Hacking 2011: Lessons for 2012/ 黑客攻击事件2011:2012年的解决方案

Noa Bar-Yosef
Sr. Security Strategist
Imperva

OWASP

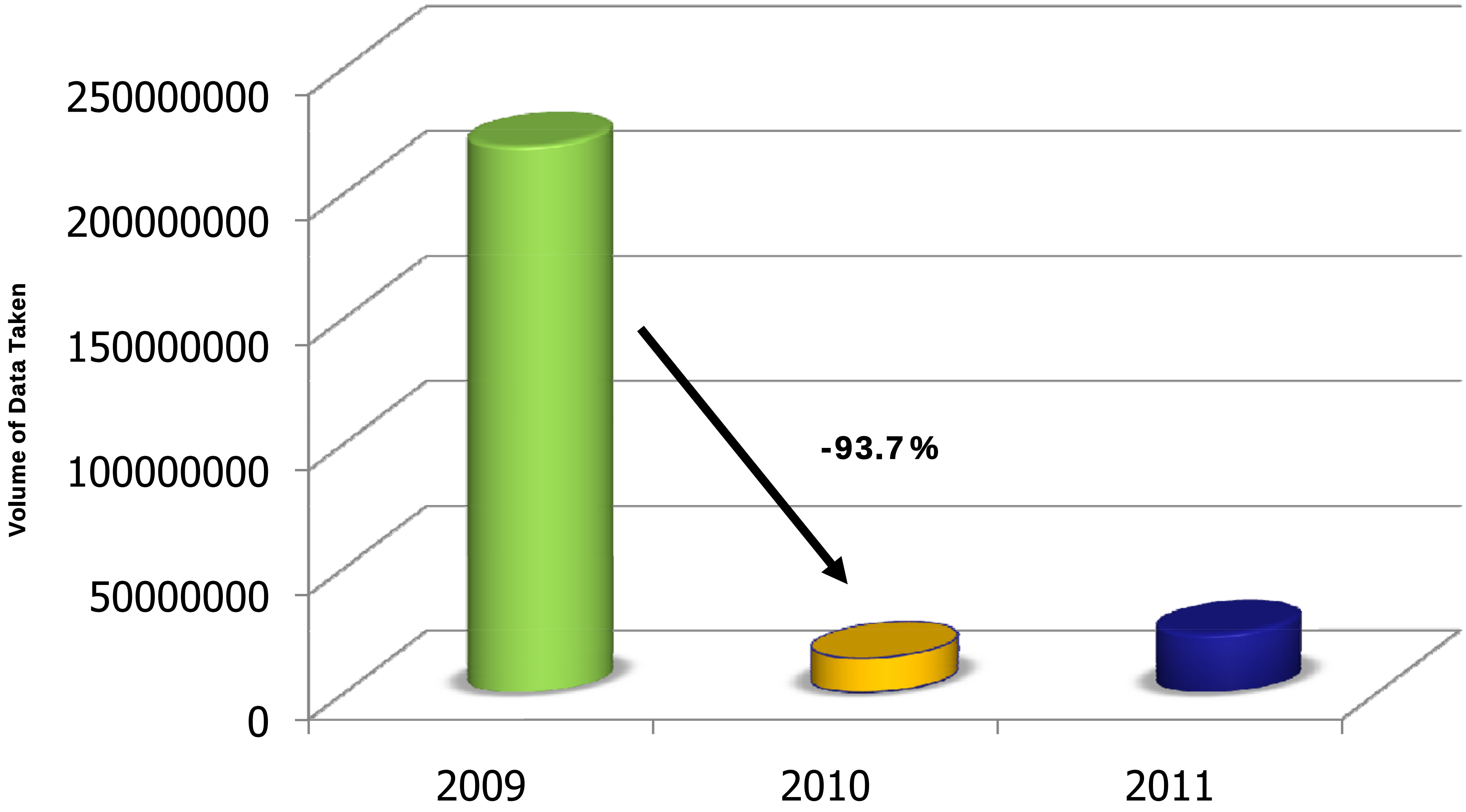
The OWASP Foundation
http://www.owasp.org

Agenda

- A statistical lookback of breaches: 2009-2011
  - 回望2009-2011年攻击事件统计
- Cybercrime 2011: reality checks
  - 2011网络犯罪:现实调查
- Top 5 data breaches of 2011
  - 2011年前5个攻击
- Security lessons from 2011
  - 2011年的安全教训

LOOKING BACK/回望

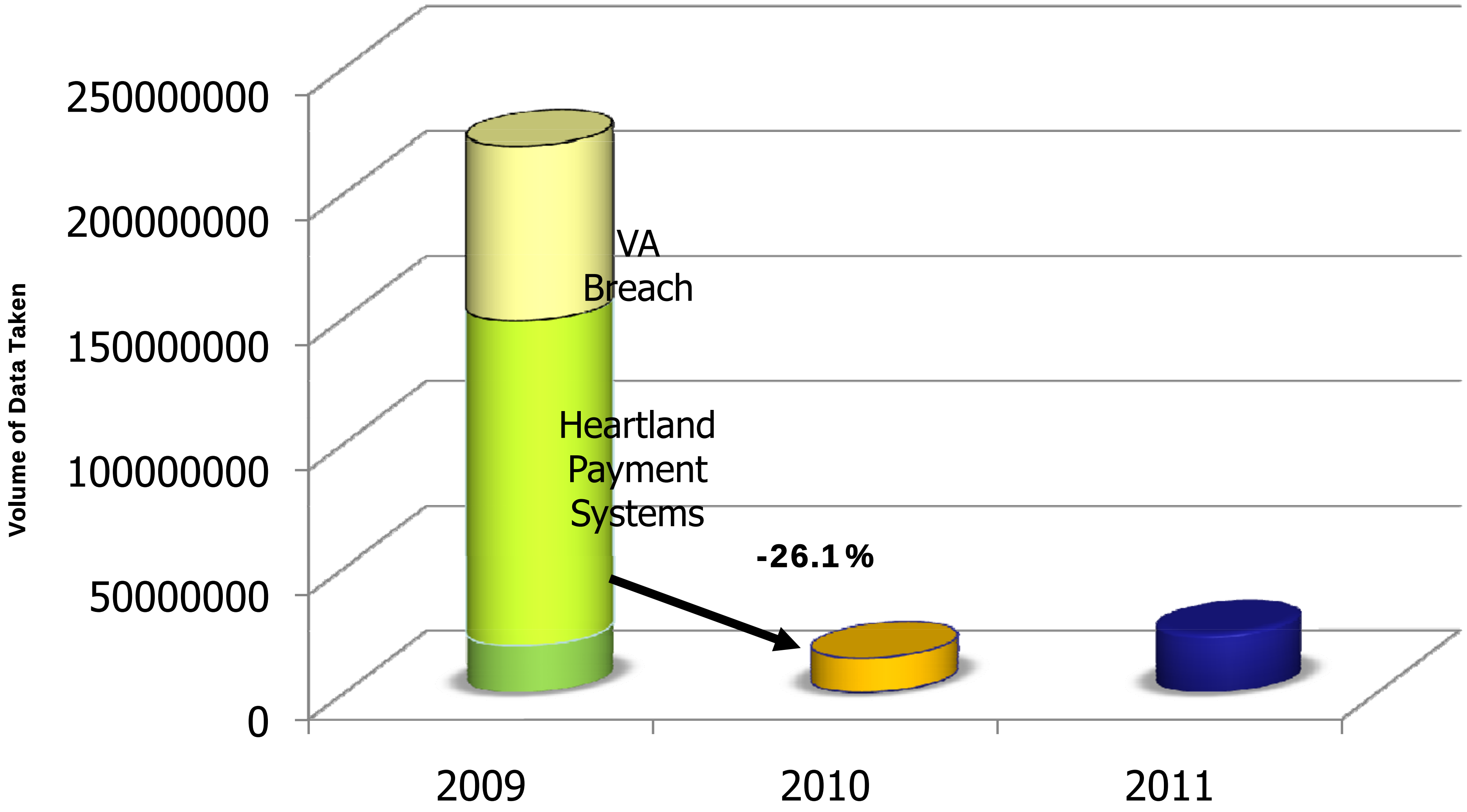
Data Breach Volume /数据泄漏量



Source: http://www.privacyrights.org/data-breach

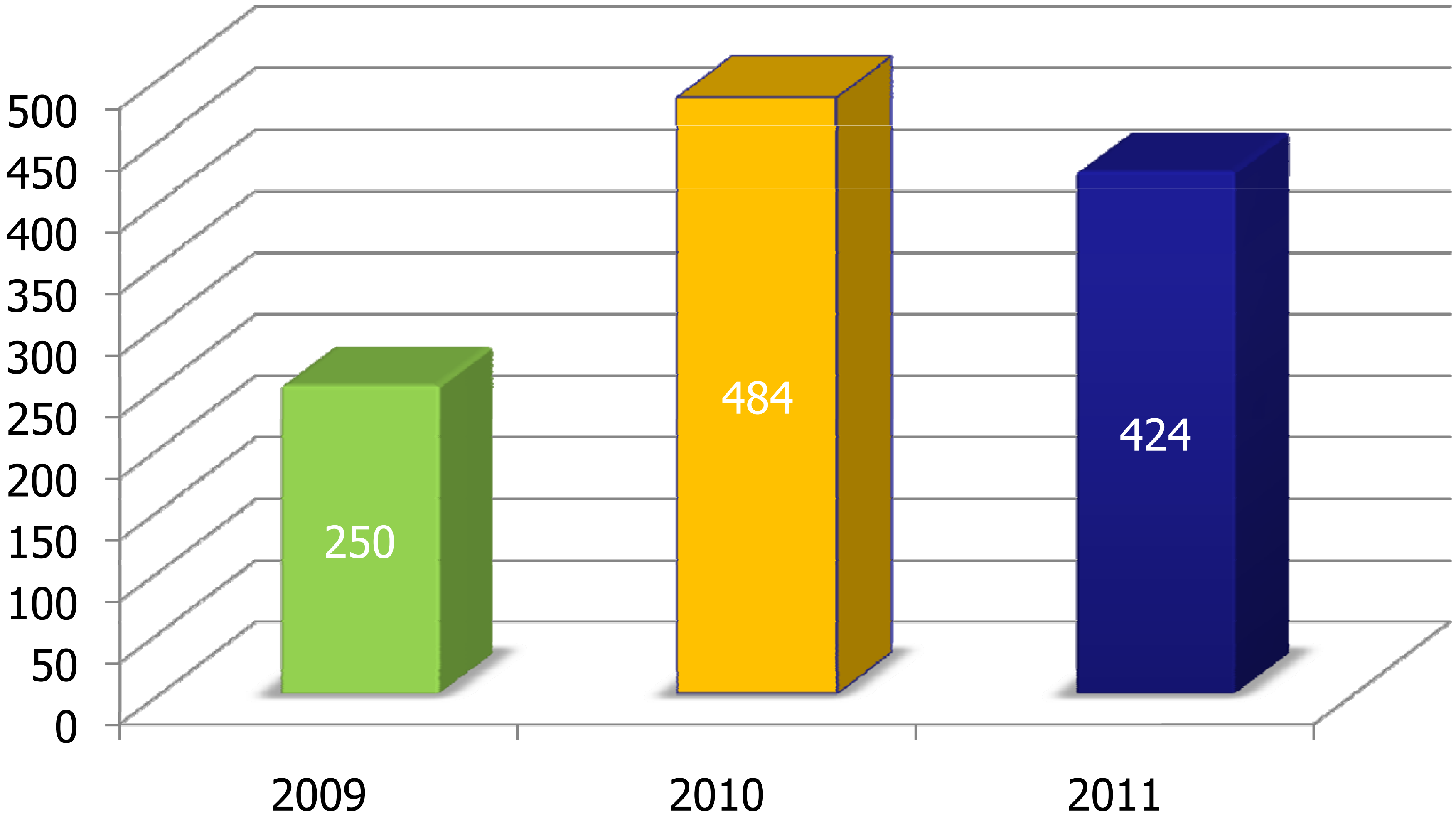
OWASP

Data Breach Volume /数据泄漏量

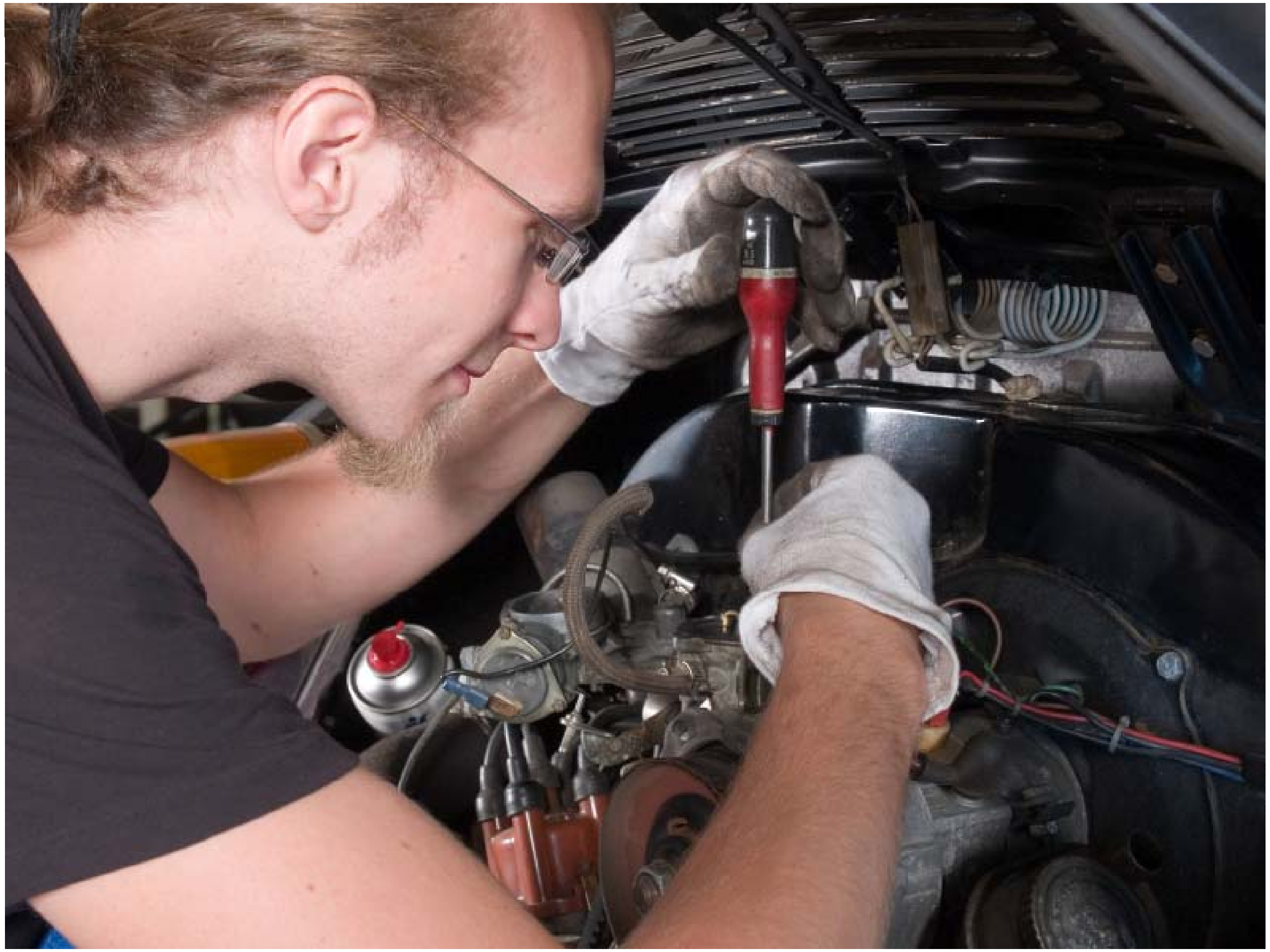


Source: http://www.privacyrights.org/data-breach

Data Breach Incidents/资料外泄事件

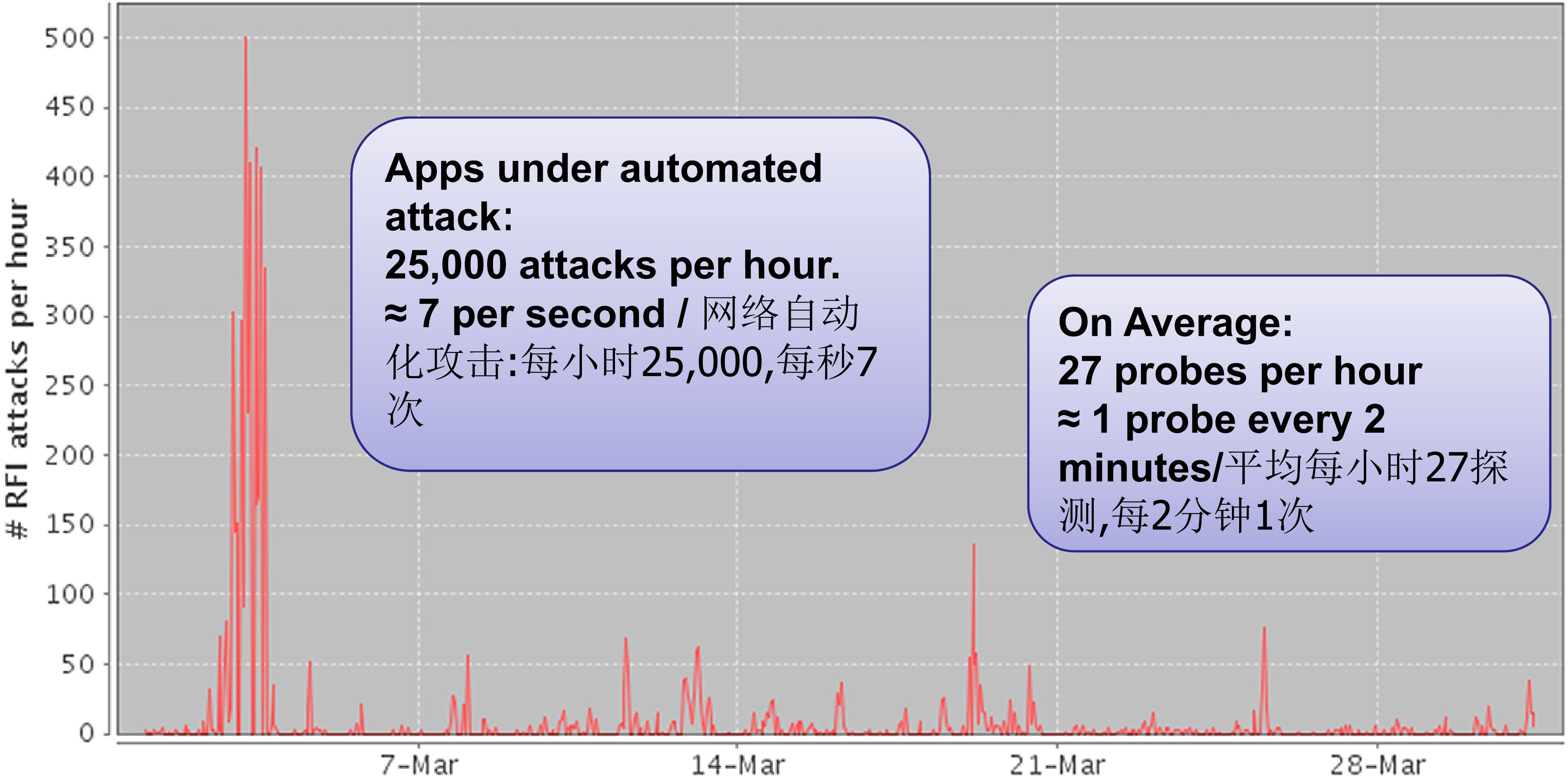


Source: http://www.privacyrights.org/data-breach



Reality Checks/现实调查

Reality Check#1: Automation is Prevailing/ 调查#1:自动化攻击流行

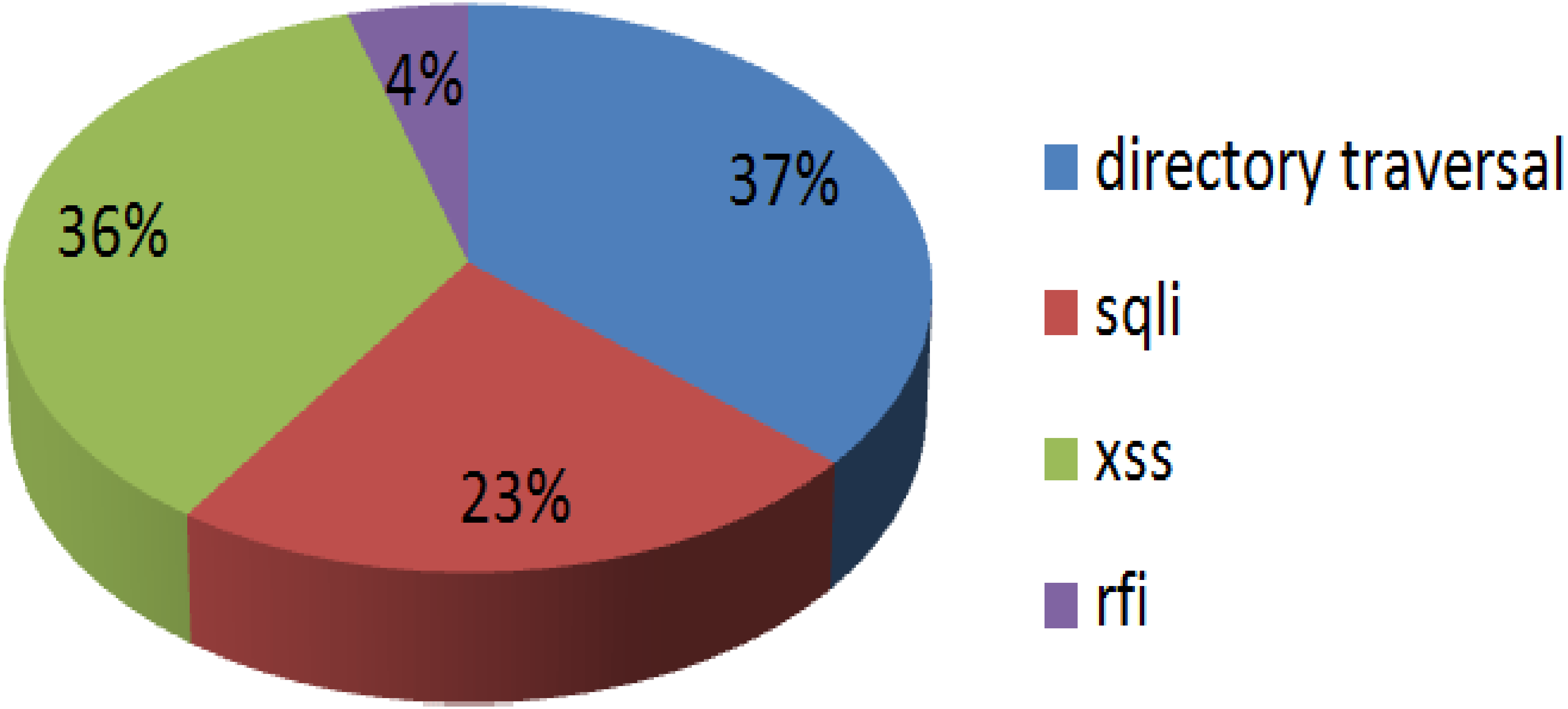


Apps under automated attack:
25,000 attacks per hour.
≈ 7 per second / 网络自动化攻击:每小时25,000,每秒7次

On Average:
27 probes per hour
≈ 1 probe every 2 minutes/平均每小时27探测,每2分钟1次

Source: Imperva's Web Application Attack Report – July 2011

Reality Check#2: The Unfab Four / 调查#2:前4种类型的攻击



Source: Imperva's Web Application Attack Report – July 2011

Reality Check #3: Repeat Offenders/调查#3: 重复的攻击

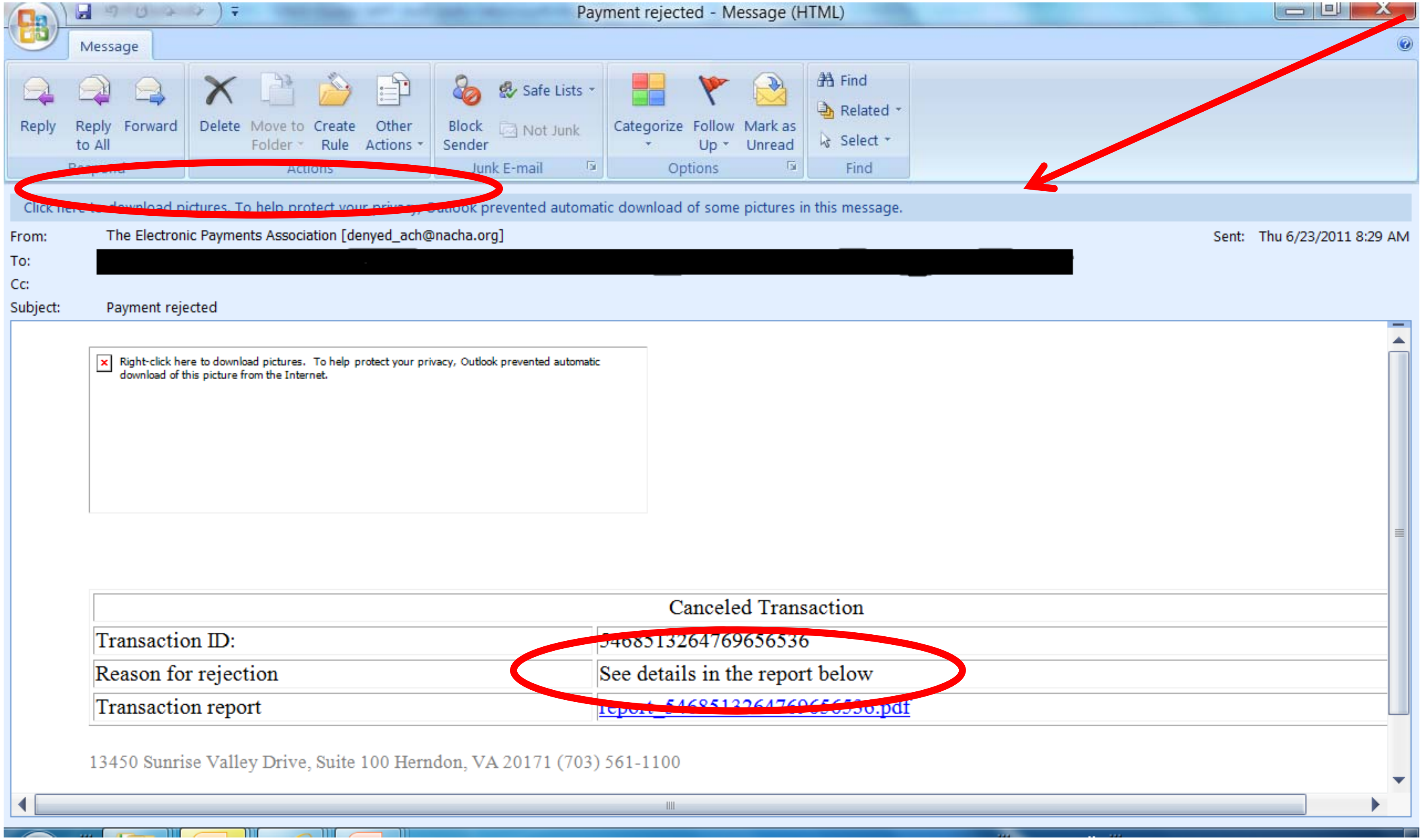
The average number of attacks a single host initiated:

- RFI: 10
- SQL Injection: 40
- Directory Traversal: 25

29% of attack events originated from just 10 sources.

Reality Check#4: Redefine Internal Threat/ 调查#4:内部威胁

- Have you ever received one of these?/你曾经收到了这吗？



Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: The Electronic Payments Association [denyed_ach@nacha.org]

Sent: Thu 6/23/2011 8:29 AM

To: [redacted]

Cc:

Subject: Payment rejected

Right-click here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.

	Canceled Transaction
Transaction ID:	5468513264769656536
Reason for rejection	See details in the report below
Transaction report	report_5468513264769656536.pdf

13450 Sunrise Valley Drive, Suite 100 Herndon, VA 20171 (703) 561-1100

5

RSA

The Details/信息

- Breach Size: Data related to SecureID tokens/数据被窃取的程度: SecureID令牌相关的数据
- Date: March 2011/日期: 2011年3月
- Source:/来源: http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/
- Why Significant?/为什么会显著？
  - Targeted criminal hacking/有针对性的犯罪黑客
  - External threat goes inside the corporation/外部威胁进入公司内
    - Enhanced by the Consumerization of IT/增强IT消费

4

8Million Compromised Websites/800万被攻破的网站

The Details /信息

- Breach Size: 8Million websites serve malware/攻击程度: 800万网站被植入恶意软件
- Date: August 2011/日期: 2011年8月
- Source:/来源:

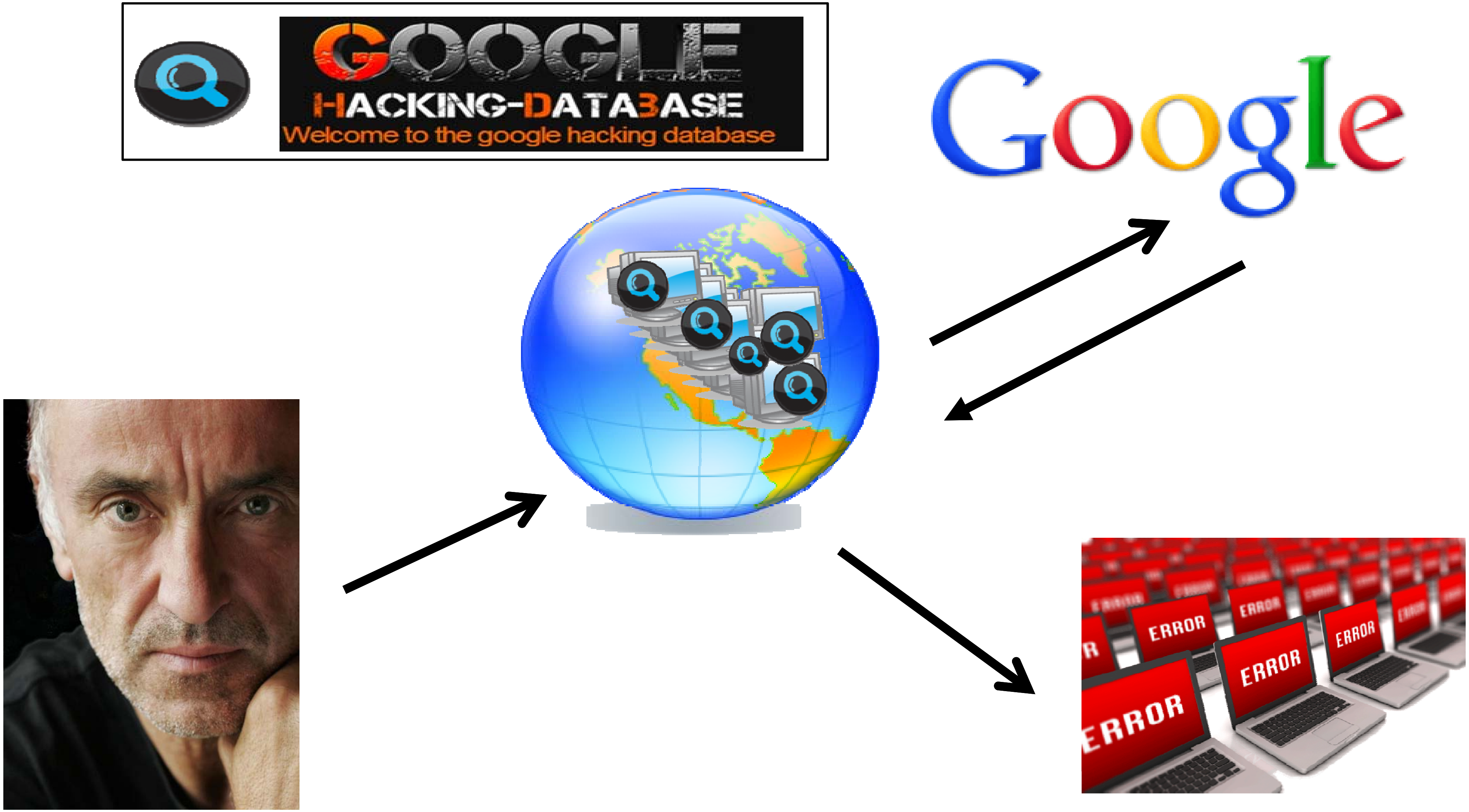
  http://www.usatoday.com/money/industries/technology/2011-08-11-mass-website-hacking_n.htm
- Why Significant? /为什么会显著？
  - The power of automation/自动化的力量
  - Google Dorks/谷歌Dorks

Zooming into Google Dorks (1) / 分析谷歌 Dorks (1)

80,000/

Google
Google Search
I'm Feeling Lucky
Advanced search
Language tools
Advertising Programs
Business Solutions
About Google
Privacy

Zooming into Google Dorks (2) / 分析谷歌 Dorks (2)



3

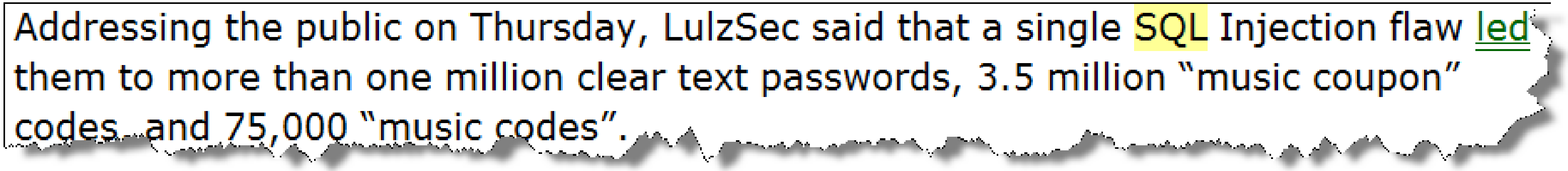
LulzSec’s 50-days of Hacking/LulzSec’s 50天的黑客

The Details /信息

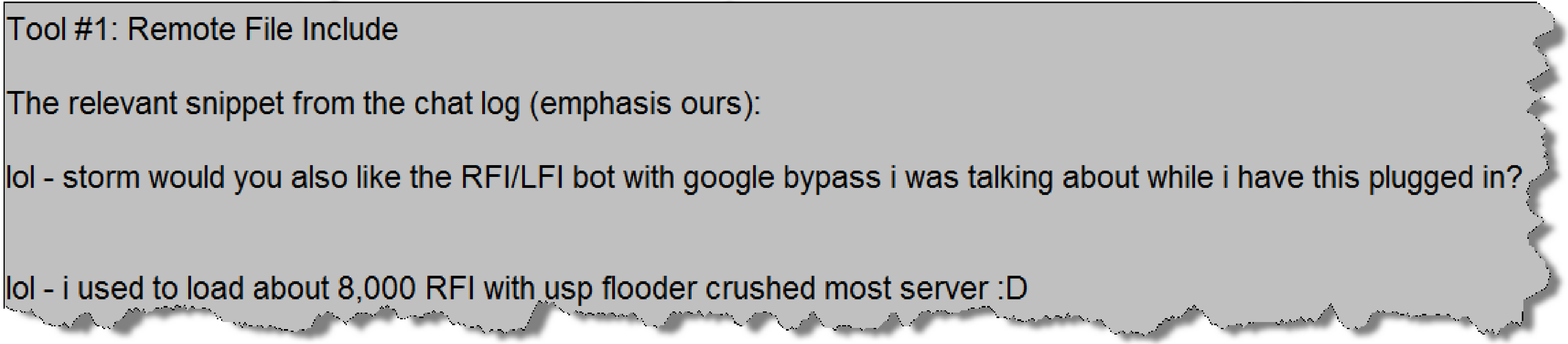
- Breach Size: X-Factor, Fox.com, Sony Music + Pictures, PBS.org, Infragard, Arizona Dept. of Public Safety… /破坏程度:
- Date: May-June 2011/日期: 2011年5月- 6月
- Source:/来源:

  http://www.reuters.com/article/2011/06/22/us-cybersecurity-lulzsec-timeline-idUSTRE75L4NC20110622
- Why Significant? /为什么会显著?
  - What do hackers hack?/黑客寻找什么?

LulzSec Activity Samples/LulzSec活动实例



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".



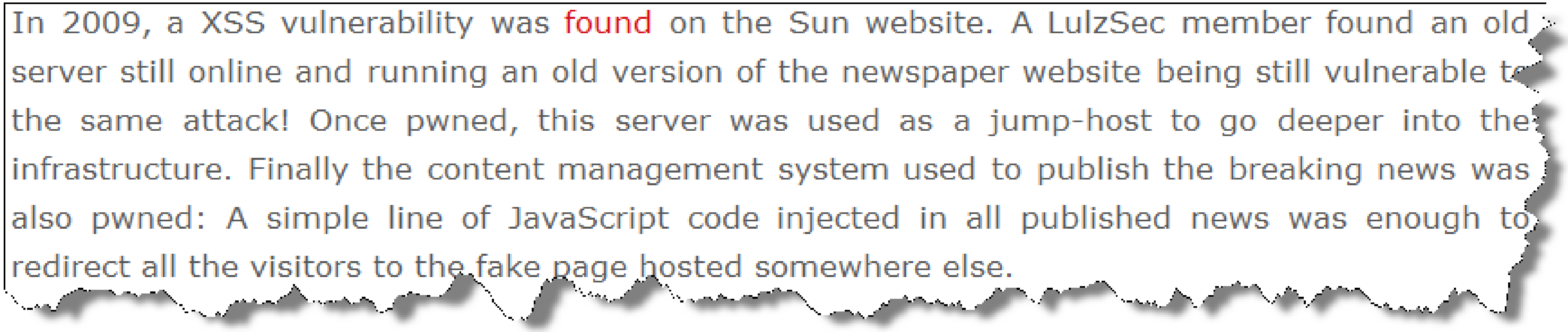
Tool #1: Remote File Include

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.

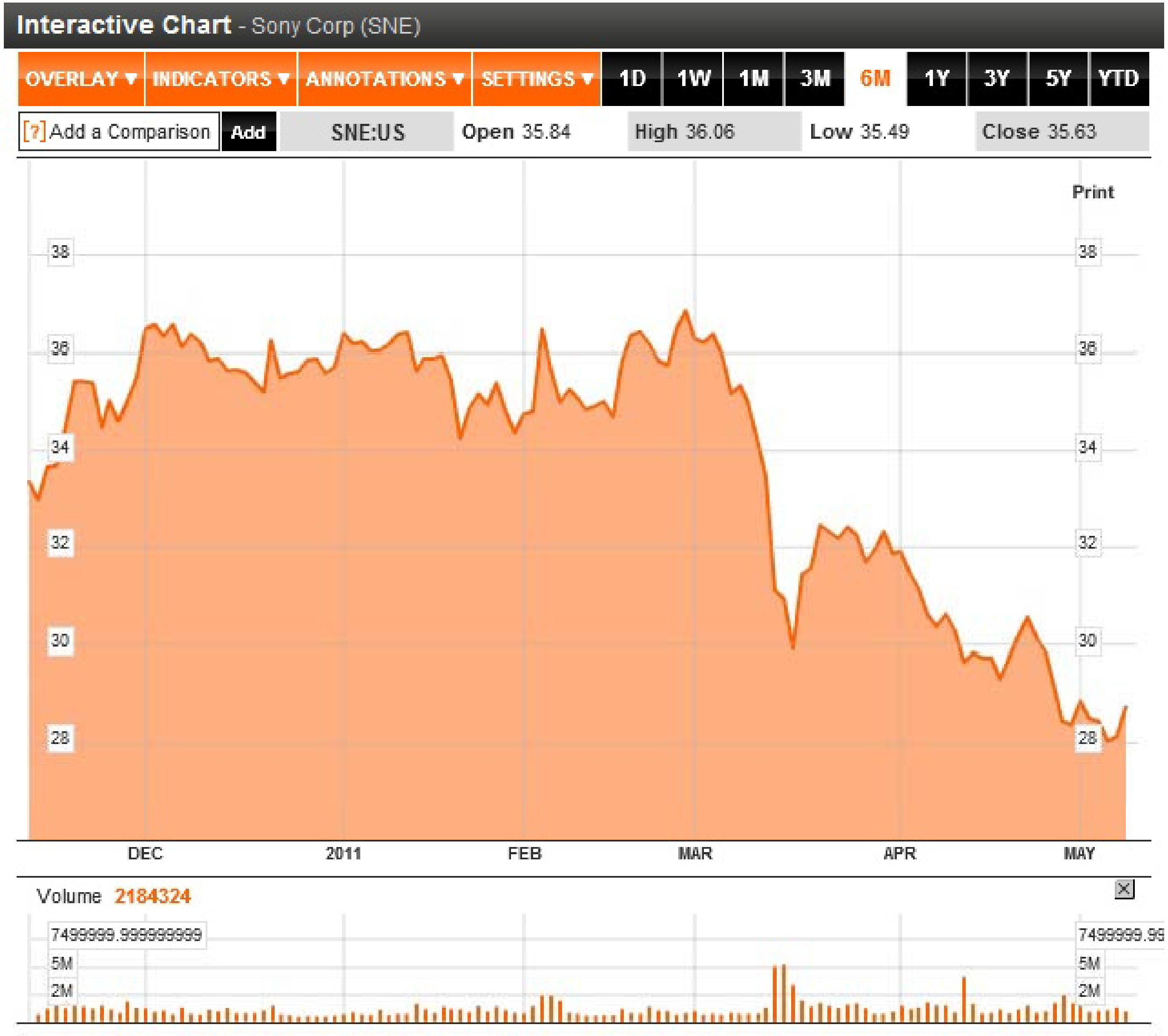
2

Sony/索尼

The Details /信息

- Size: 77M credit cards (12M unencrypted) /影响程度: 7700万信用卡 (1200万未加密)
- Date: April 2011/日期：2011年4月
- Source: /来源: http://blog.us.playstation.com/2011/05/05/a-letter-from-howard-stringer/
- Why Significant? /为什么会显著？
  - Made security a business problem, not just a set of technologies./安全是业务问题，不只是一套技术。
    - Data governance just as important as financial reporting or brand management/数据治理跟财务报告或品牌管理一样重要
    - Put the role of a CISO in proper perspective: You should have one/首席信息安全官的角色放置在正确的角度

Need To Justify The Cost of Security? / 需要证明安全的代价吗?



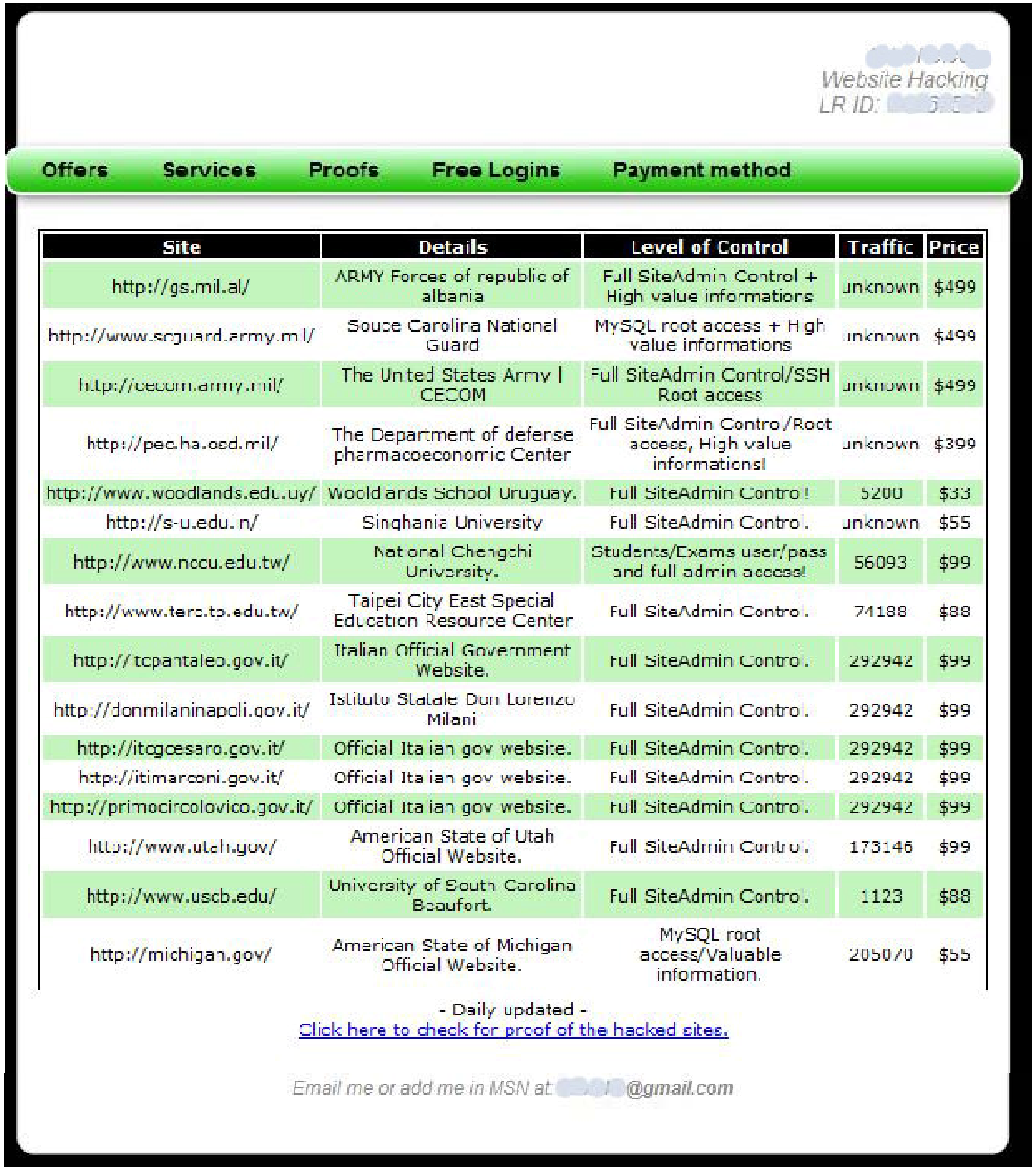
Interactive Chart - Sony Corp (SNE)

SNE:US Open 35.84 High 36.06 Low 35.49 Close 35.63

Volume 2184324

1

Government Websites for Sale/出售政府网站



[redacted]
Website Hacking
LR ID: [redacted]

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/	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://tcpantaleo.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 -

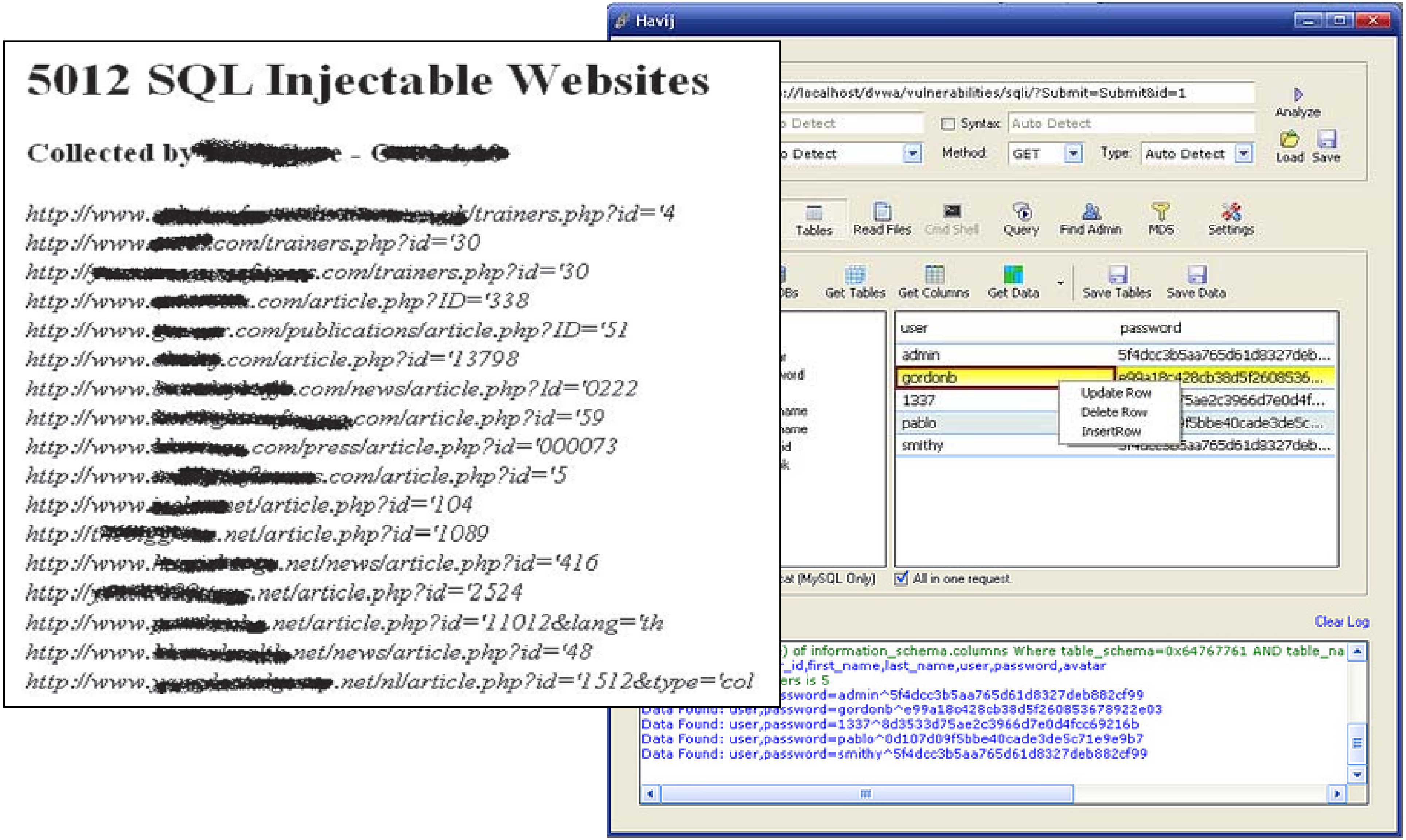
Click here to check for proof of the hacked sites.

Email me or add me in MSN at [redacted]@gmail.com

The Details/信息

- Size: Dozens of websites for sale /严重程度:数十家网站出售
- Date: January 2011/日期：2011年1月
- Source:/ 来源: http://krebsonsecurity.com/2011/01/ready-for-cyberwar/
- Why Significant? /为什么会显著？
  - The power of automation/自动化的力量
  - SQL Injection gives birth to a business/SQL注入促使一项业务的诞生

The Power of Automation / 自动化的力量



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]et/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

:://localhost/dvwa/vulnerabilities/sqli/?Submit=Submit&id=1

o Detect
□ Syntax: Auto Detect
o Detect
Method: GET
Type: Auto Detect

user	password
admin	5f4dcc3b5aa765d61d8327deb...
gordonb	e99a18c428cb38d5f2608536...
1337	5ae2c3966d7e0d4f...
pablo	9f5bbe40cade3de5c...
smithy	5aa765d61d8327deb...

cat (MySQL Only)   ☑ All in one request.

```
) of information_schema.columns Where table_schema=0x64767761 AND table_na
_id,first_name,last_name,user,password,avatar
ers is 5
ssword=admin^5f4dcc3b5aa765d61d8327deb882cf99
Data Found: user,password=gordonb^e99a18c428cb38d5f260853678922e03
Data Found: user,password=1337^8d3533d75ae2c3966d7e0d4fcc69216b
Data Found: user,password=pablo^0d107d09f5bbe40cade3de5c71e9e9b7
Data Found: user,password=smithy^5f4dcc3b5aa765d61d8327deb882cf99
```

SUMMARY / 总结

Incidents are inevitable but…/事故是不可避免的，但…

- Most attackers are going for the low hanging fruit/大多数攻击者寻找容易攻击的目标
- Most incidents are related to simple attack techniques/事故大多是简单的攻击技术
  - Mitigation techniques and solutions do exist for those and can be easily deployed/规避技术和解决方案确实存在，并可以轻松地部署
- Many attackers are repeat offenders/许多攻击者是累犯
  - A handful of perpetrators may be responsible for a multitude of attacks/少数肇事者可能对众多的攻击负责
- Enhance Web application defenses with reputation-based controls/加强与信誉为基础的控制Web应用程序防御

Incidents are inevitable but… …/事故是不可避免的，但…

- By deploying the proper solution an organization can ensure timely detection and mitigation for most attacks/通过部署适当的解决方案，组织可以确保及时发现，大多数攻击和解决它们
- When an incident is detected your best friend is the audit trail/当检测到可疑事件时你最好的朋友是审计追踪
  - Quickly identify the root cause/快速找出问题的根源
- Contain and scope the incident/划定事件的范围
  - Track down perpetrator/追查肇事者

Targeted Criminal Hacking/有针对性的刑事黑客

- Assume compromise/Assume compromise
  - Every decent sized organization must assume a certain amount of infected machines connected to its network/每一个适当规模的组织必须假设一定量的受感染的机器连接到其网络
- It is not about technology it is about human nature/是关于人性，不是科技
- Re-define internal threat/重新定义内部威胁
- It is no longer “malicious insider” but rather “infected insider”/它不再是"恶意的内部人员”，而是"受感染的内部人员”
  - More control is required around data sources/围绕数据源需要更多的控制
- Identify abusive access patterns using legitimate privileges/使用合法的特权来确定滥用的访问模式

QUESTIONS? / 问题?

THANK YOU! / 谢谢!