RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

Don’t Bring A Knife To A Gun Fight: The Hacker Intelligence Initiative

Speaker：Noa Bar-Yosef

Job Title: Sr. Security Strategist

Company Name: Imperva

Agenda

- The state of application security
- Studying hackers
  - Why? Prioritizing defenses
  - How? Methodology
- Analyzing real-life attack traffic
  - Key findings
- Technical Recommendations

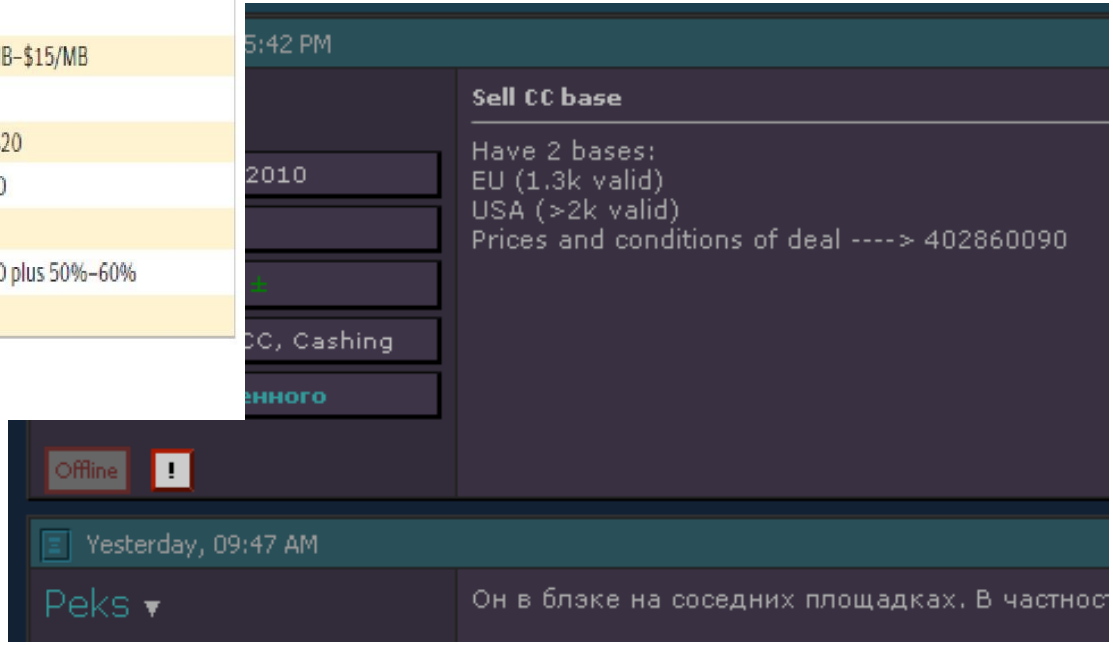
Why Data Security?

DATA IS HACKER CURRENCY

The Underground Markets

Overall Rank 2009	Overall Rank 2008	Item	Percentage 2009	Percentage 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/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
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 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Table 5. Goods and services advertised on underground economy servers
Source: Symantec



Website Access Up for Sale

Website Hacking
LR ID: [redacted]

Offers | Services | Proofs | Free Logins | Payment method

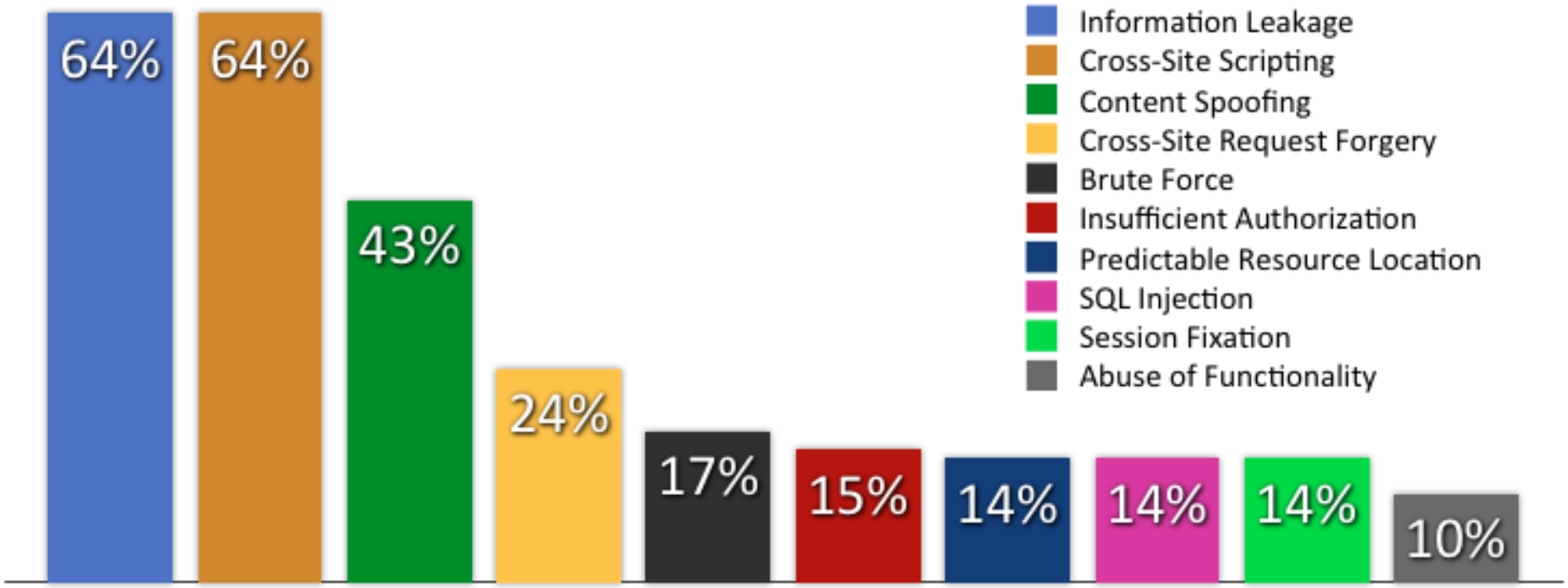
Site	Details	Level of Control	Traffic	Price
http://gs.mil.al/	ARMY Forces of republic of albania	Full SiteAdmin Control + High value informations	unknown	$499
http://www.scguard.army.mil/	Souce Carolina National Guard	MySQL root access + High value informations	unknown	$499
http://cecom.army.mil/	The United States Army | CECOM	Full SiteAdmin Control/SSH Root access	unknown	$499
http://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 [redacted]@gmail.com

THE CURRENT STATE OF WEB APPLICATION SECURITY

WhiteHat Security Top 10 - 2010



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

Situation Today

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

X

# of vulnerabilities : 230

1%

821,771,600

vulnerabilities in active circulation

Situation Today

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

X

of

But which will be exploited?

821,771,600

vulnerabilities in active circulation

Studying Hackers

- Focus on actual threats
  - 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
- Devise new defenses based on real data
  - Reduce guess work

Understanding the Threat Landscape - Methodology

1. Tap into hacker forums

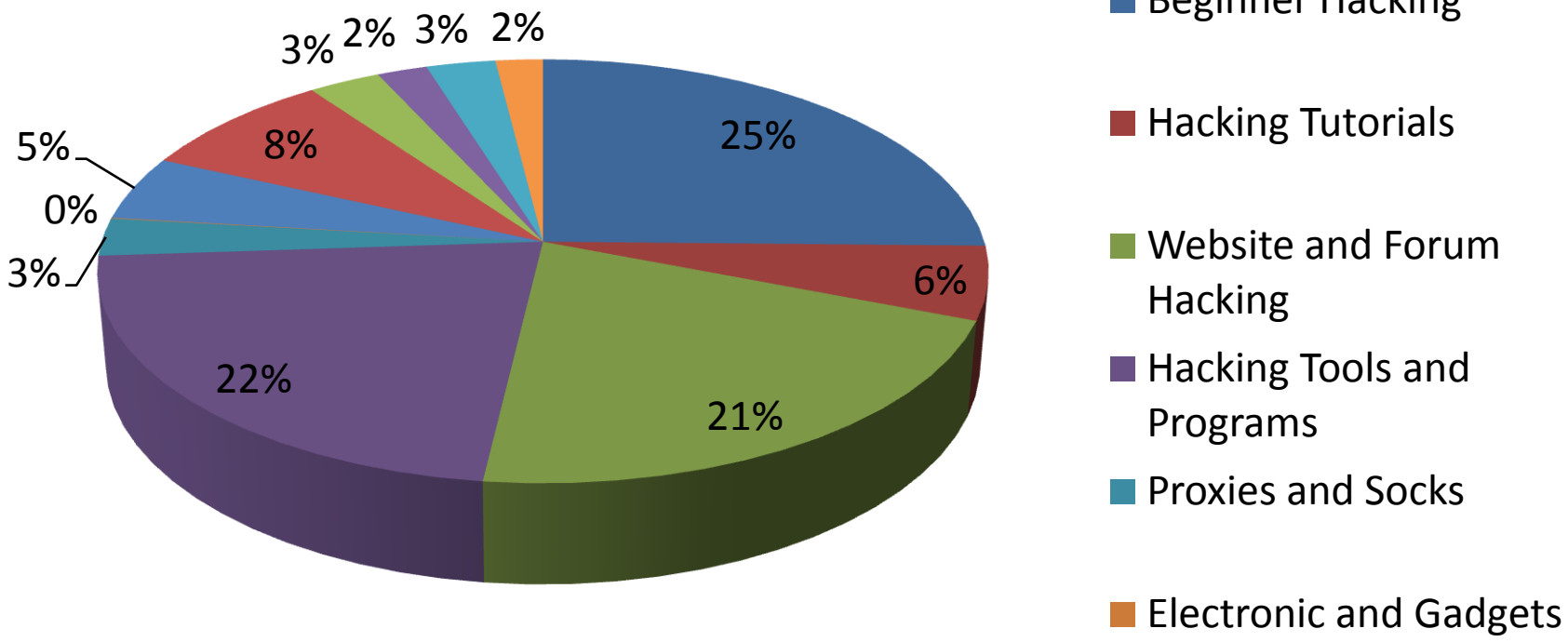
2. Analyze hacker tools and activity

3. Record and monitor hacker activity

What are Hackers Hacking?

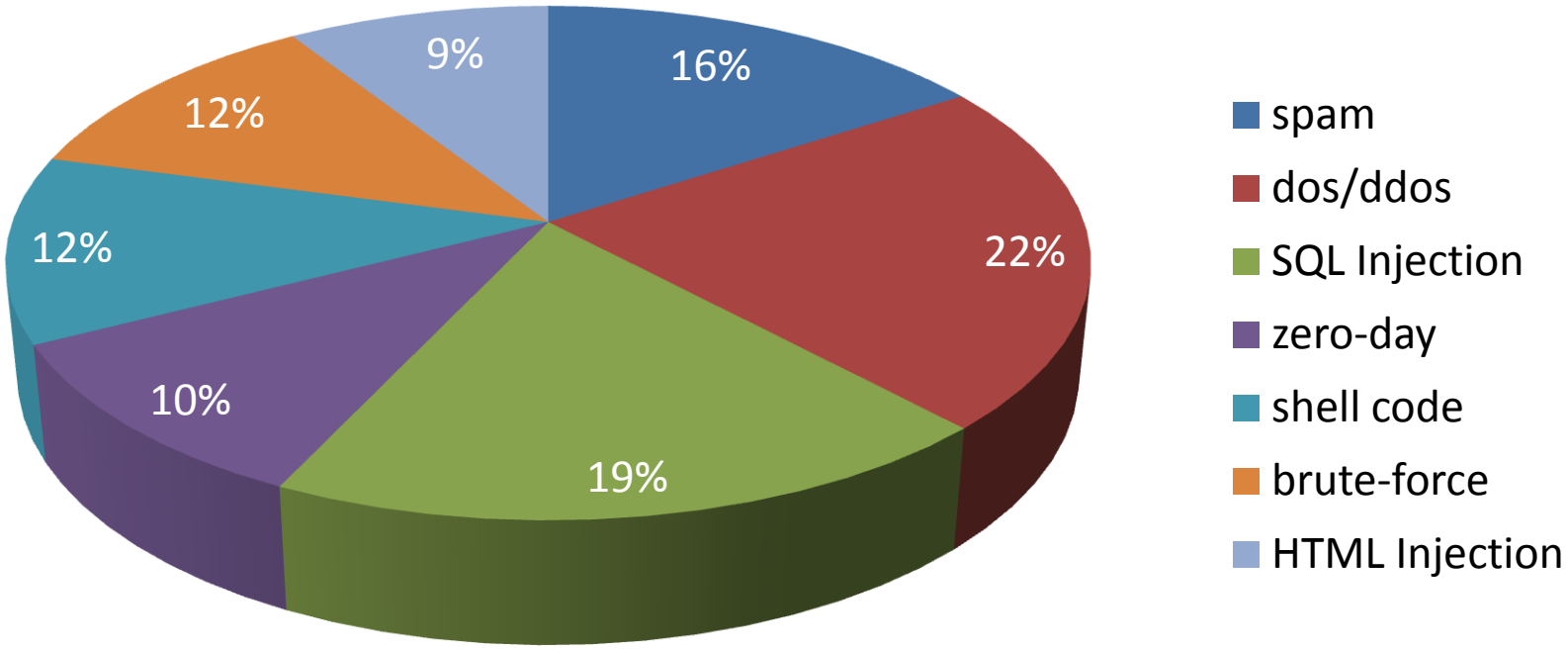
PART I: HACKER FORUMS

General Topics



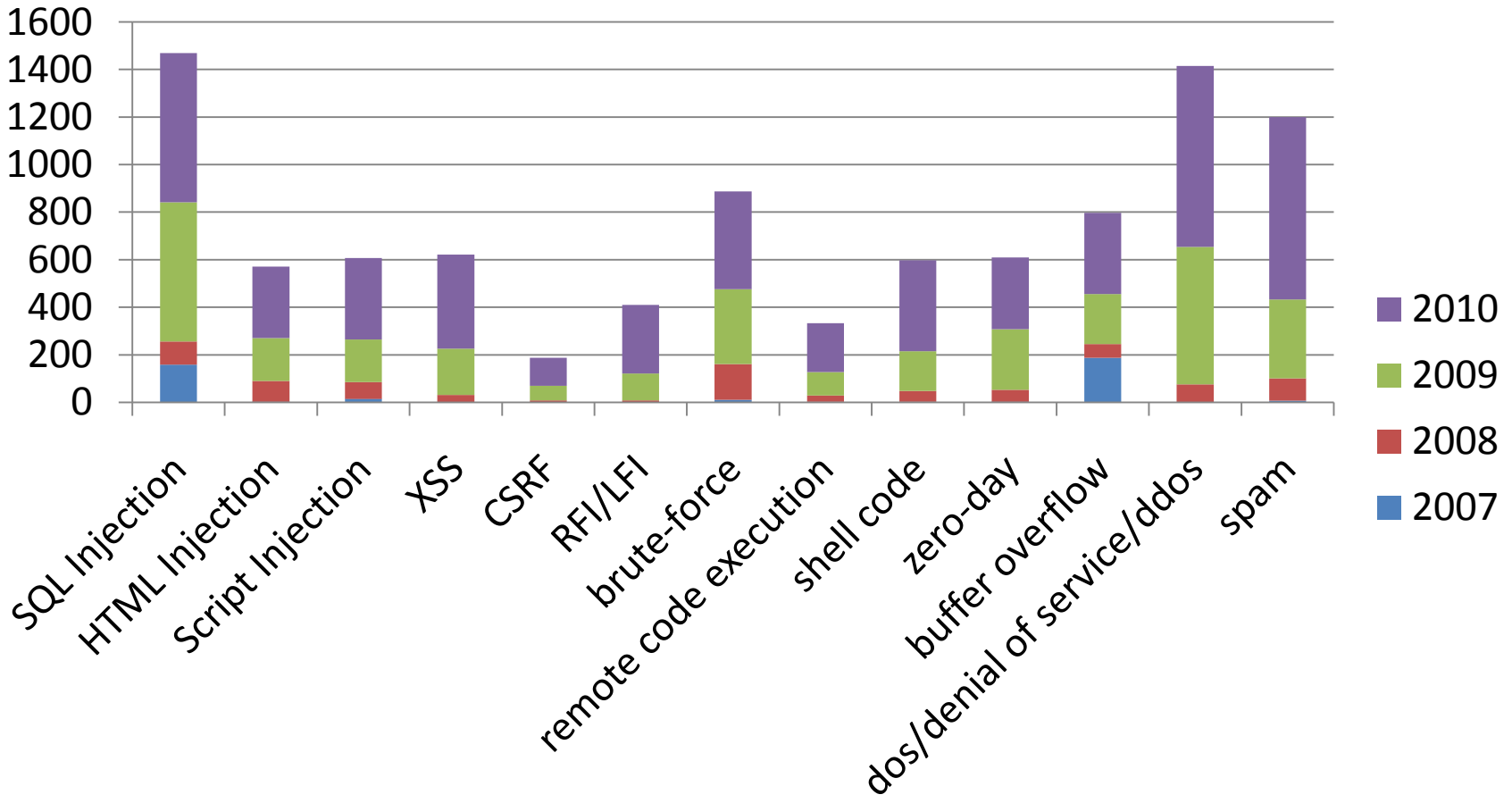
Dates: 2007- 2011

Top 7 Attack Techniques



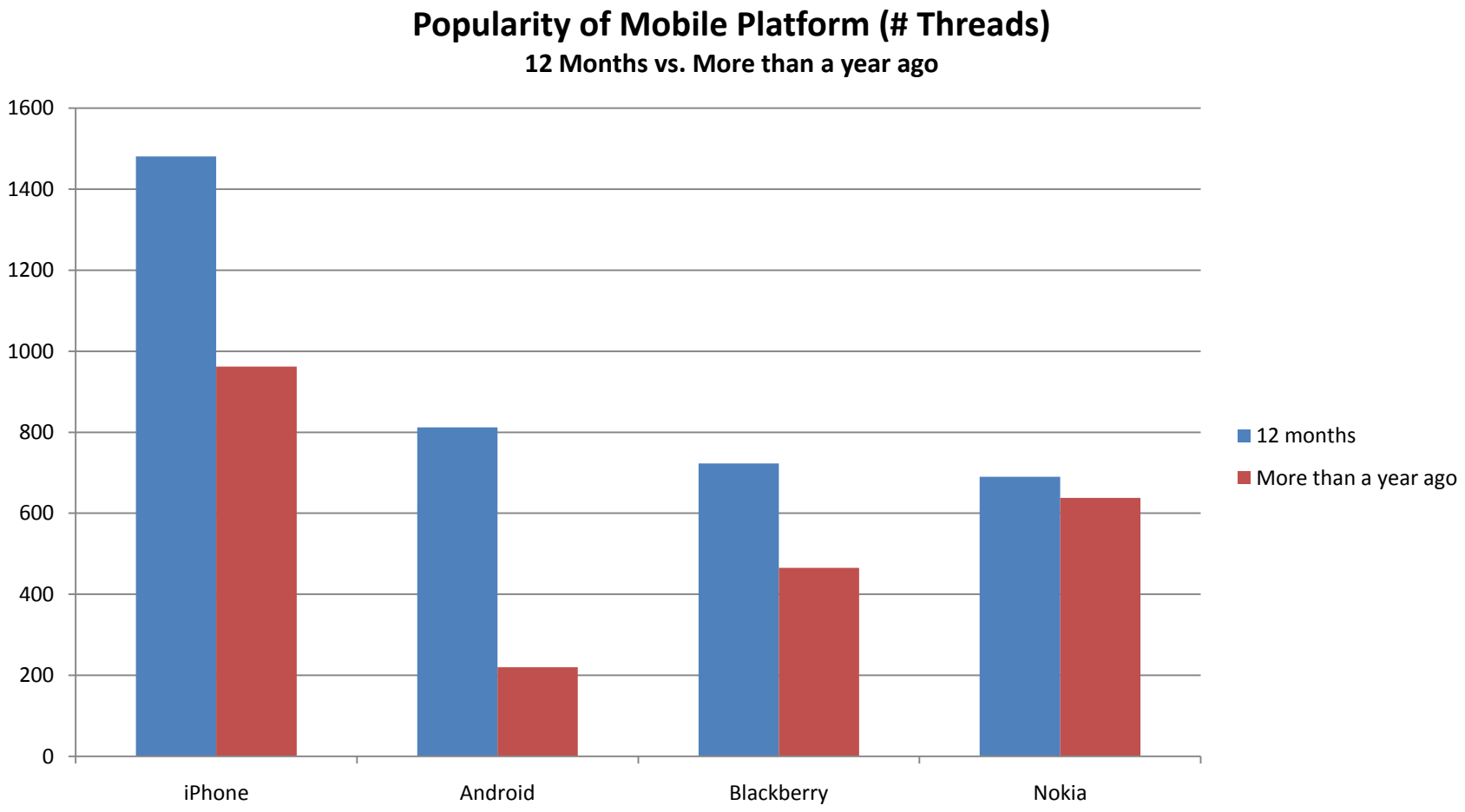
Dates: July 2010 -July 2011

Growth of Discussion Topics by Year



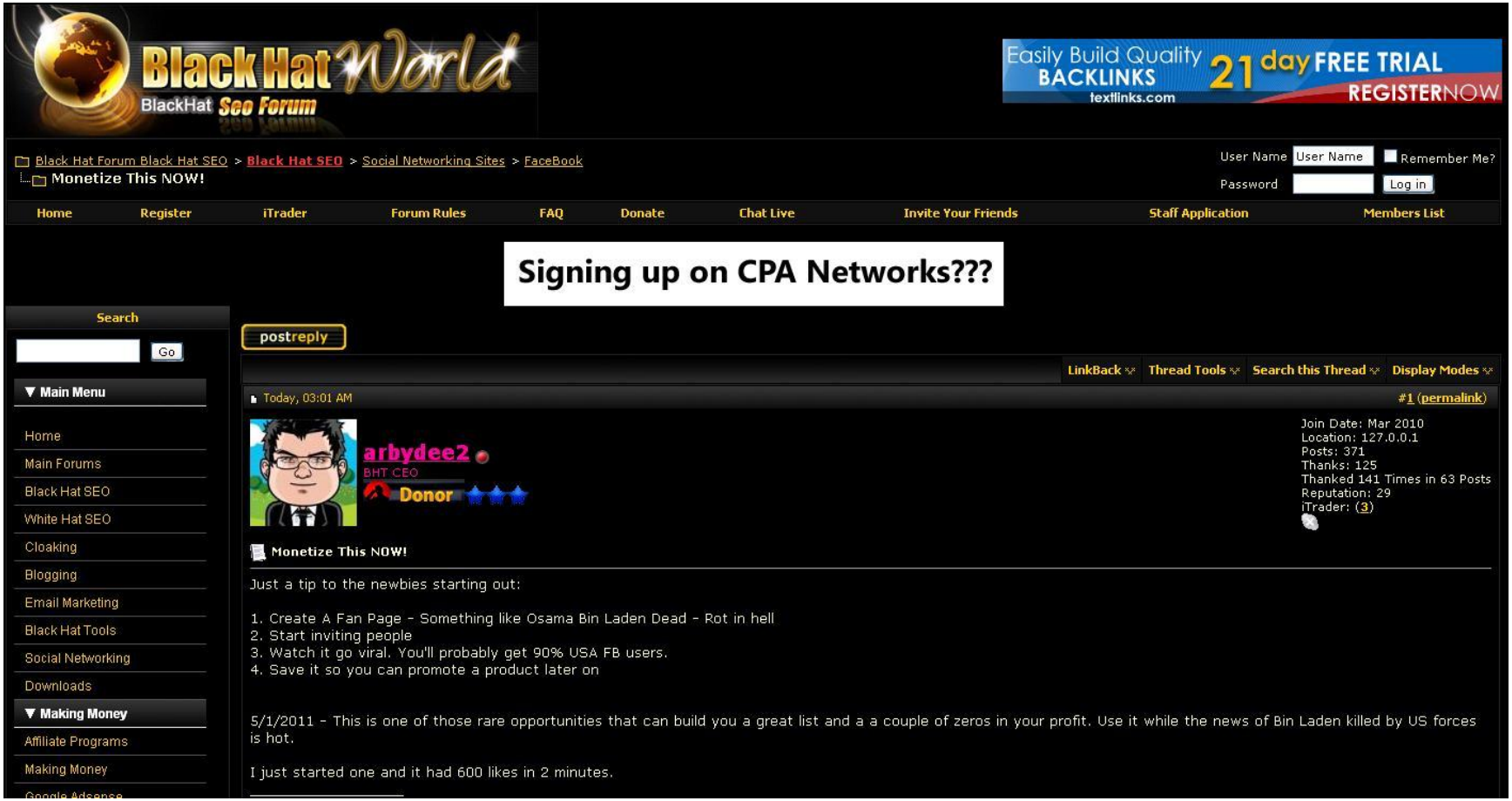
Dates: 2007- July 2010

Mobile (in)Security



Dates: July 2010-July 2011

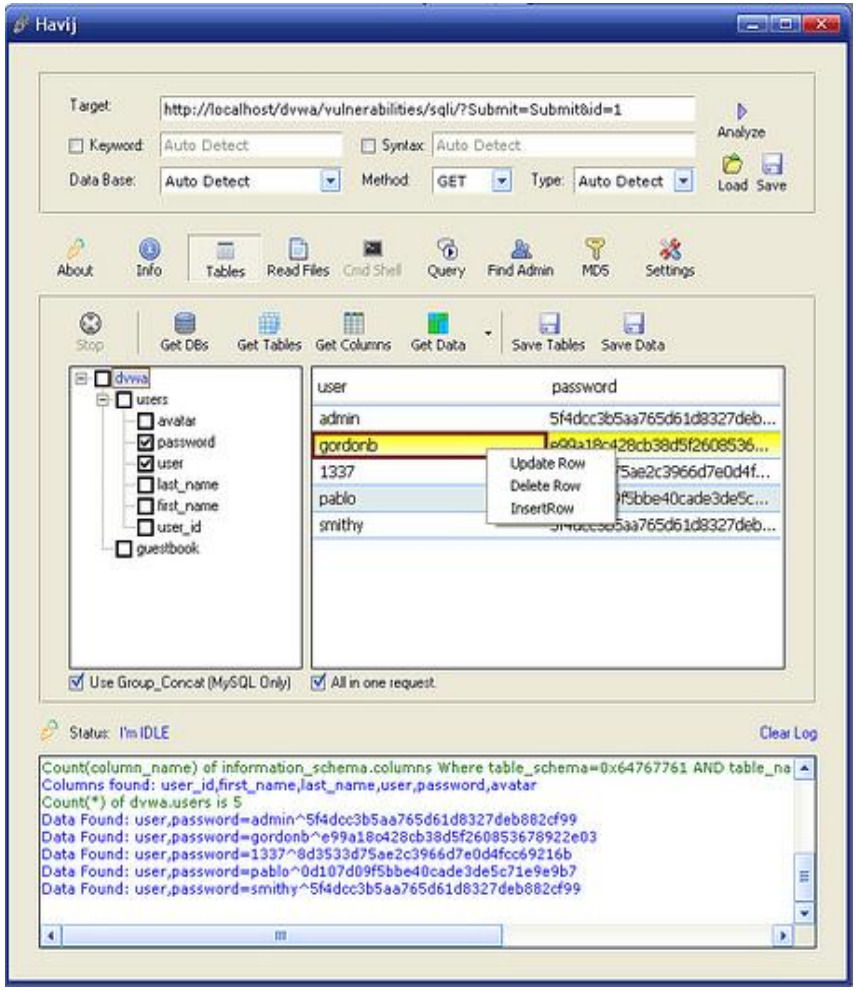
Qualitative Analysis



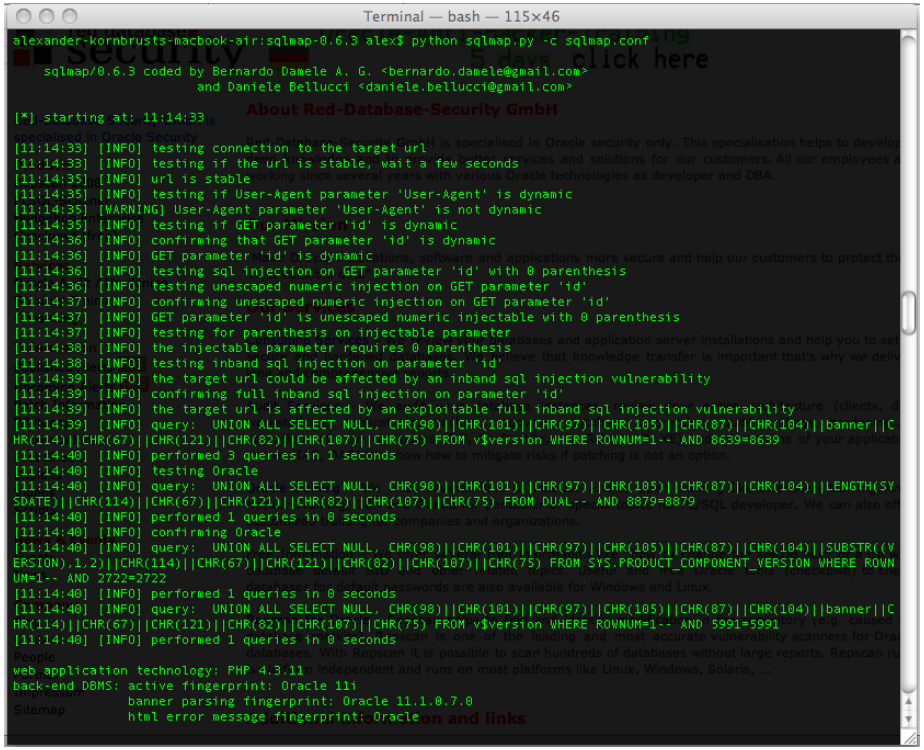
What are Hackers Hacking?

PART II: ATTACK TECHNOLOGIES

Example: SQL Injection Attack Tools

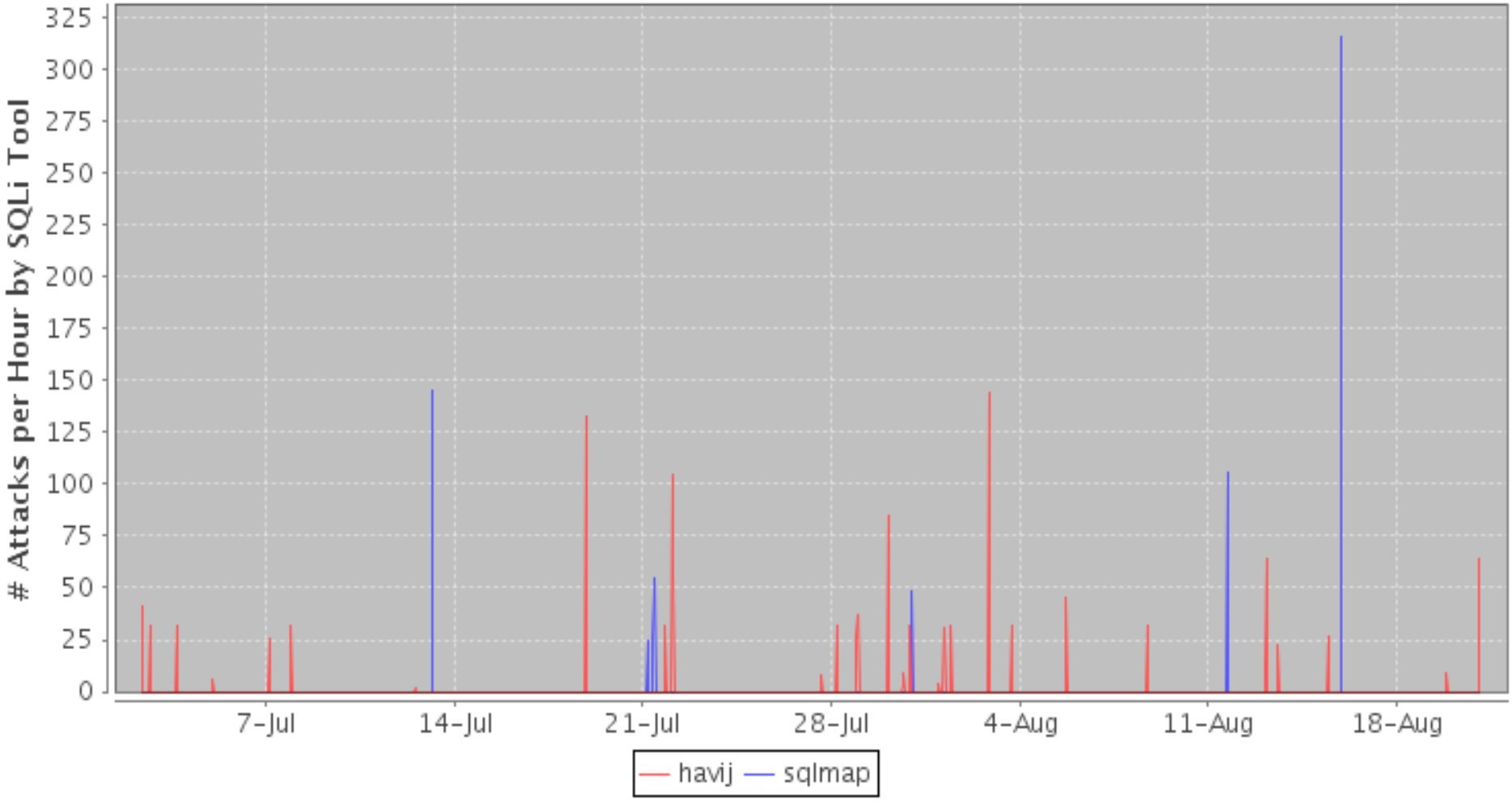


Havij

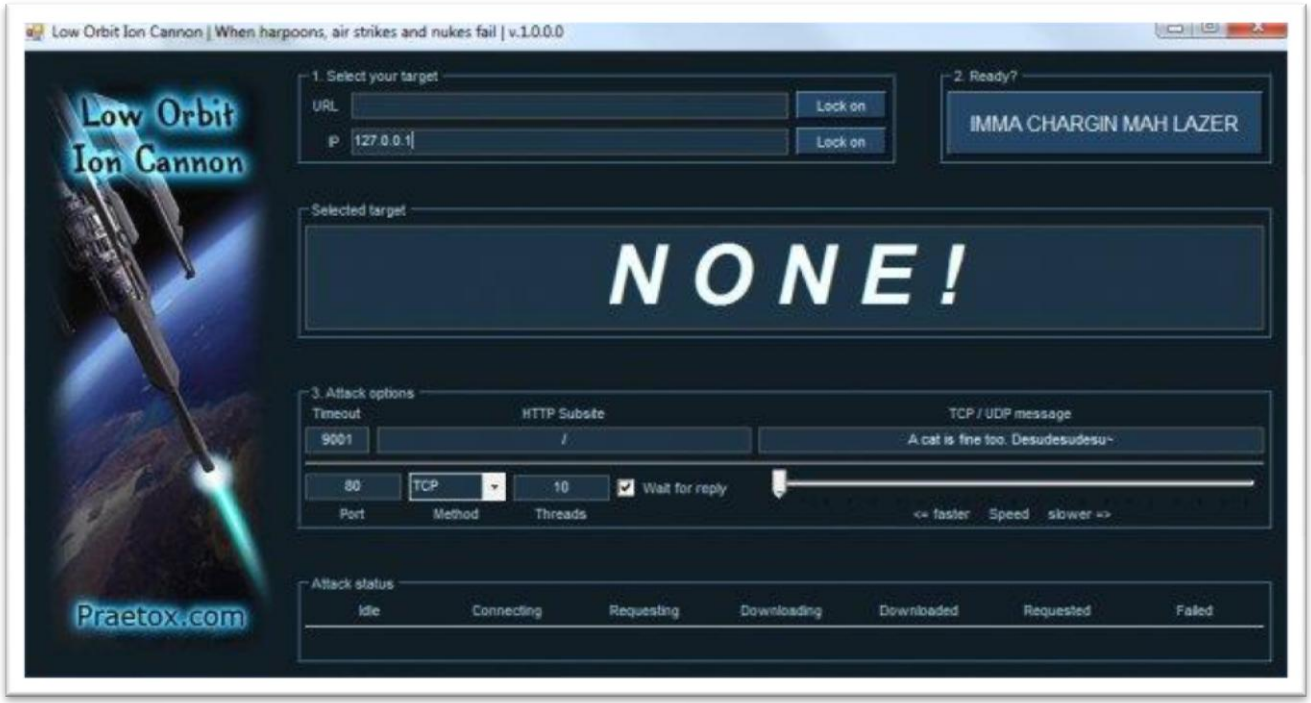


SQLMap

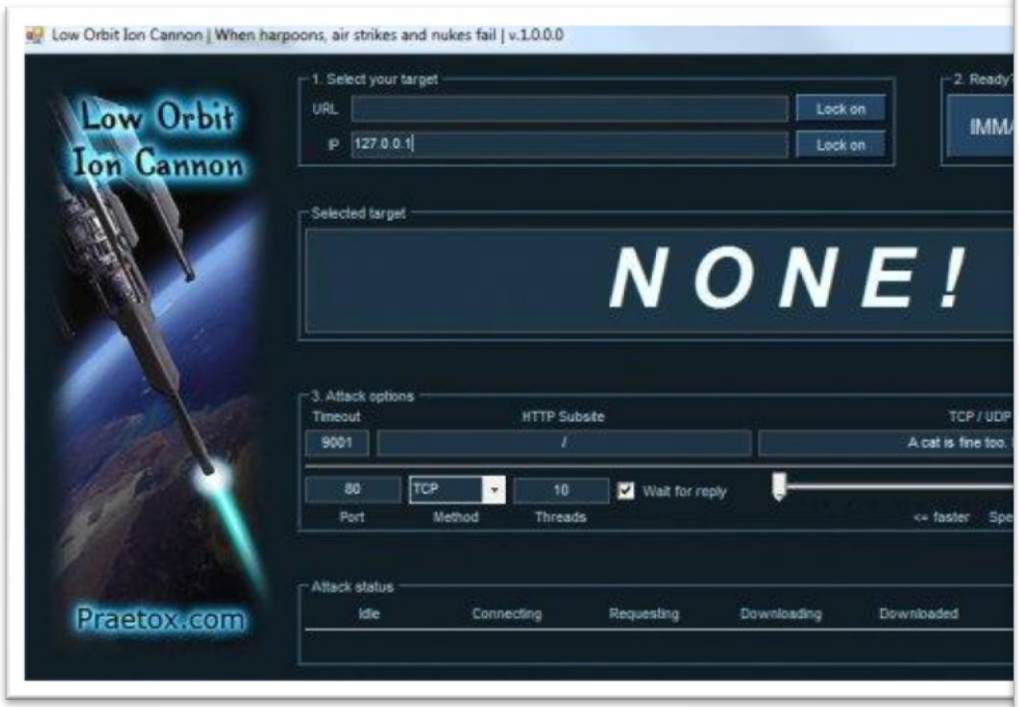
Attacks from Automated Tools

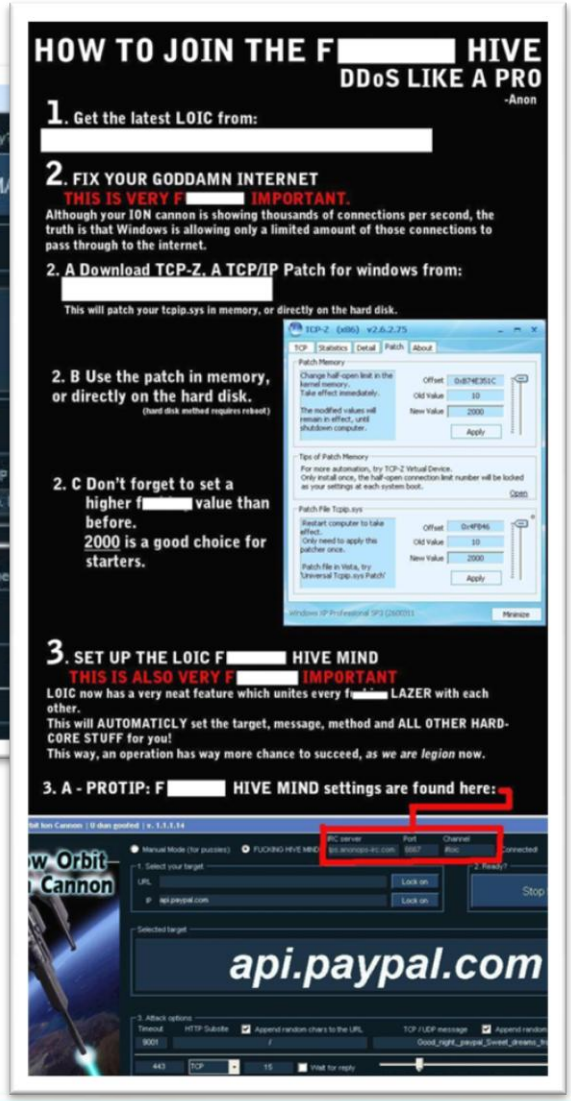


Low Orbit Ion Cannon

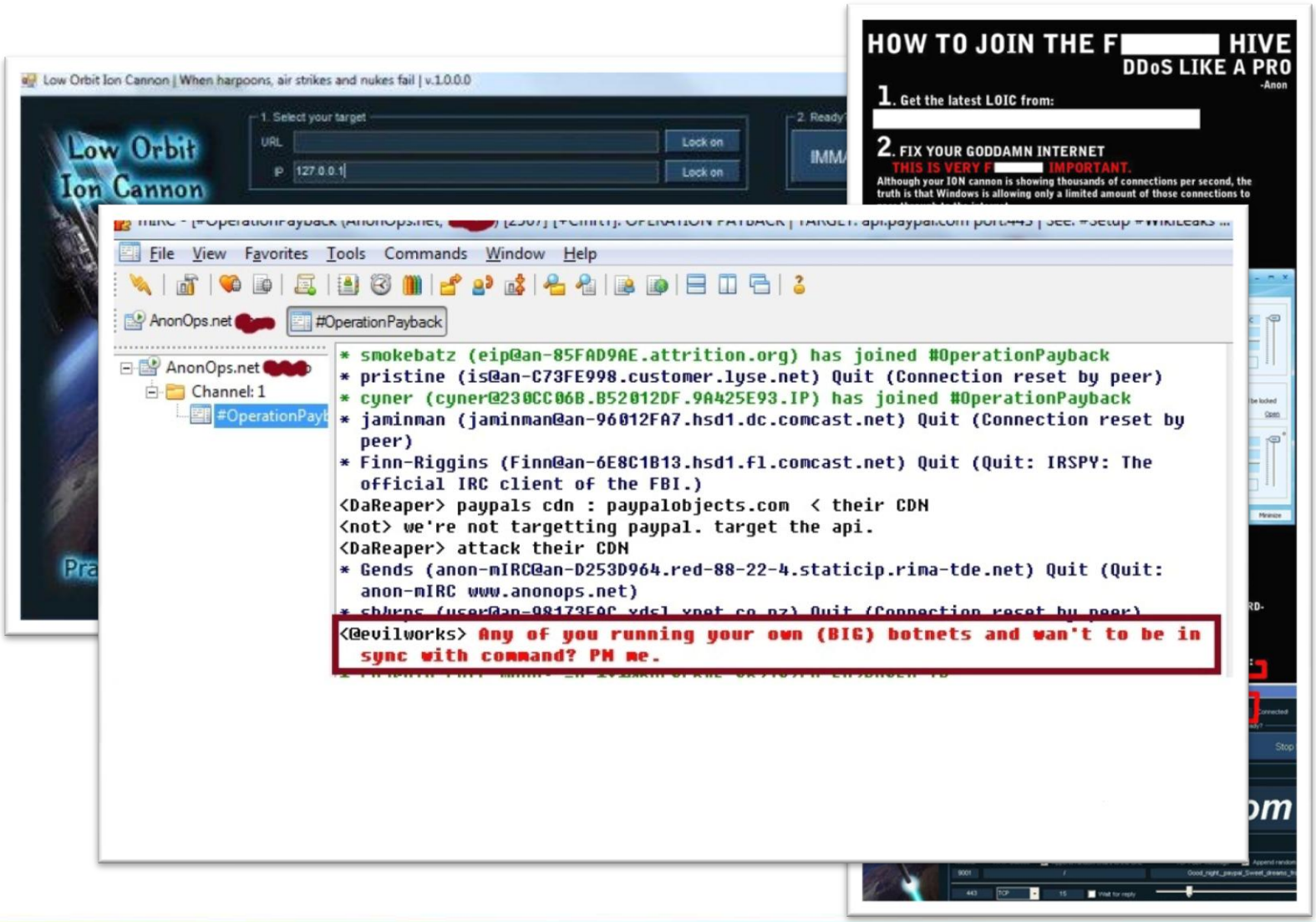


Low Orbit Ion Cannon





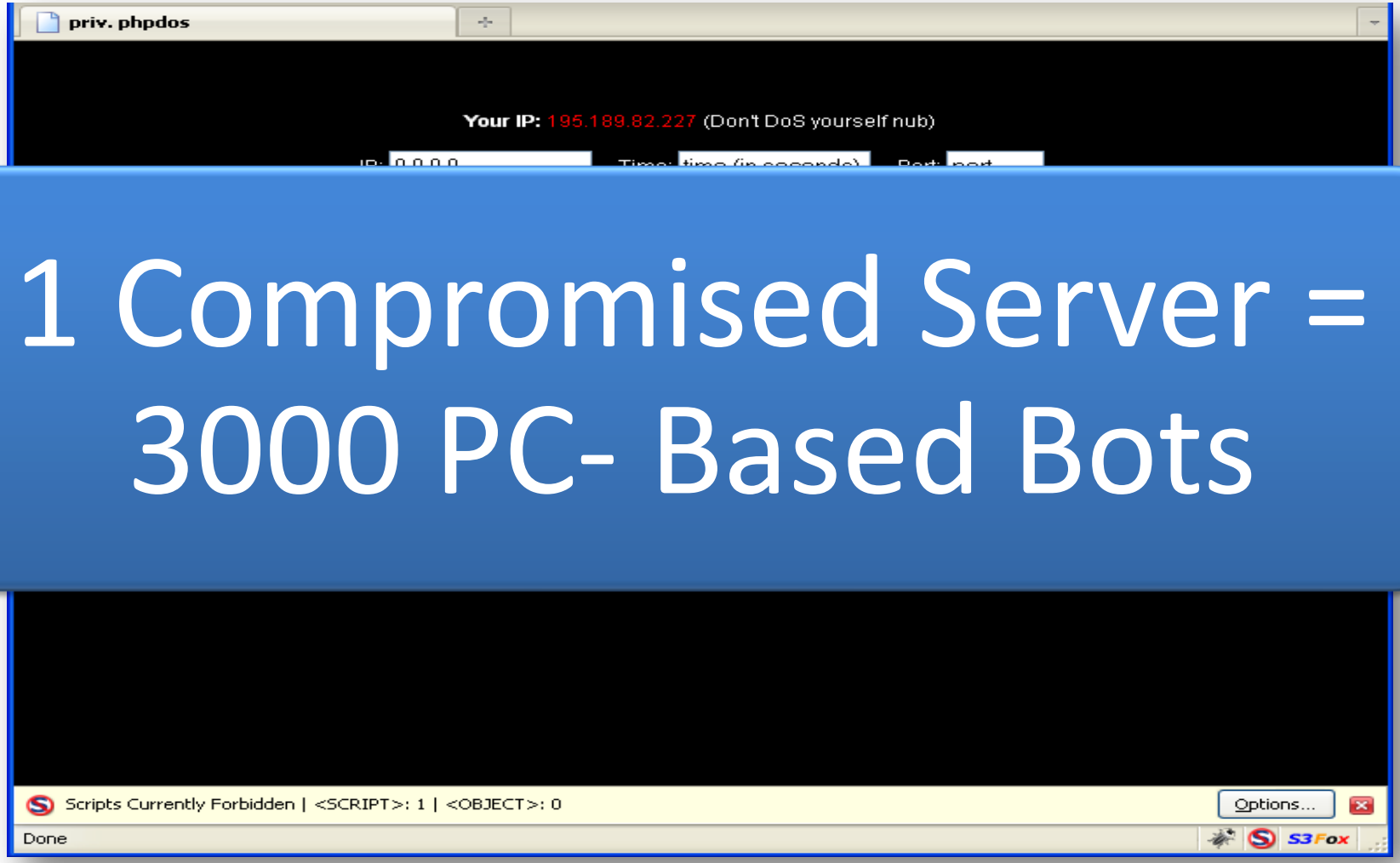
Low Orbit Ion Cannon



DDoS 2.0


priv. phpdos
Your IP: 195.189.82.227 (Don't DoS yourself nub)
IP: 0.0.0.0
Time: time (in seconds)
Port: port
Start the Attack—>
Scripts Currently Forbidden | <SCRIPT>: 1 | <OBJECT>: 0
Options...
Done
S3Fox

DDoS 2.0

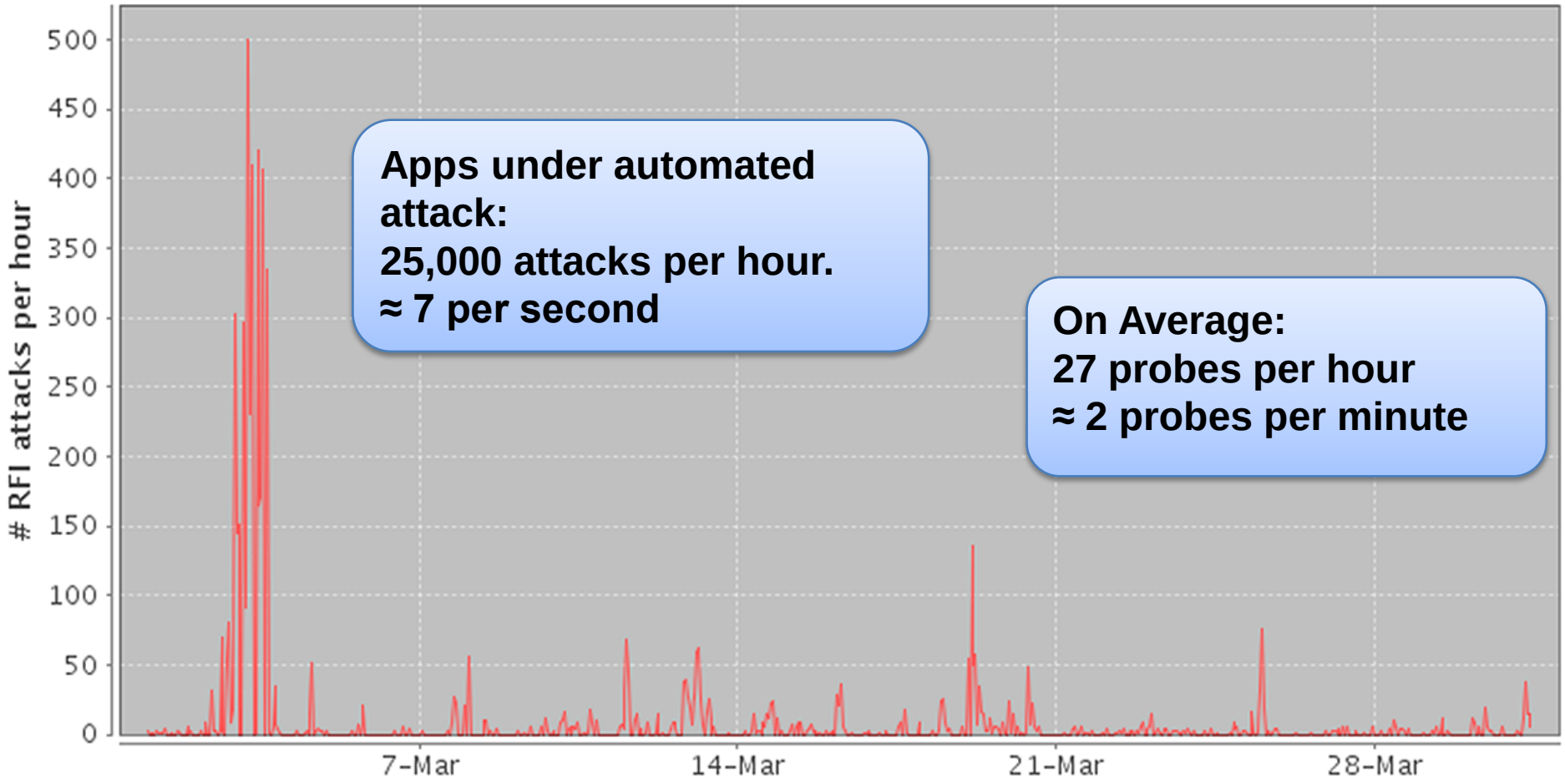


1 Compromised Server = 3000 PC- Based Bots

What are Hackers Hacking?

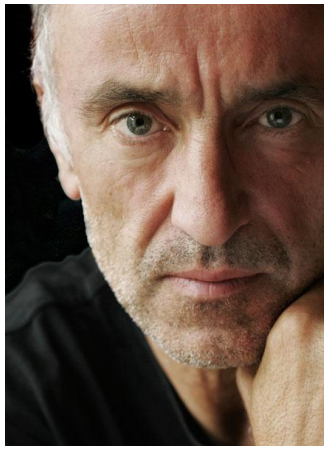
PART III: MONITORING TRAFFIC

Lesson #1: Automation is Prevailing



Lesson #1: Automation is Prevailing

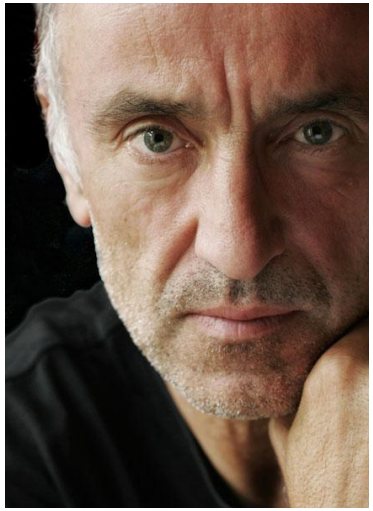
- Example: Google Dorks Campaign

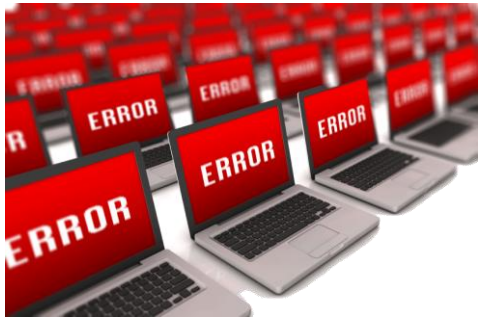


80,000

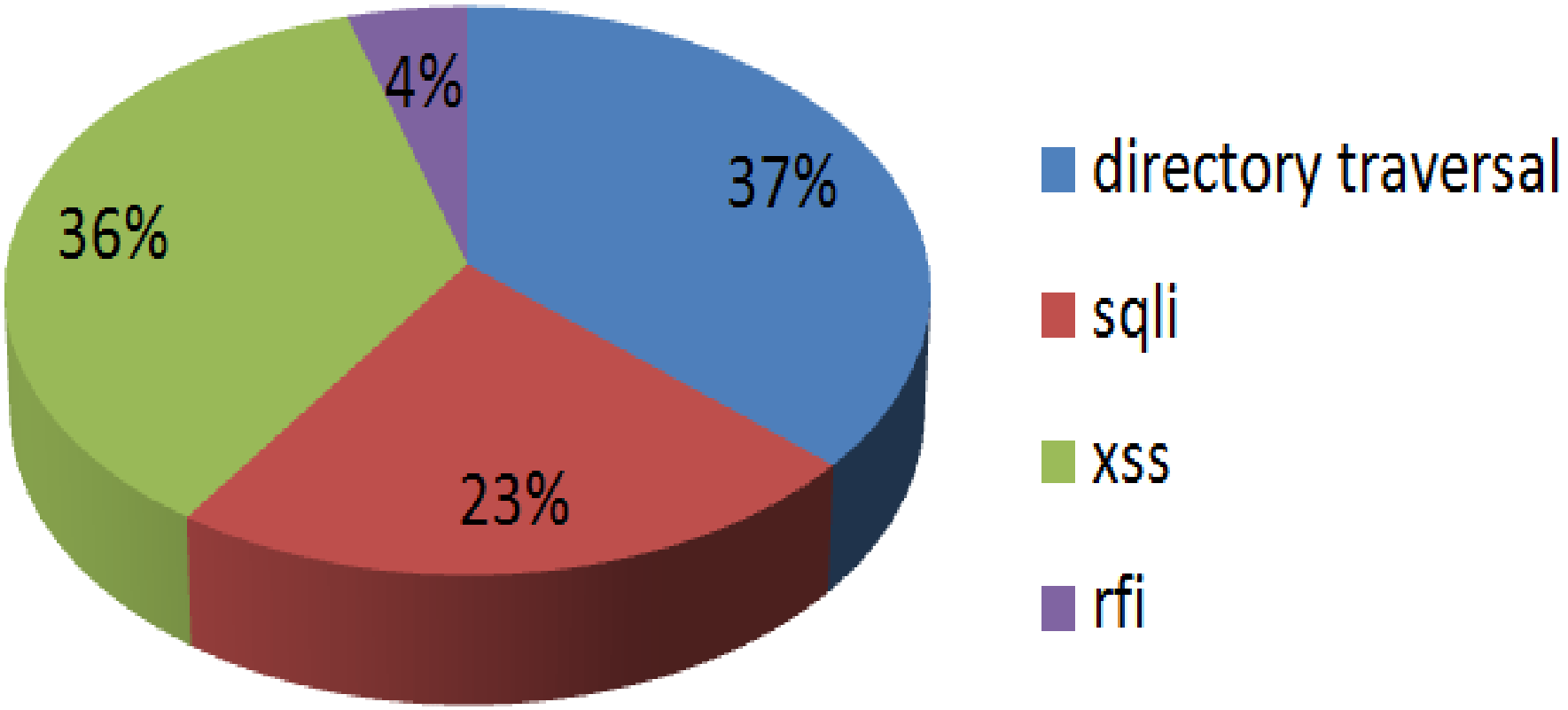
Lesson #1: Automation is Prevailing

Google



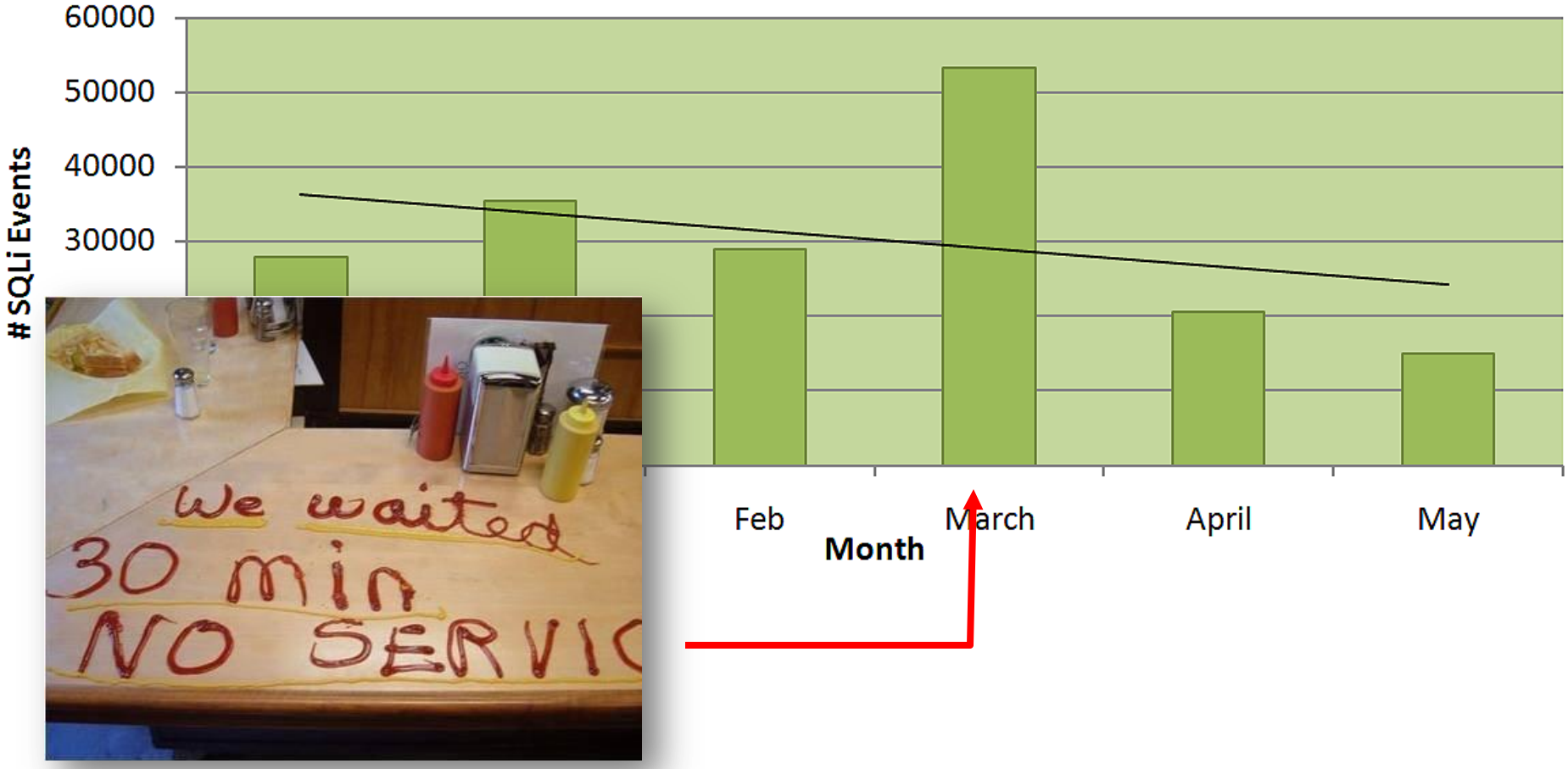


Lesson #2: The Unfab Four



Lesson #2A: The Unfab Four

SQL Injection



Lesson #2A: The Unfab Four

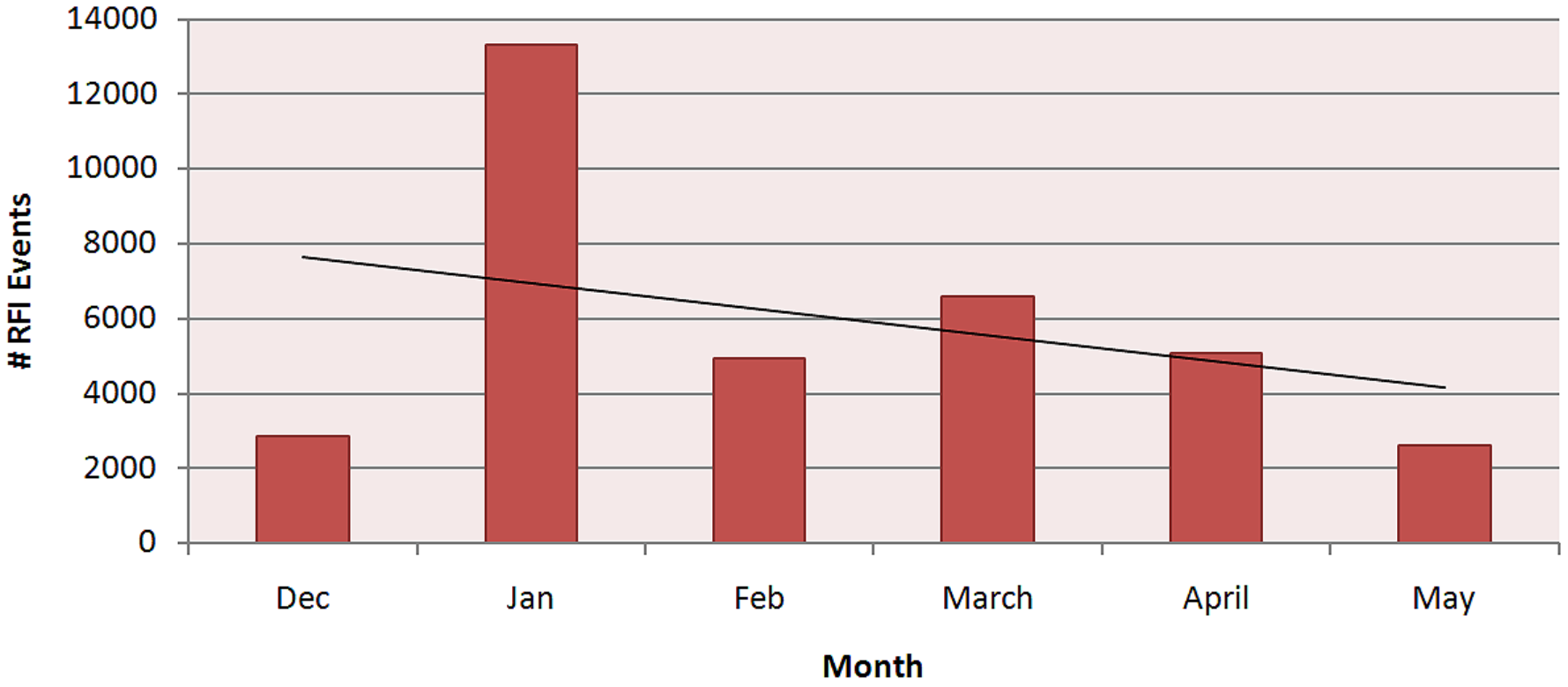
SQL Injection

		Average	Min	Max	Median	Standard Deviation
Attacks / hour	Since December 2010	53	1	7950	9	197
	Since July	71	1	4937	8	259
Attacks / day	Since December 2010	1093	44	21724	600	1909
	Since July	1589	106	8204	1162	1508

Table 1 : Statistics of SQLi occurrences

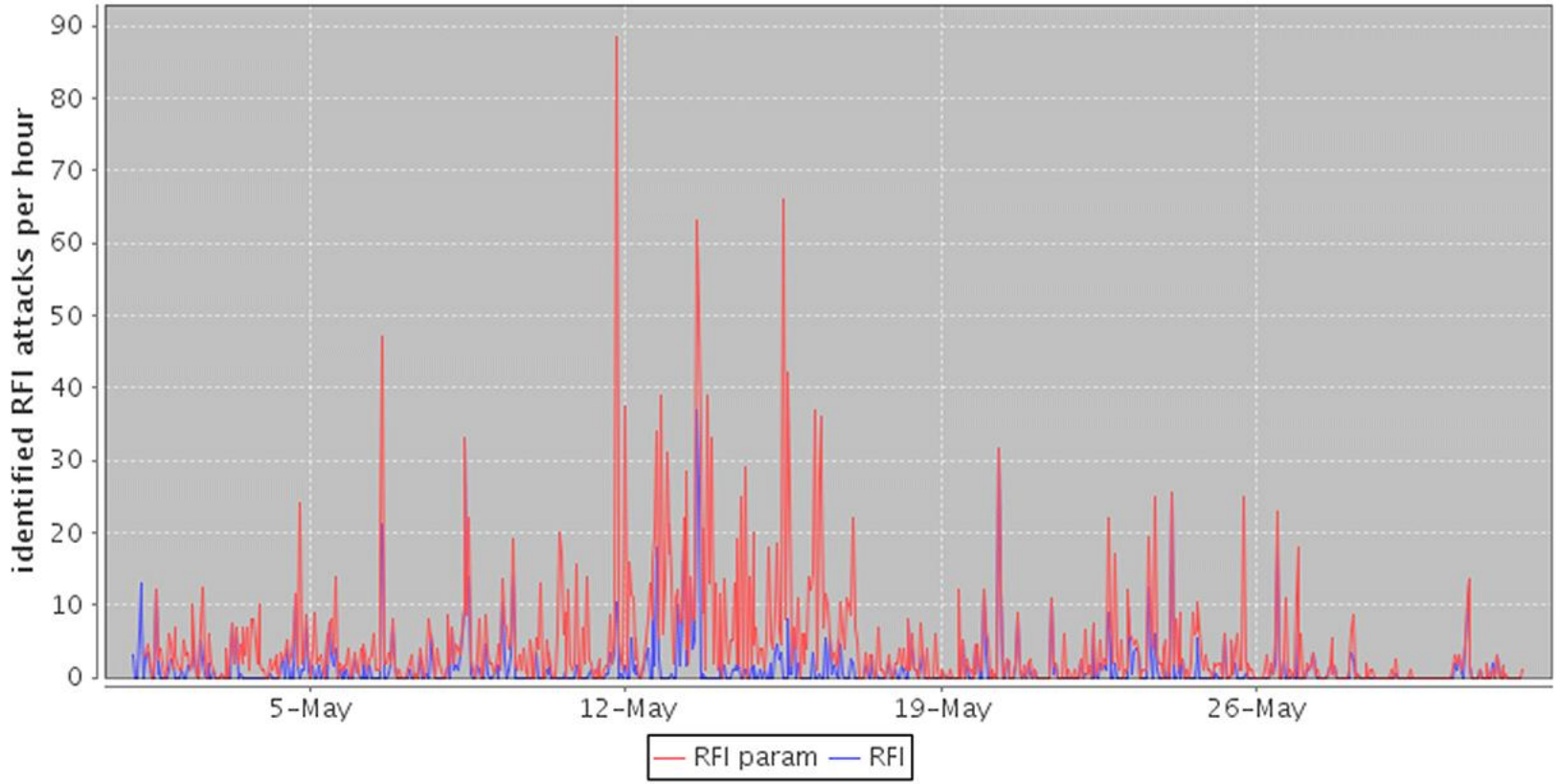
Lesson #2B: The Unfab Four

Remote File Inclusion



Lesson #2B: The Unfab Four

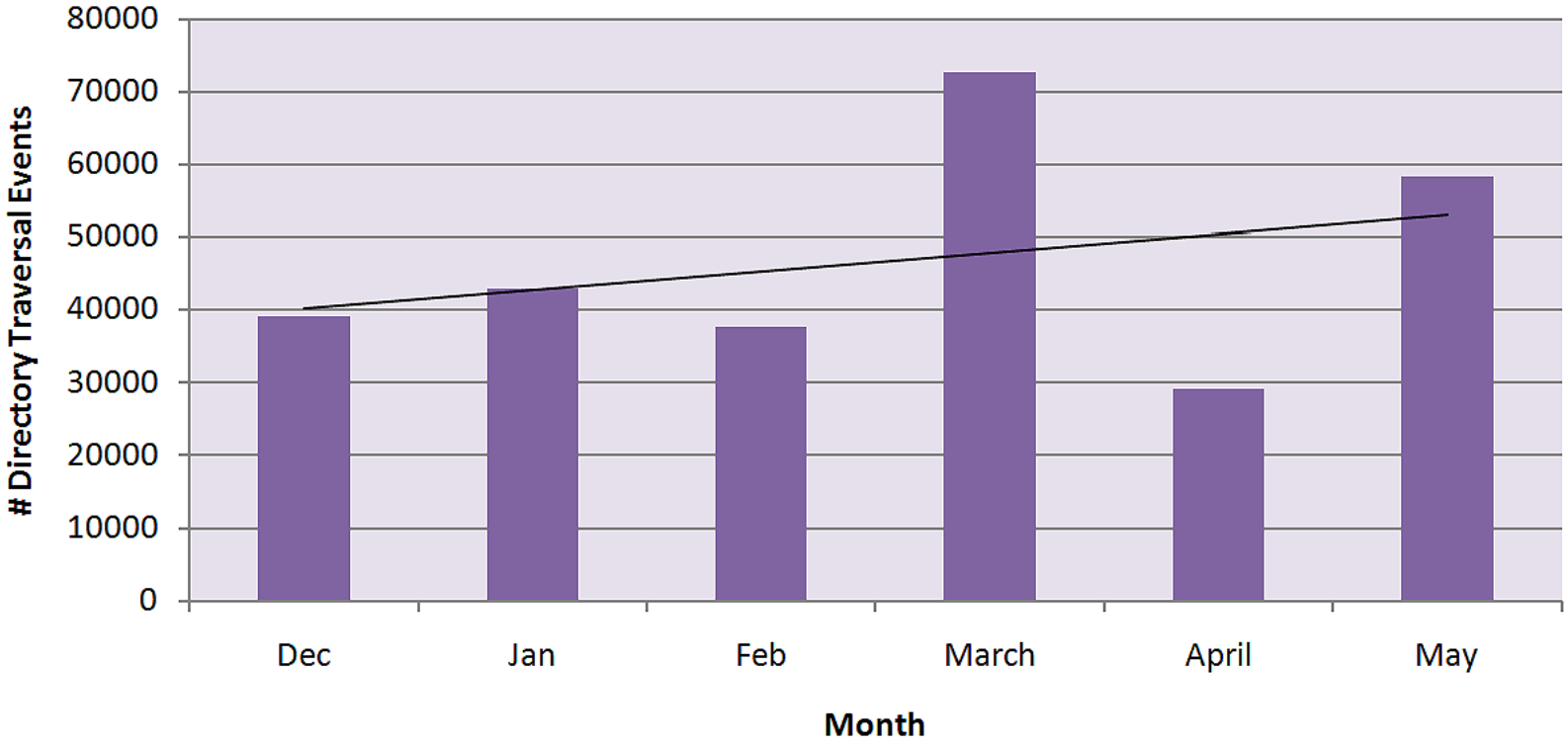
Remote File Inclusion



Analyzing the parameters and source of an RFI attack enhances common signature-based attack detection.

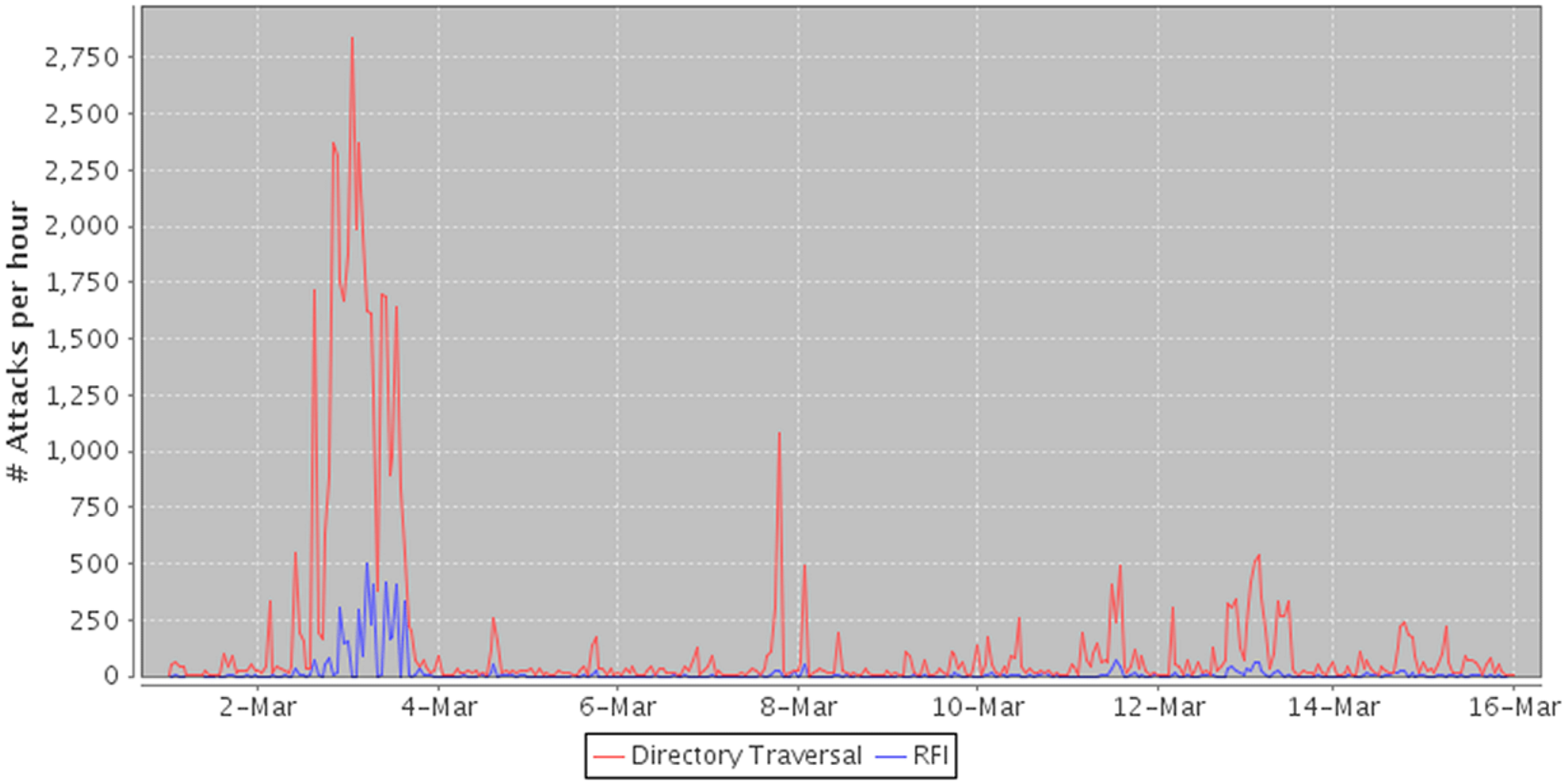
Lesson #2C: The Unfab Four

Directory Traversal



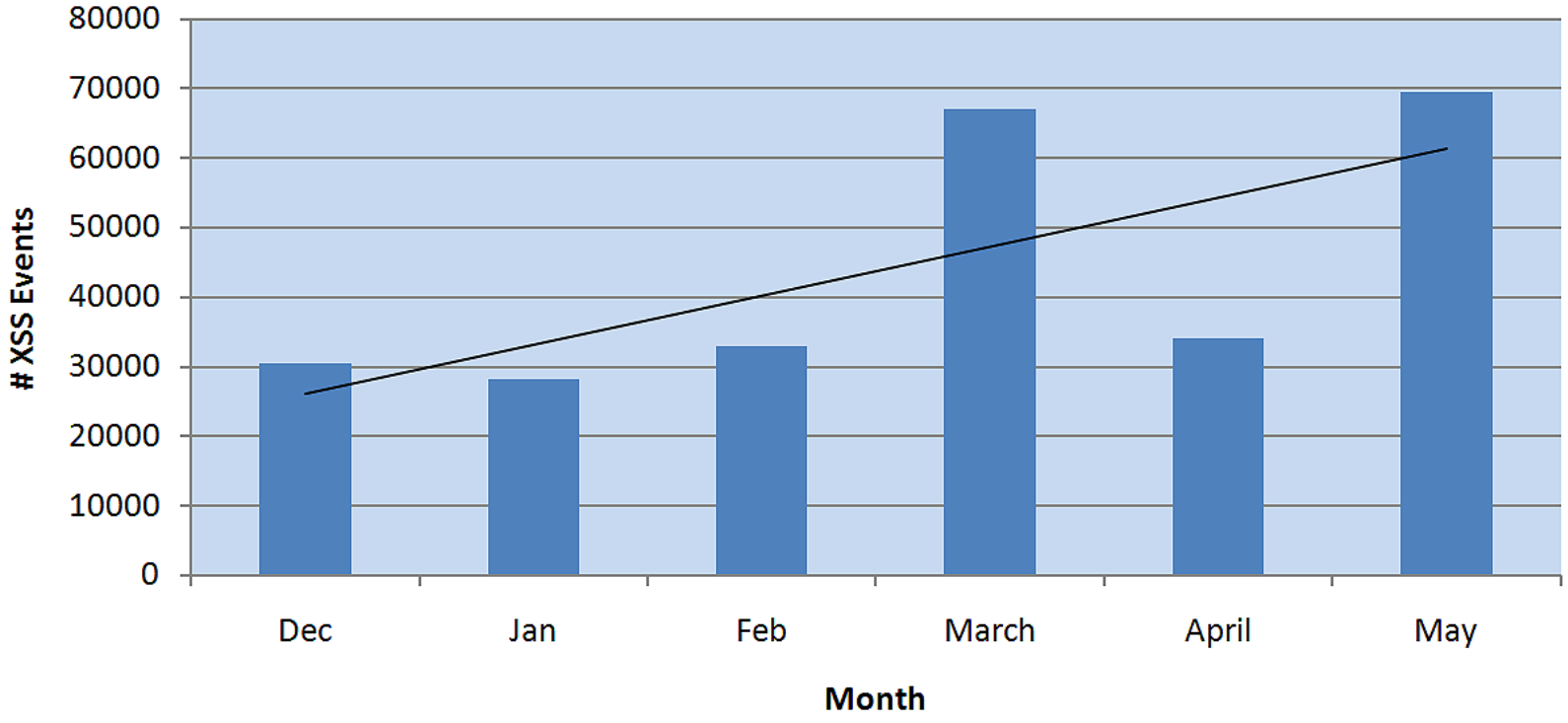
Lesson #2C: The Unfab Four

Directory Traversal



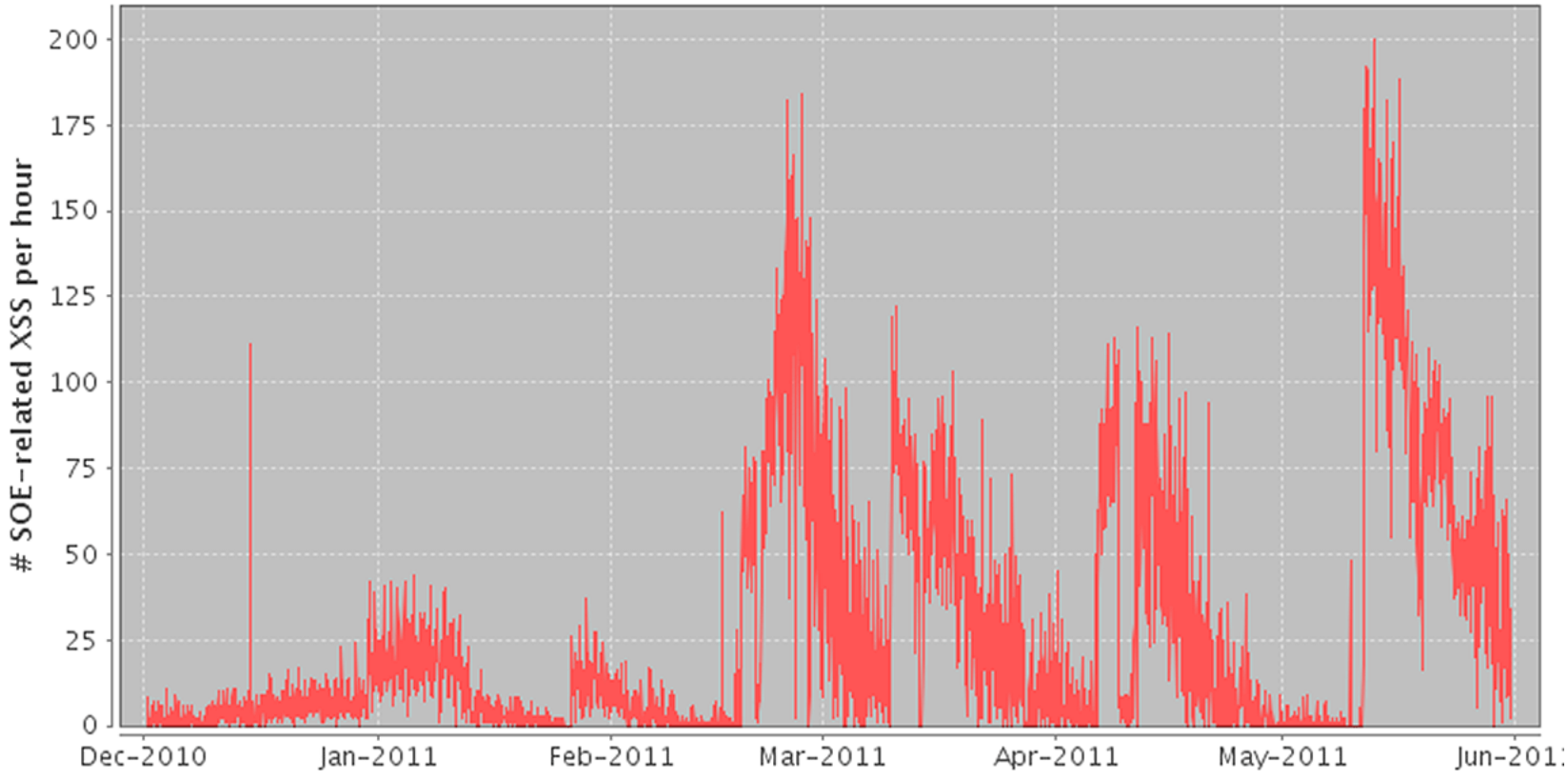
Lesson #2D: The Unfab Four

Cross Site Scripting



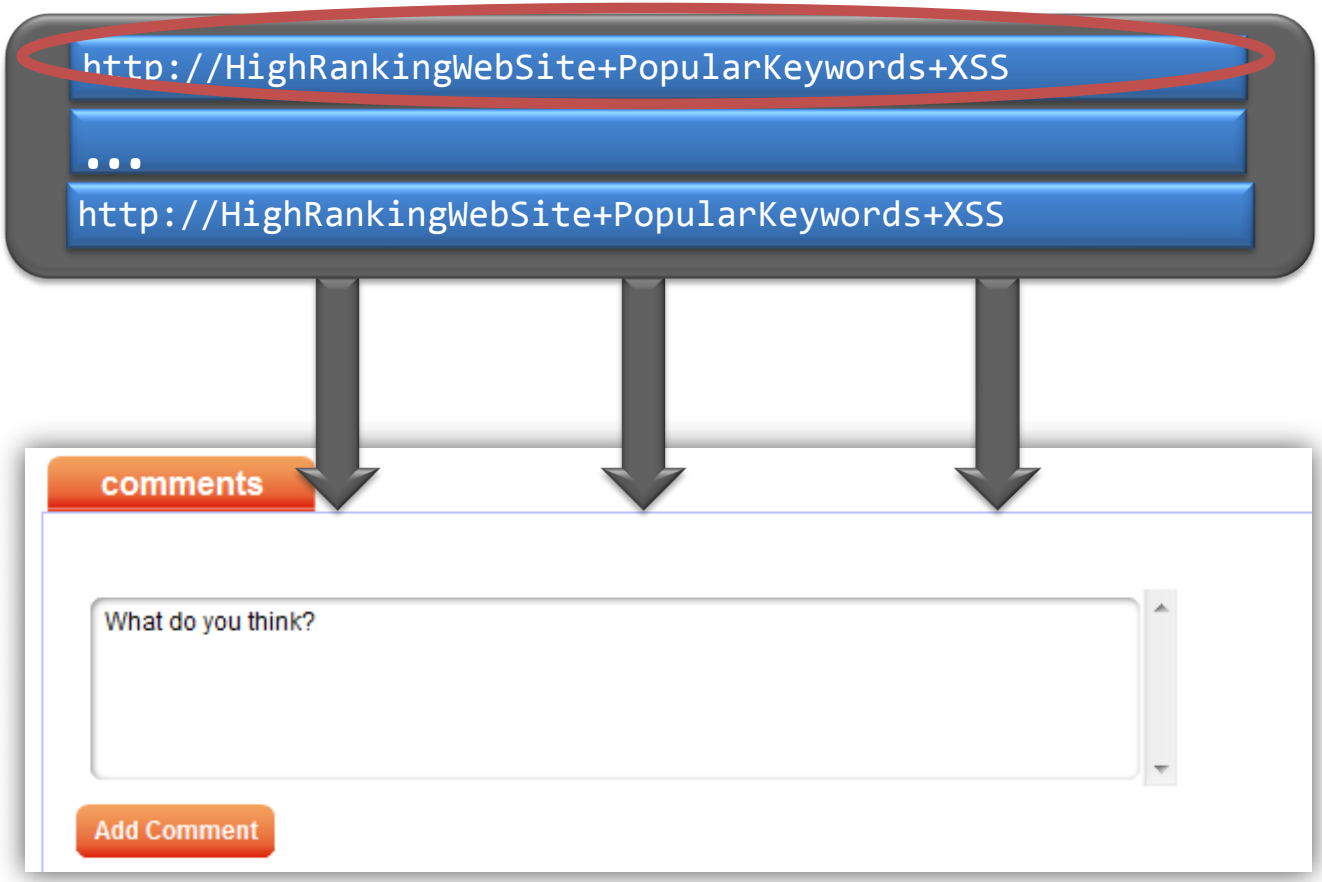
Lesson #2D: The Unfab Four

Cross Site Scripting



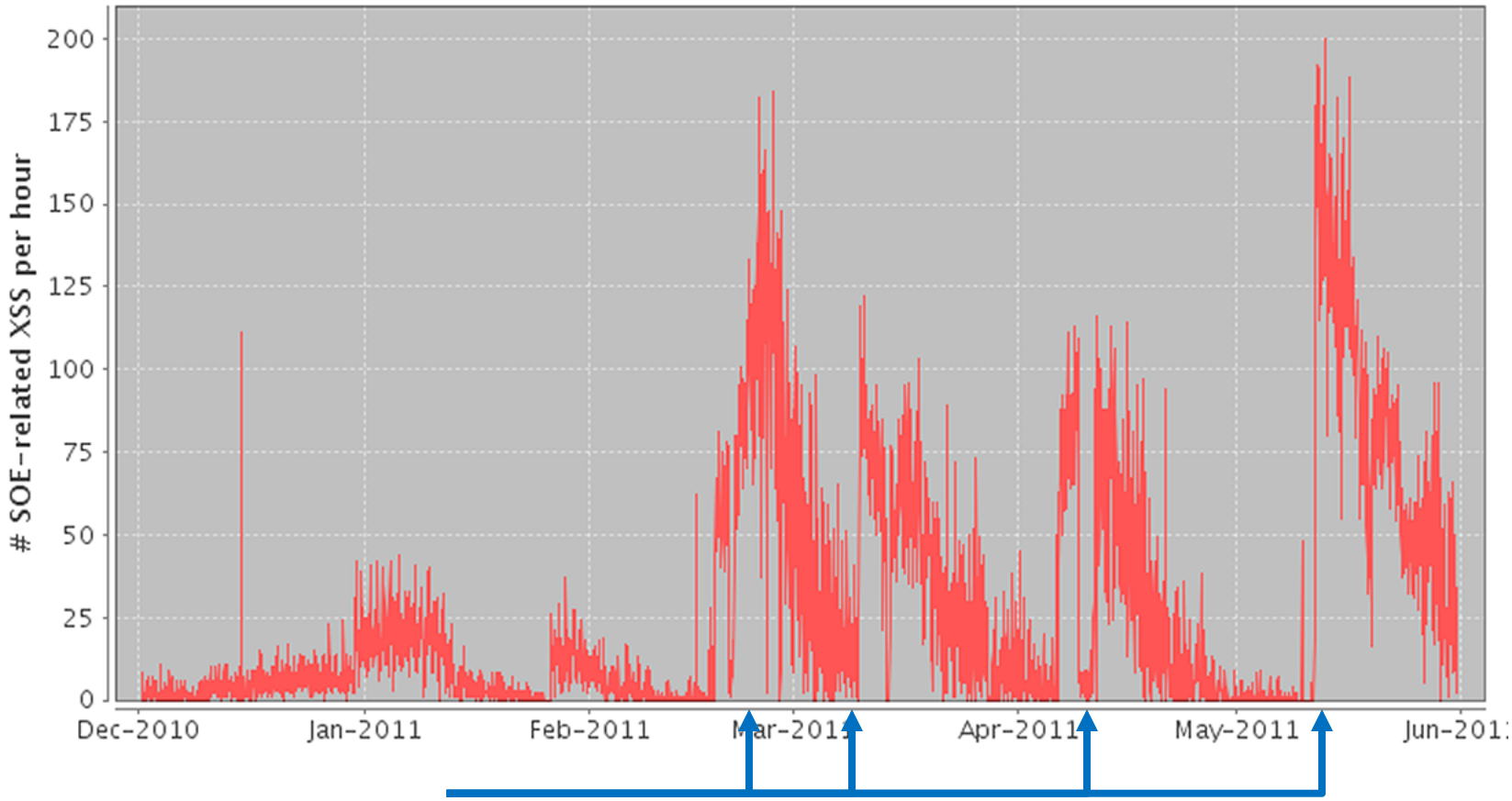
Lesson #2D: The Unfab Four

Cross Site Scripting – Zooming into Search Engine Poisoning



Lesson #2D: The Unfab Four

Cross Site Scripting



New Search Engine Indexing Cycle

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):

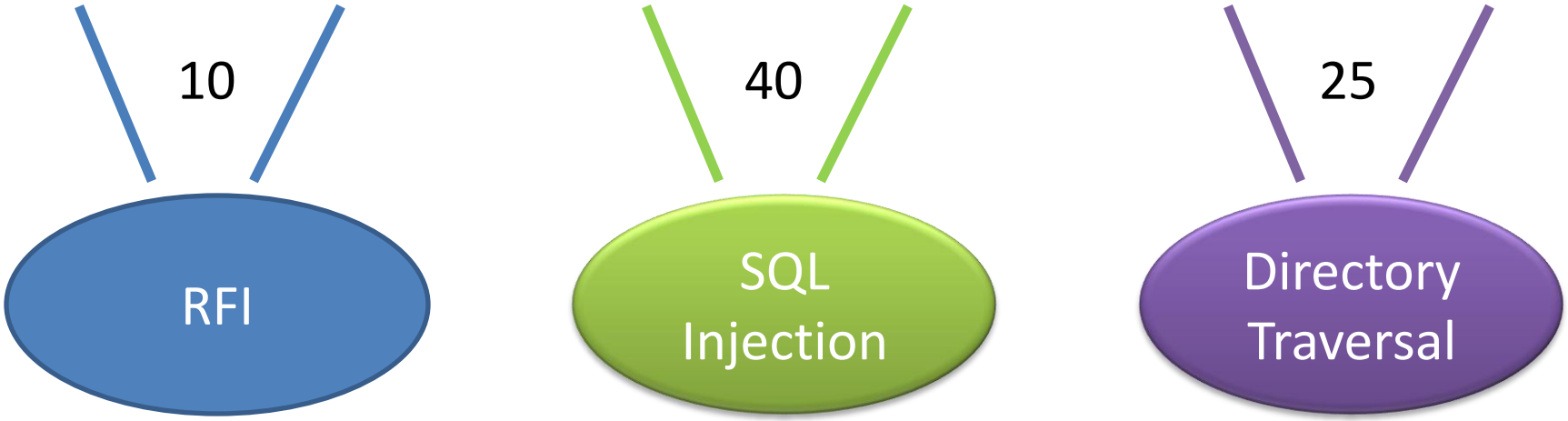
lol - storm would you also like the RFI/LFI bot with google bypass i was talking about while i have this plugged in?

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

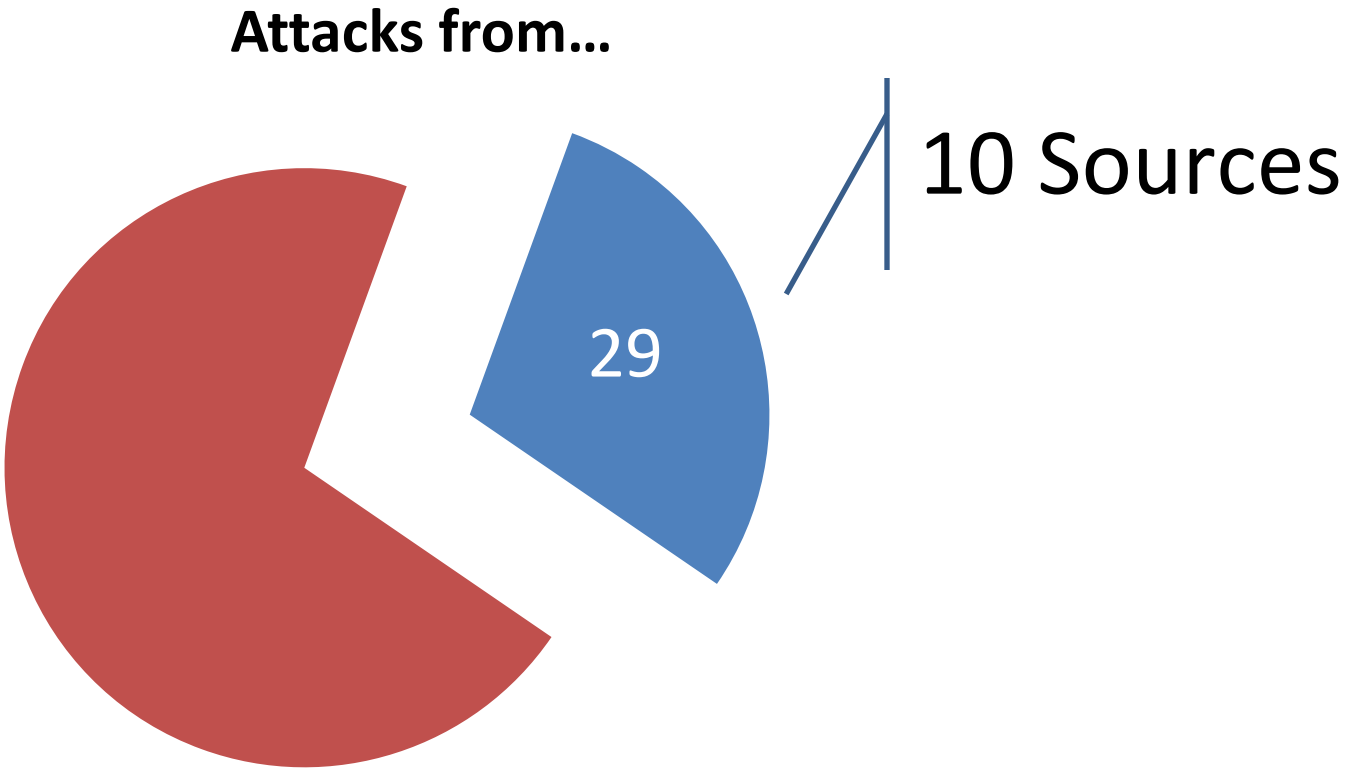
In 2009, a XSS vulnerability was found on the Sun website. A LulzSec member found an old server still online and running an old version of the newspaper website being still vulnerable to the same attack! Once pwned, this server was used as a jump-host to go deeper into the infrastructure. Finally the 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.

Lesson #3: Repeating Offenders

- The average number of attacks a single host initiated



Lesson #3: Repeating Offenders



MITIGATION

Underlying Assumptions…

- If you're online and vulnerable, you will be attacked
- Most organizations must assume a certain amount of infected machines connected to its network
  - It is not about technology it is about human nature

Effective Security (1)

- Deploy security solutions that deter automated attacks
  - Slowing down an attack is most often the best way to make it ineffective
  - Defeating automated browser activity:
    - Detecting protocol anomalies even if they are not considered malicious
    - Feed the client with bogus information (e.g hidden links)
  - Defeating automated non-browser activity
    - Access rate control for individual clients
    - Detection of non-human behavior (e.g. CAPTCHA, computational challenges)
    - Click rate measurements

Effective Security (2)

- Detect known vulnerabilities attack
  - Most attackers are going for the low hanging fruit
  - These may seem obvious common attacks, but RFI and DT do not even appear in OWASP's top 10 list.
  - Early detection of malicious scans can assist in mitigating unknown "0 days" vectors included in the scan

Effective Security (3)

- Acquire intelligence on malicious sources and apply it in real time
  - Sort traffic based on reputation
  - Blacklisting of: compromised servers, botnet Command and Control (C&C) servers, infected devices, active spam sources, crawlers…
  - Whitelisting of: legitimate search engine bots, aggregators
  - Enhances protection against automated attacks
  - Enhances protection against “zero”-day attacks

Effective Security (4)

- Participate in a security community and share data on attacks
  - Some of the attacks' scanning is horizontal across similar applications on the internet.
  - Assists in early detection of automation and blocking of attacks.

Effective Security (5)

- Take into consideration compromised machines within your network
  - More control is required around data sources
  - Identify abusive access patterns using legitimate privileges

Summary

"Foreknowledge cannot be gotten from ghosts and spirits, cannot be had by analogy, cannot be found out by calculation. It must be obtained from people, people who know the conditions of the enemy"*

*Sun Tzu – The art of war

QUESTIONS?

THANK YOU!