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.

IMPERVA®

Hack Fact #1:

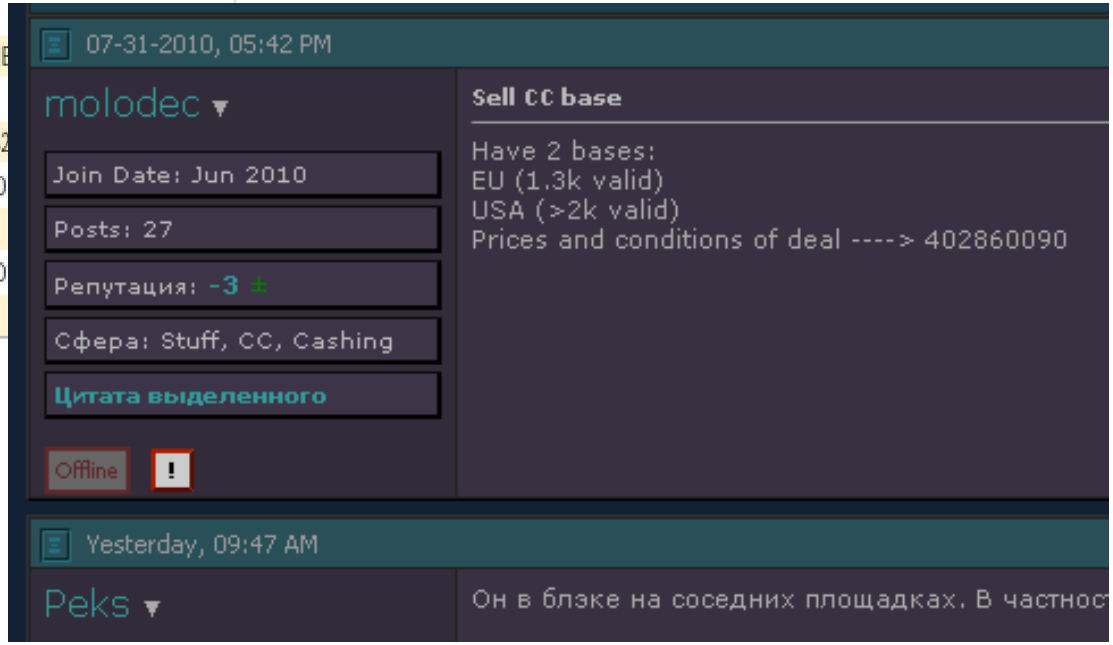
Hackers Know the Value of Data Better Than the Good Guys

IMPERVA®

Data is hacker currency

Overall Rank 2009	2008	Item	Percentage 2009	2008	Range of Prices
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/ME
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	Mailers	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



IMPERVA®

Website Access up for Sale

Website Hacking
LR ID: [redacted]

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 pharmacoeconomic Center	Full SiteAdmin Control/Root access, High value informations!	unknown	$399
http://www.woodlands.edu.uy/	Wooldlands 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 [redacted]@gmail.com

IMPERVA®

Website Access up for Sale

Website Hacking
LR ID: [redacted]

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	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/	Wooldlands 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 [redacted]@gmail.com

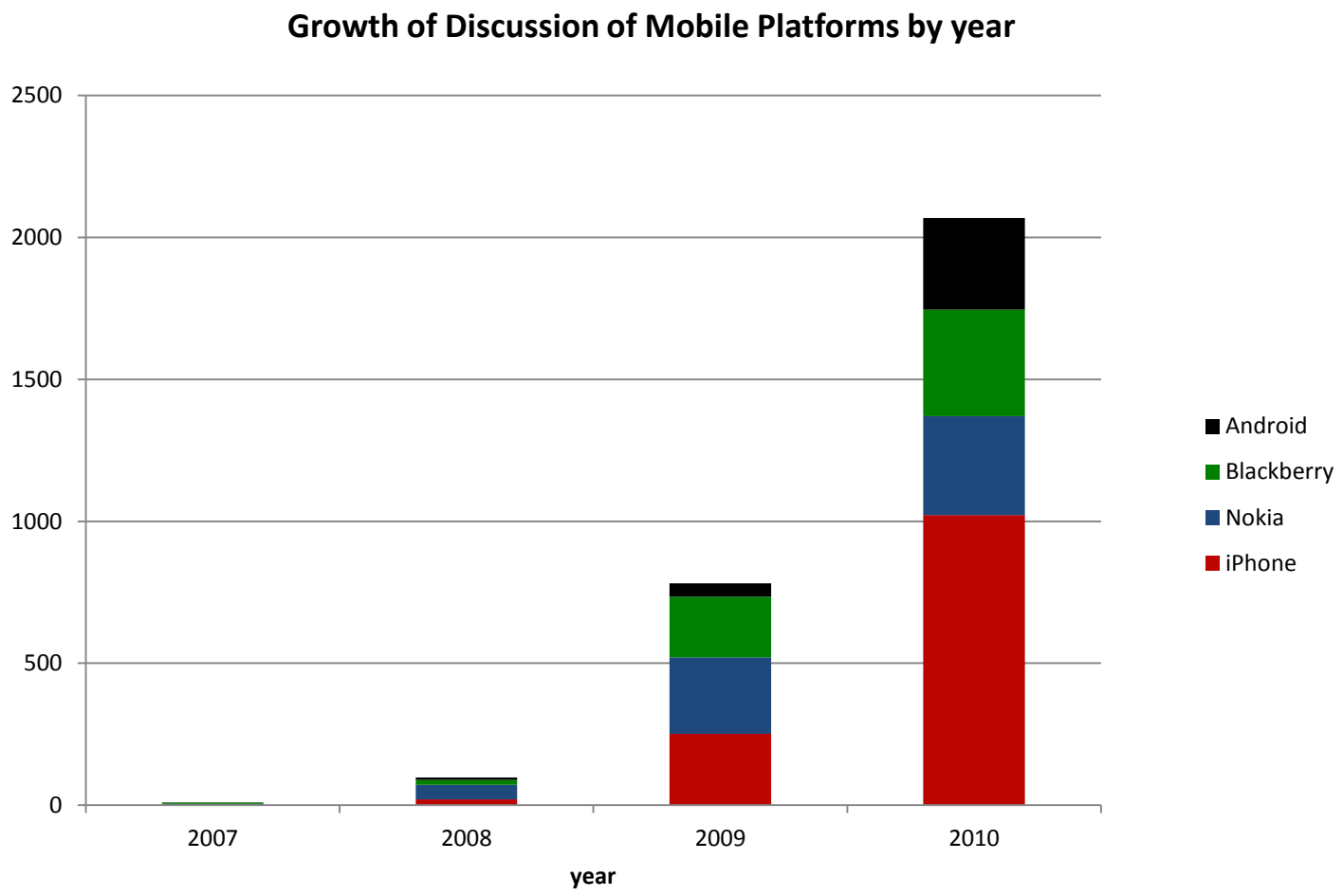
IMPERVA®

Hack Fact #2:

Hackers—By Definition—Are Early Adopters

IMPERVA®

Example: Mobile (In)Security



Source: Imperva's Application Defense Center Research

Hack Fact #3:

The Good Guys Have More Vulnerabilities Than Time, Resourcing Can Manage

IMPERVA®

Situation Today

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

X

# of vulnerabilities : 230

1%

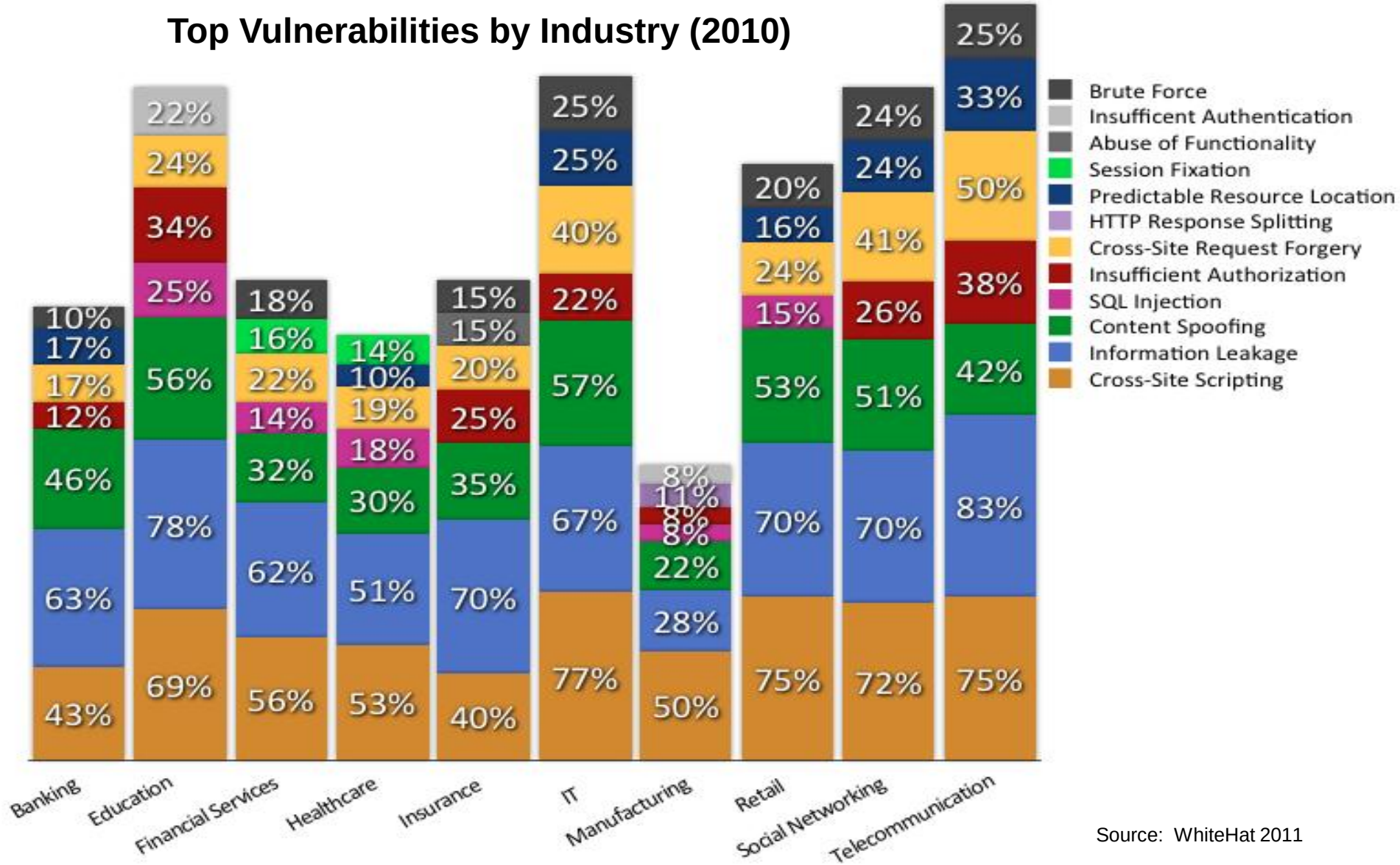
821,771,600

vulnerabilities in active circulation

Source: http://news.netcraft.com/archives/2011/07/08/july-2011-web-server-survey.html
https://www.whitehatsec.com/home/resource/stats.

IMPERVA®

Vulnerabilities by Industry



Source: WhiteHat 2011

Hack Fact #4:

Attack Automation is Prevailing

IMPERVA®

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 [redacted] - [redacted]

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

IMPERVA®

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

IMPERVA®

Approach #1:

Monitoring Communications

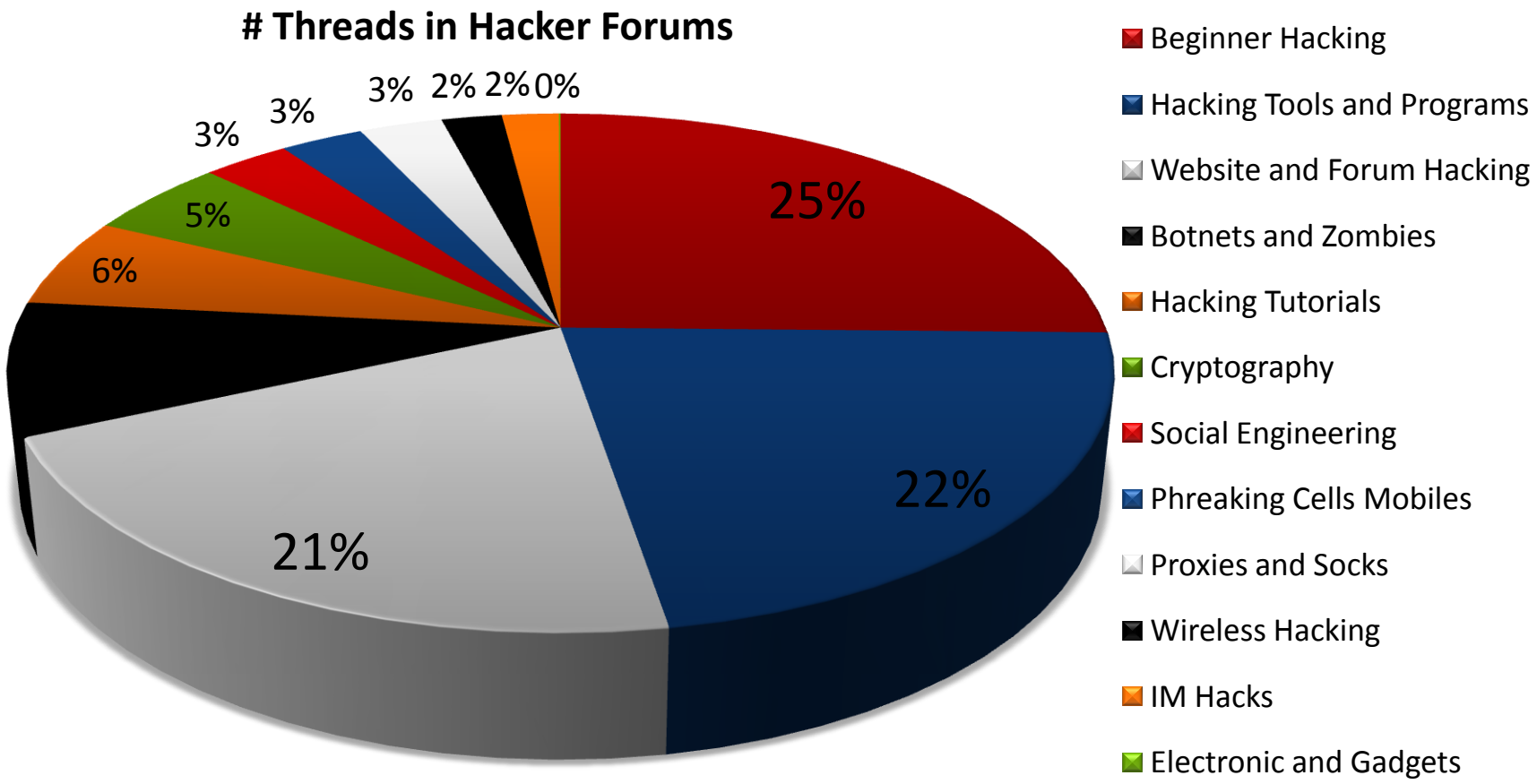
IMPERVA®

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

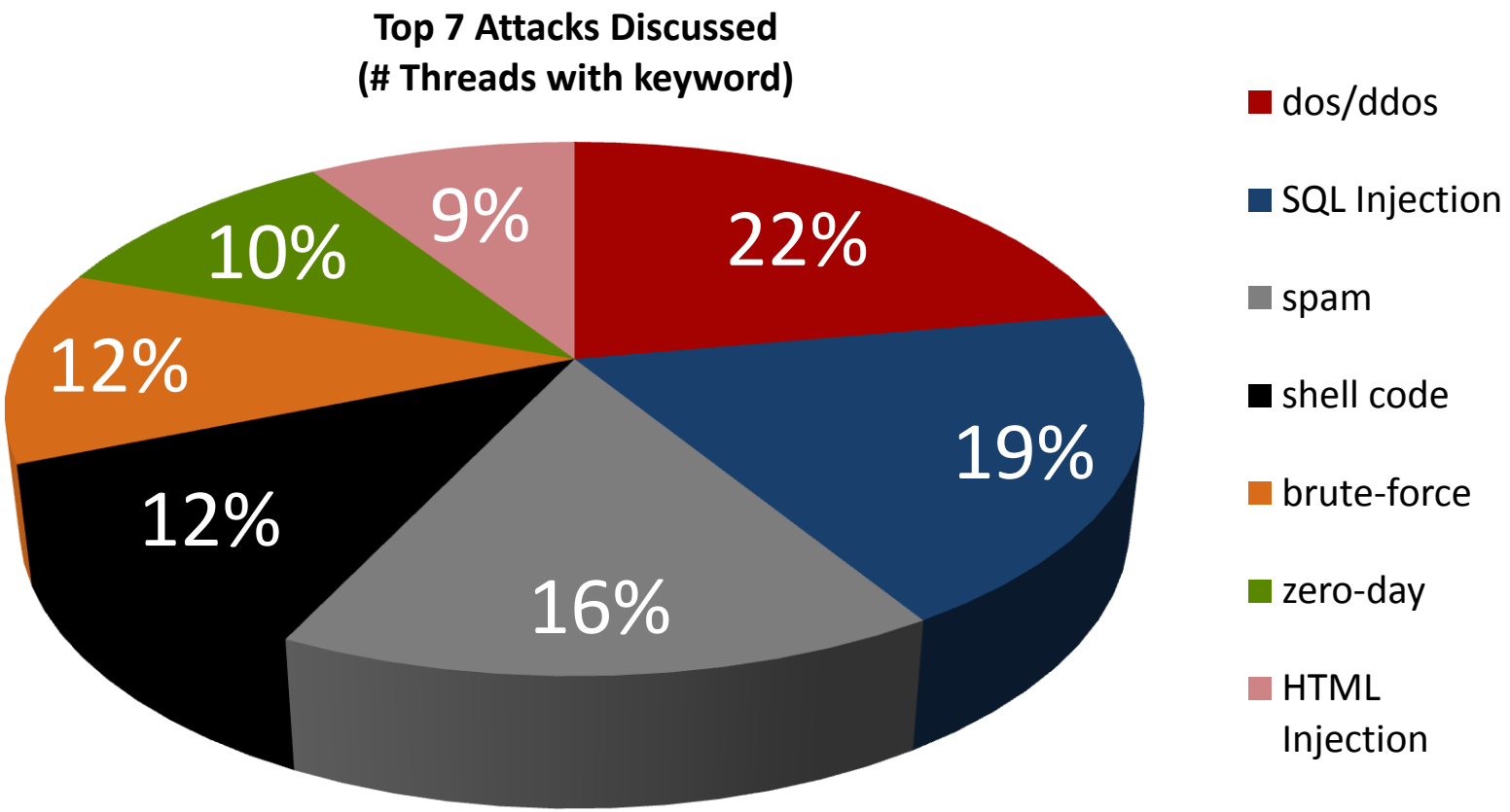


Source: Imperva

IMPERVA®

Hacker Forum Analysis #2: Tech Discussions

Jan-June 2011



IMPERVA®

Approach #2:

Knowing Hacker Business Models

IMPERVA®

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.

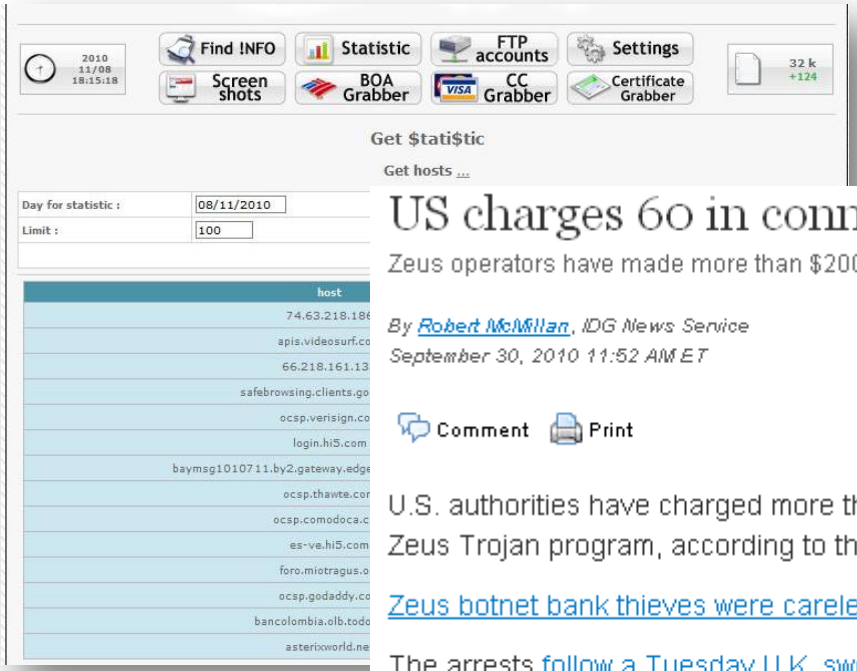
At its height, the Rustock botnet pumped out 13.82 billion emails per day, comprising 29% of the world's daily spam diet. But will the Rustock respite last?

Approach #3:

Technical Attack Analysis

IMPERVA®

Getting Into Command and Control Servers



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.

IMPERVA®

No Honor Among Thieves

And You Can Monitor Trendy Attacks

IMPERVA®

And You Can Monitor Trendy Attacks

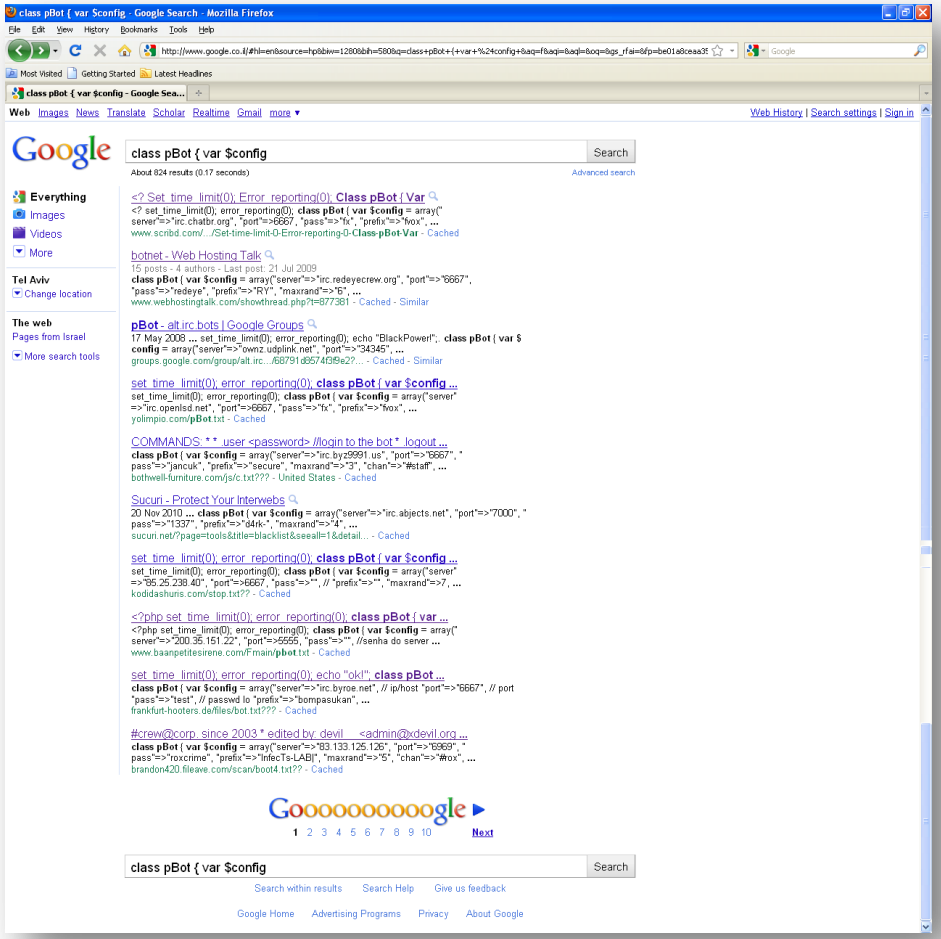
Approach #4:

Traffic Analysis Via Honeypots

IMPERVA®

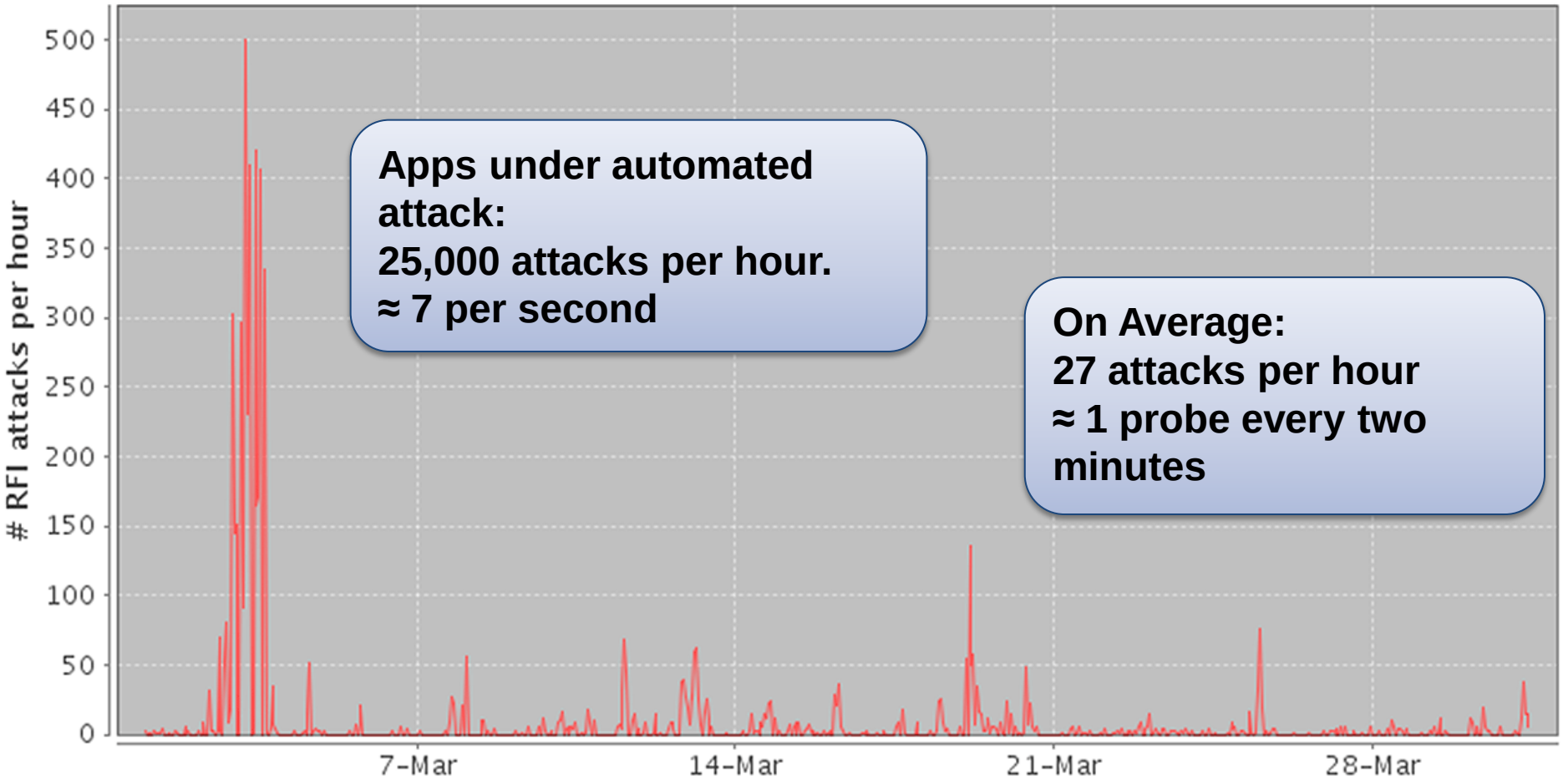
Automated Attacks

- Botnets
- Mass SQL Injection attacks
- Google dorks



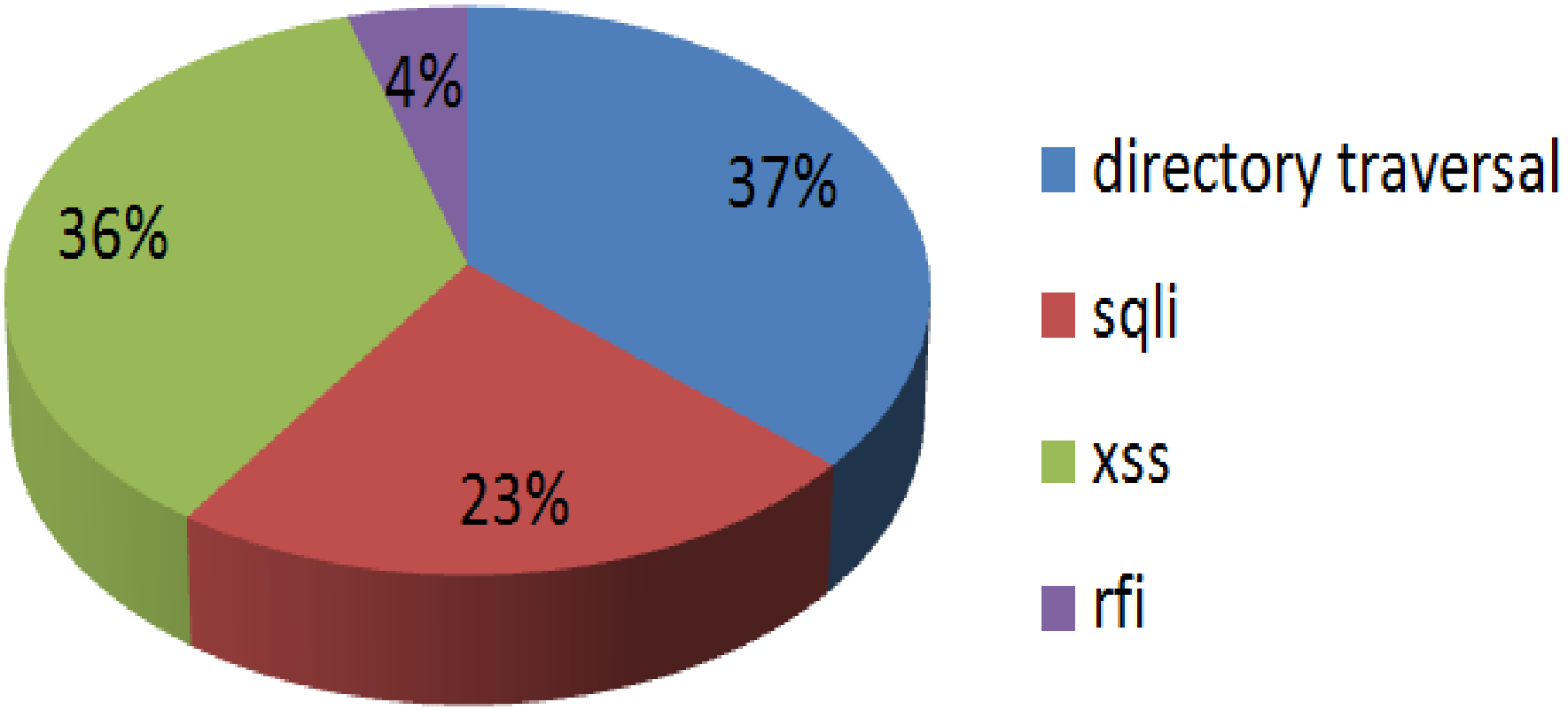
IMPERVA®

Finding#1: Automation is Prevailing



IMPERVA®

The Unfab Four



IMPERVA®

Finding #2: Reputation Matters

29 percent of the attack events originated from the 10 most active attack sources

IMPERVA®

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 ≈ 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.

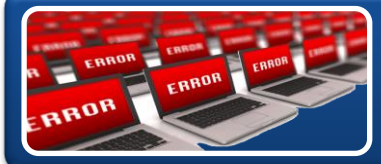
Conclusions

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.

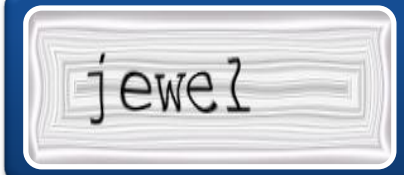
Introduce reputation-based controls.

IMPERVA®

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

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

Client-side computational challenges

- Slow on the client, quick on the server

Disinformation

- Bogus links
- Hidden Links

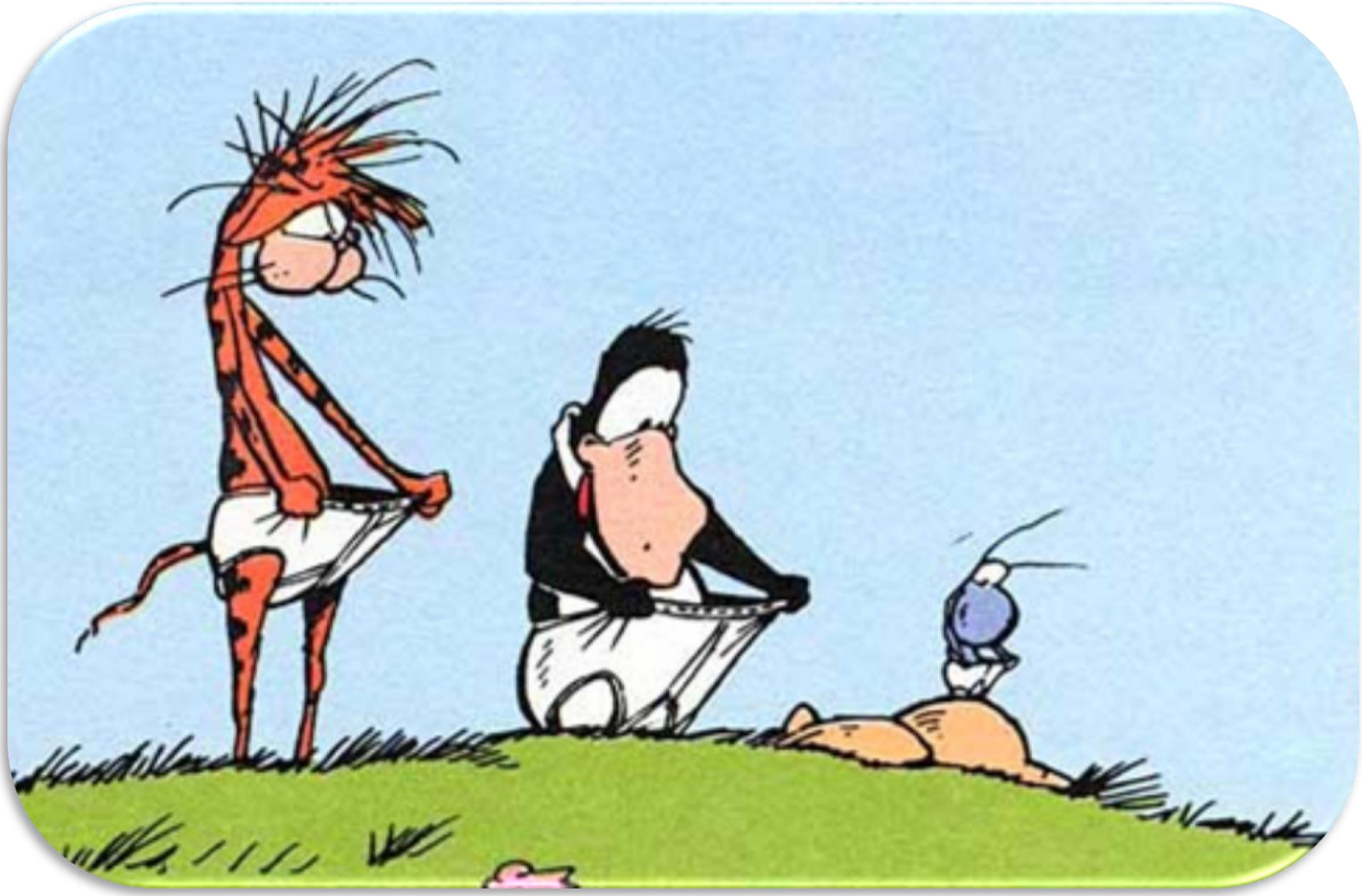
IMPERVA®

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

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 Dtails

- ✓ If you want slides, send: your credit card number, mother's maiden name and an email to:

rob.rachwald@imperva.com

Thank You