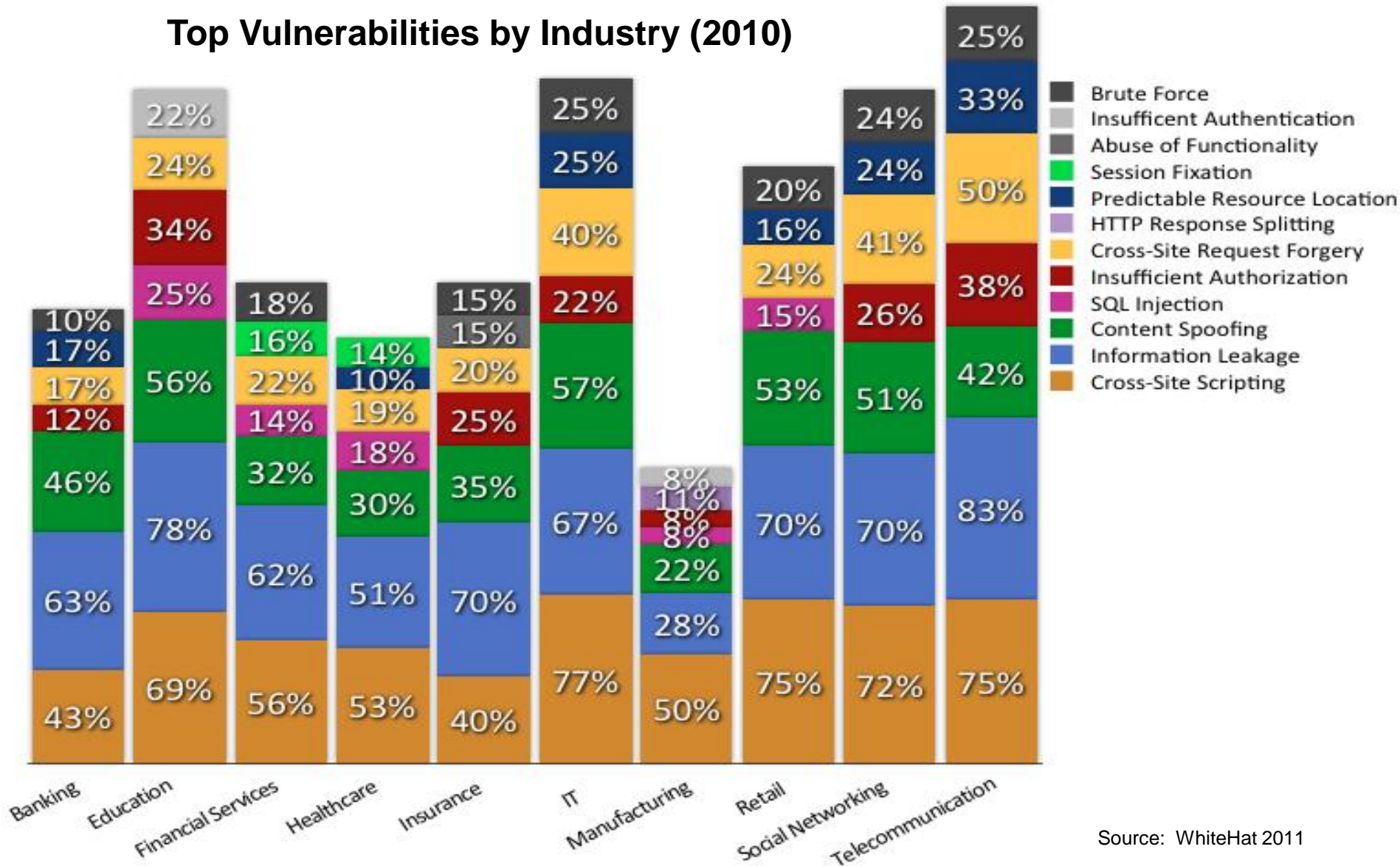
1%

821,771,600

vulnerabilities in active circulation

Vulnerabilities by Industry

Top Vulnerabilities by Industry (2010)



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.

5012 SQL Injectable Websites

Collected by ██████████ - ██████████

```
http://www.██████████.com/trainers.php?id='4
http://www.██████████.com/trainers.php?id='30
http://www.██████████.com/trainers.php?id='30
http://www.██████████.com/article.php?ID='338
http://www.██████████.com/publications/article.php?ID='51
http://www.██████████.com/article.php?id='13798
http://www.██████████.com/news/article.php?id='0222
http://www.██████████.com/article.php?id='59
http://www.██████████.com/press/article.php?id='000073
http://www.██████████.com/article.php?id='5
http://www.██████████.net/article.php?id='104
http://www.██████████.net/article.php?id='1089
http://www.██████████.net/news/article.php?id='416
http://www.██████████.net/article.php?id='2524
http://www.██████████.net/article.php?id='11012&lang='th
http://www.██████████.net/news/article.php?id='48
http://www.██████████.net/nl/article.php?id='1512&type='col
```

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



Cyber Vigilantes



Approach #1:

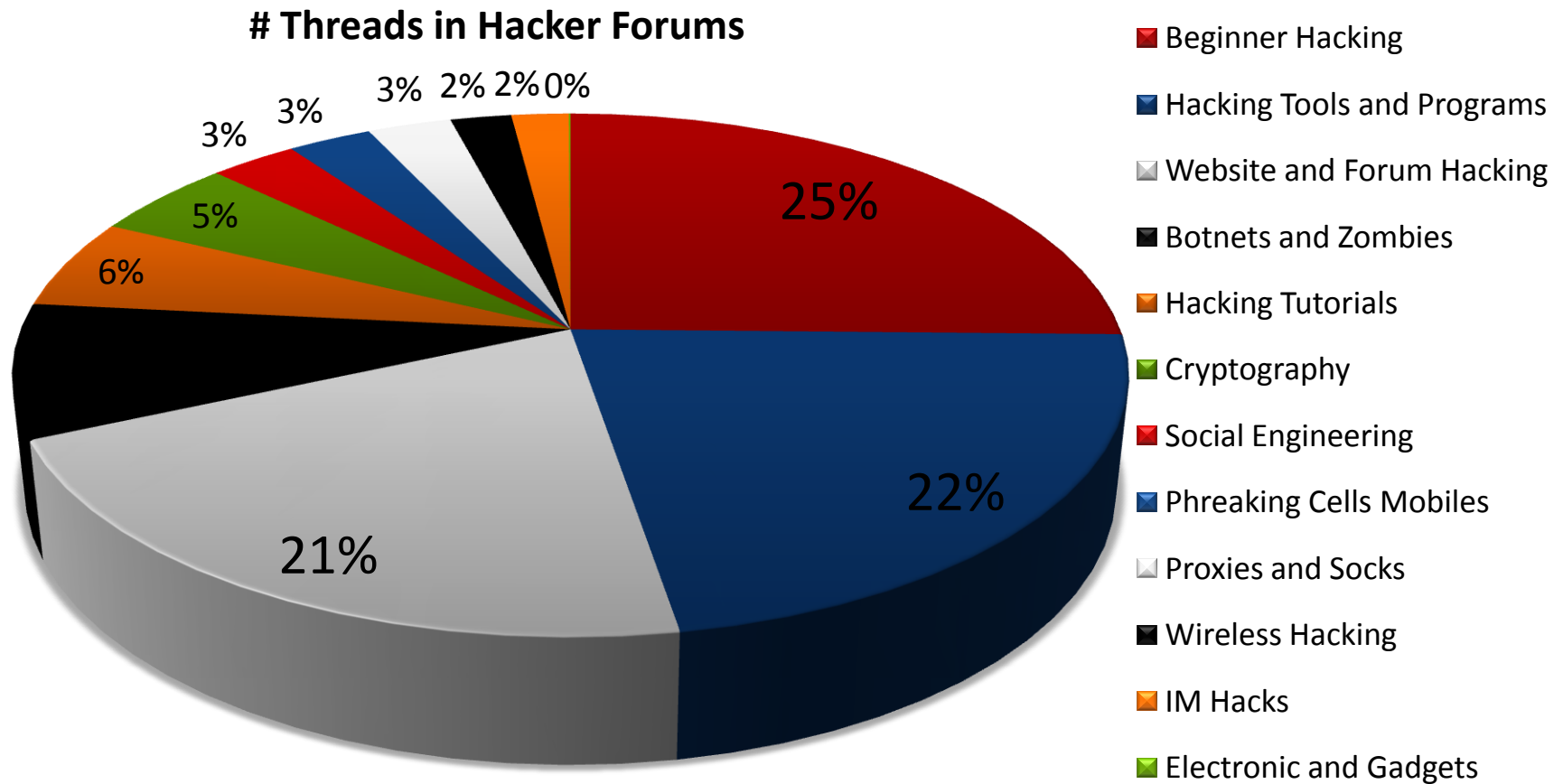
Monitoring Communications

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

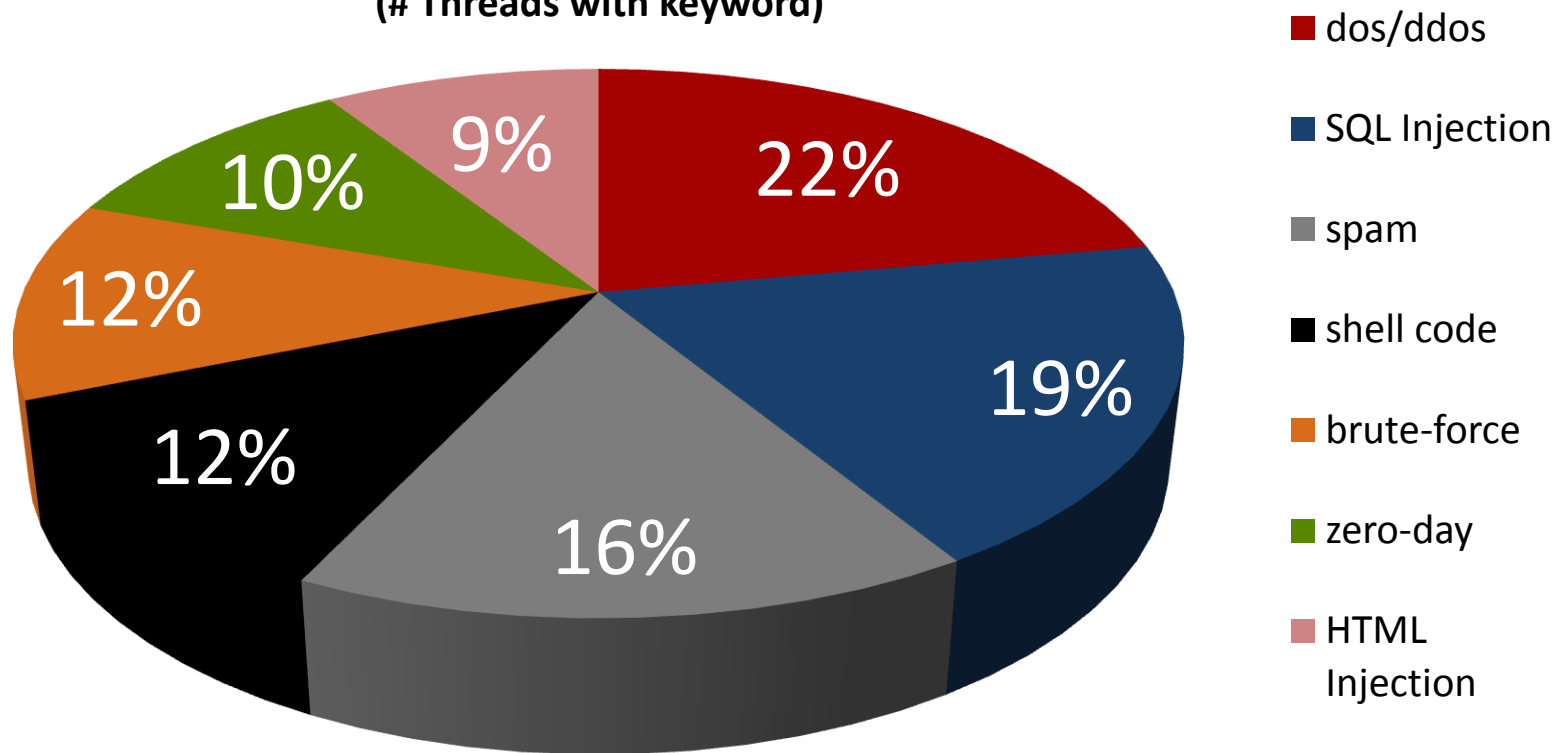
Jan-June 2011



Hacker Forum Analysis #2: Tech Discussions

Jan-June 2011

Top 7 Attacks Discussed
(# Threads with keyword)



Approach #2:

Knowing Hacker Business Models

Example: Rustock

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

Getting Into Command and Control Servers

host
74.63.218.188
apis.videosurf.co
66.218.161.13
safebrowsing.clients.go
ocsp.verisign.co
login.hi5.com
baymsg1010711.by2.gateway.edge
ocsp.thawte.co
ocsp.comodoca.c
es-ve.hi5.com
foro.miustragus.o
ocsp.godaddy.co
bancolumbia.olb.todo
asterixworld.ne

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

[Comment](#) [Print](#)

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

The image shows the 'Quick Setup: Login Spoofer 2010' window. The main window, 'Login Spoofer v1.5 by hol4ko', features a 'Fake Pages' list with radio buttons for Hotmail, Gmail, Yahoo!, Gamezzer, Facebook, MSN Block Checker, Skyrock, Skype, PayPal, Travian, Maktoob, RapidShare, Myspace, 4Shared, CamFrog, and MegaUpload. The 'Options' section includes checkboxes for 'Open Folder', 'Page Preview', 'Encrypt', and 'File encryption'. The 'Advanced' section has radio buttons for 'File Extension' (HTML or PHP) and a checked 'File encryption' option. A 'Save in' field shows 'C:\' with a 'Browse Folder' button. At the bottom, there are buttons for 'Start', 'Create The Fake page', 'About!', and 'Show / Hide Victim'. Red arrows point from these buttons to Arabic text boxes: 'Start' points to 'لنا لتشغيل لأول مرة', 'Create The Fake page' points to 'زر صنع الصفحة المزورة', 'About!' points to 'عن البرنامج', and 'Show / Hide Victim' points to 'أو اخفاء ايا'. Other annotations include 'فتح المجلد بعد الصنع' pointing to 'Open Folder', 'معاينة الصفحة بعد' pointing to 'Page Preview', and 'You have (19) Victimes | [Refresh]' pointing to the victim list.

Terms:
This is a freeware program. Coded by hol4ko. Clicking "Start" button you are agree with the terms of the program. That you have full responsibility of using it!

Options:
 Open Folder
 Page Preview

Advanced:
File Extension: HTML PHP
Encrypt
 File encryption

Save in: C:\ Browse Folder

Buttons: Start, Create The Fake page, About!, Show / Hide Victim

Victims List:

Username: vikkie_██████████@yahoo.com
Password: zmu██████████
Type: Yahoo
IP: 116.71.62.117

Username: vikkie_██████████@yahoo.com
Password: zmu██████████
Type: Yahoo
IP: 116.71.62.117

Username: vikkie_██████████
Password: zmu██████████
Type: Yahoo
IP: 116.71.62.117

Username: not
Password: atall
Type: Paypal
IP: 192.251.226.205

Username: not
Password: atall
Type: Paypal
IP: 203.174.87.18

And You Can Monitor Trendy Attacks



And You Can Monitor Trendy Attacks



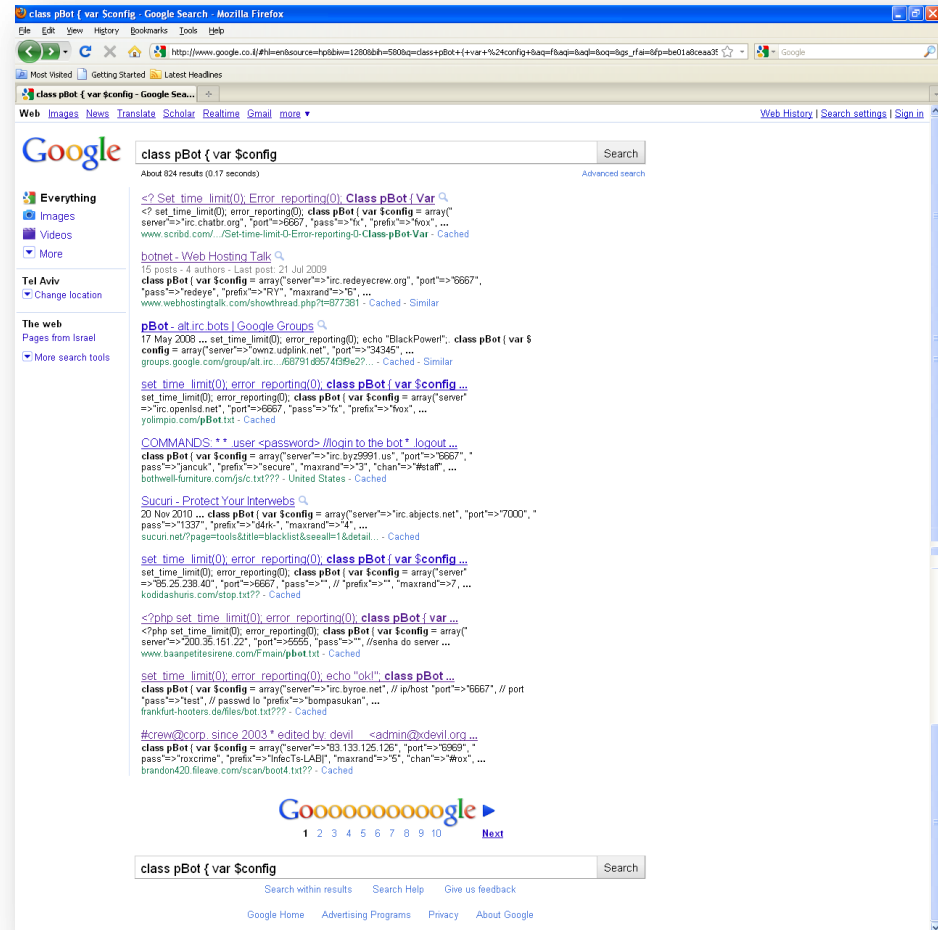
The image shows a screenshot of a Facebook interface. At the top left is the 'facebook' logo. To its right is a search bar with the word 'Search' and a magnifying glass icon. Below the search bar is a post with the following text: 'Get LAID With Girls From FBook Transform Your PC Into a Seduction Machine'. To the right of this text is a 'Like' button with a thumbs-up icon. Below the text is the word 'Website'. To the left of the post is a profile picture of a woman in a black bikini. Below the post is a large red banner with the word 'LEARN' in white, bold, capital letters. To the right of the banner is another image of the same woman in a black bikini.

Approach #4:

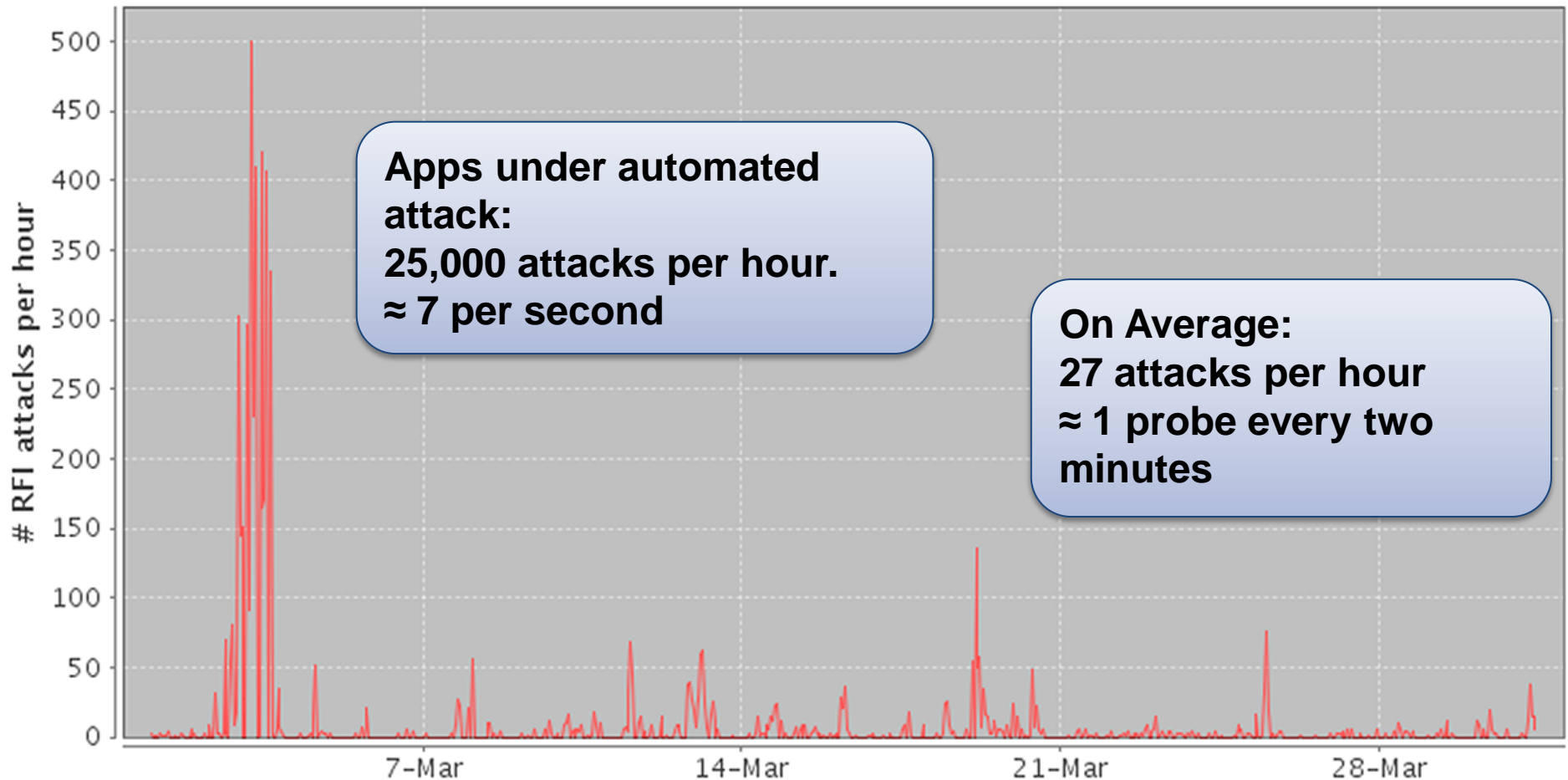
Traffic Analysis Via Honeypots

Automated Attacks

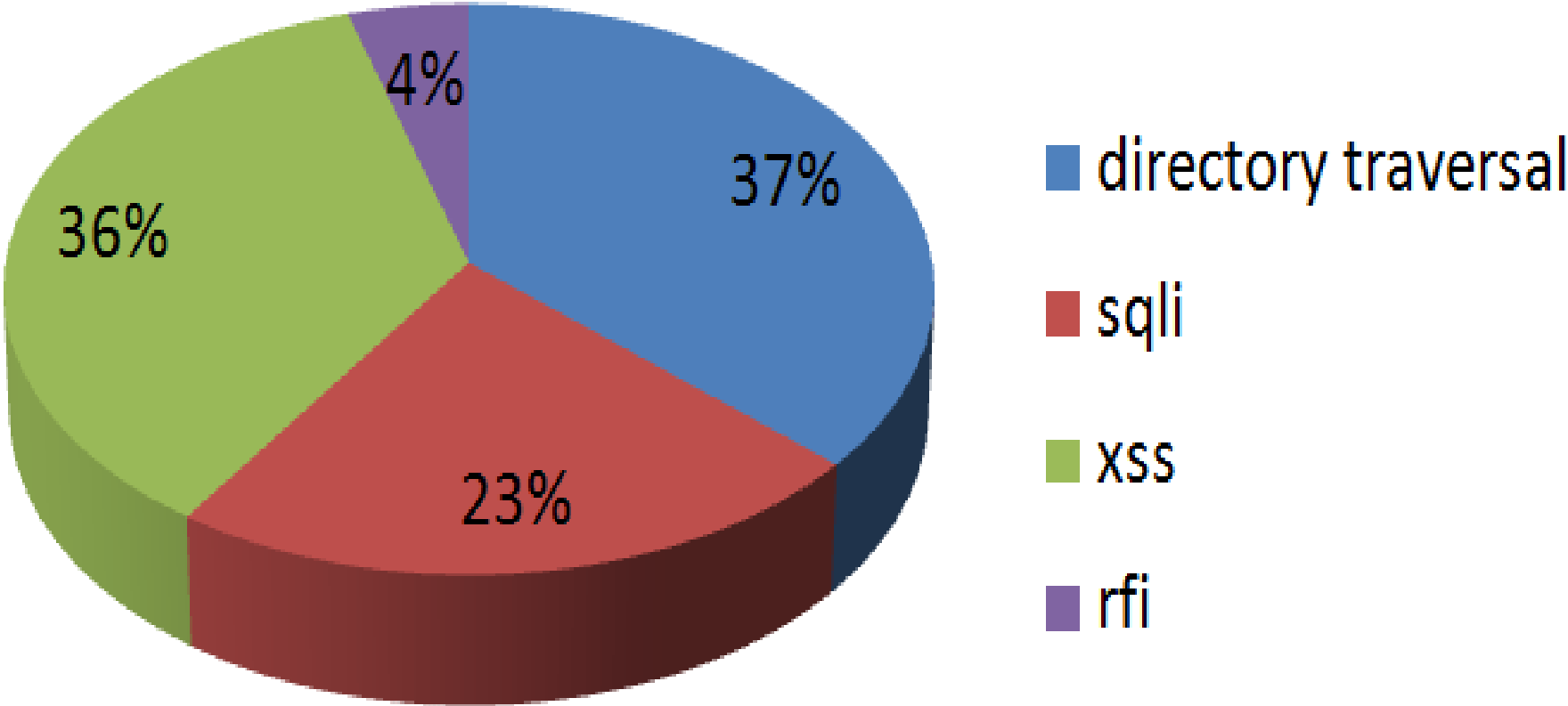
- Botnets
- Mass SQL Injection attacks
- Google dorks



Finding#1: Automation is Prevailing



The Unfab Four



Finding #2: Reputation Matters

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.



Lulzsec Activity Samples

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 \approx 3000 bot infected PC power
- ❖ 8000 infected servers \approx 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



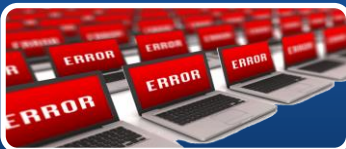
Quickly identify and block source of recent malicious activity.



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

$$\frac{d}{dt} \int_{V_0} \left[k + \rho\phi + \frac{a_0^2}{8\pi G} F \left(\frac{\|\nabla\phi\|}{a_0} \right) \right] d^3x$$
$$= \frac{1}{4\pi G} \int_{\partial V_0} \mu \frac{\partial\phi}{\partial t} (\nabla\phi, \hat{n}) da, \quad (8)$$

Client-side computational challenges

- Slow on the client, quick on the server



Disinformation

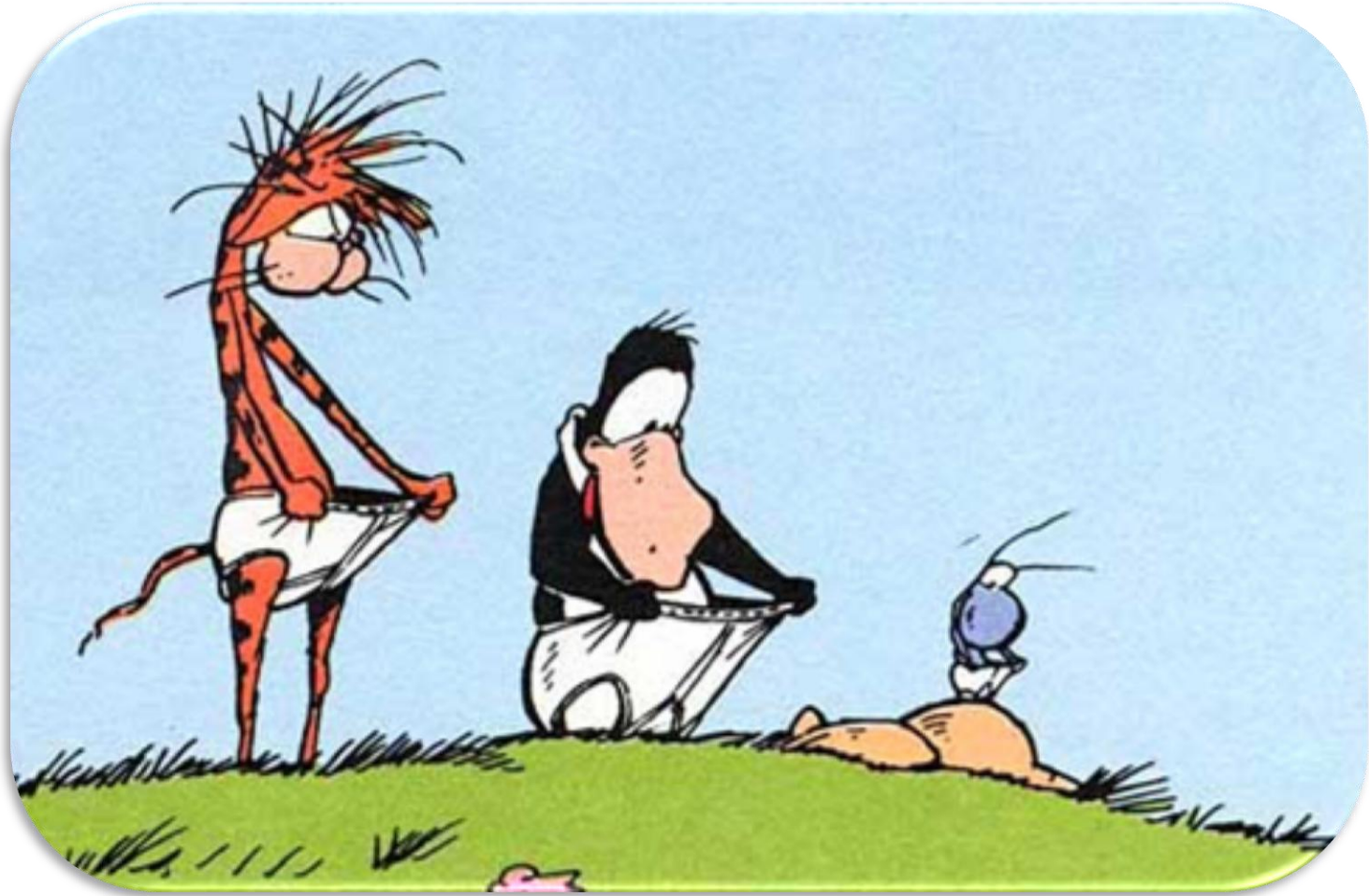
- Bogus links
- Hidden Links

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.

Source: <http://www.bloomberg.com/news/2011-08-04/hacker-armageddon-forces-symantec-mcafee-to-search-for-fixes.html>

Conclusion



Conclusion

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

McAfee

Source: <http://www.nytimes.com/external/readwriteweb/2011/08/23/23readwriteweb-mcafee-to-security-industry-are-we-really-p-70470.html?partner=rss&emc=rss>

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