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

OWASP

Robert Rachwald

Imperva
Director, Security Strategy

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

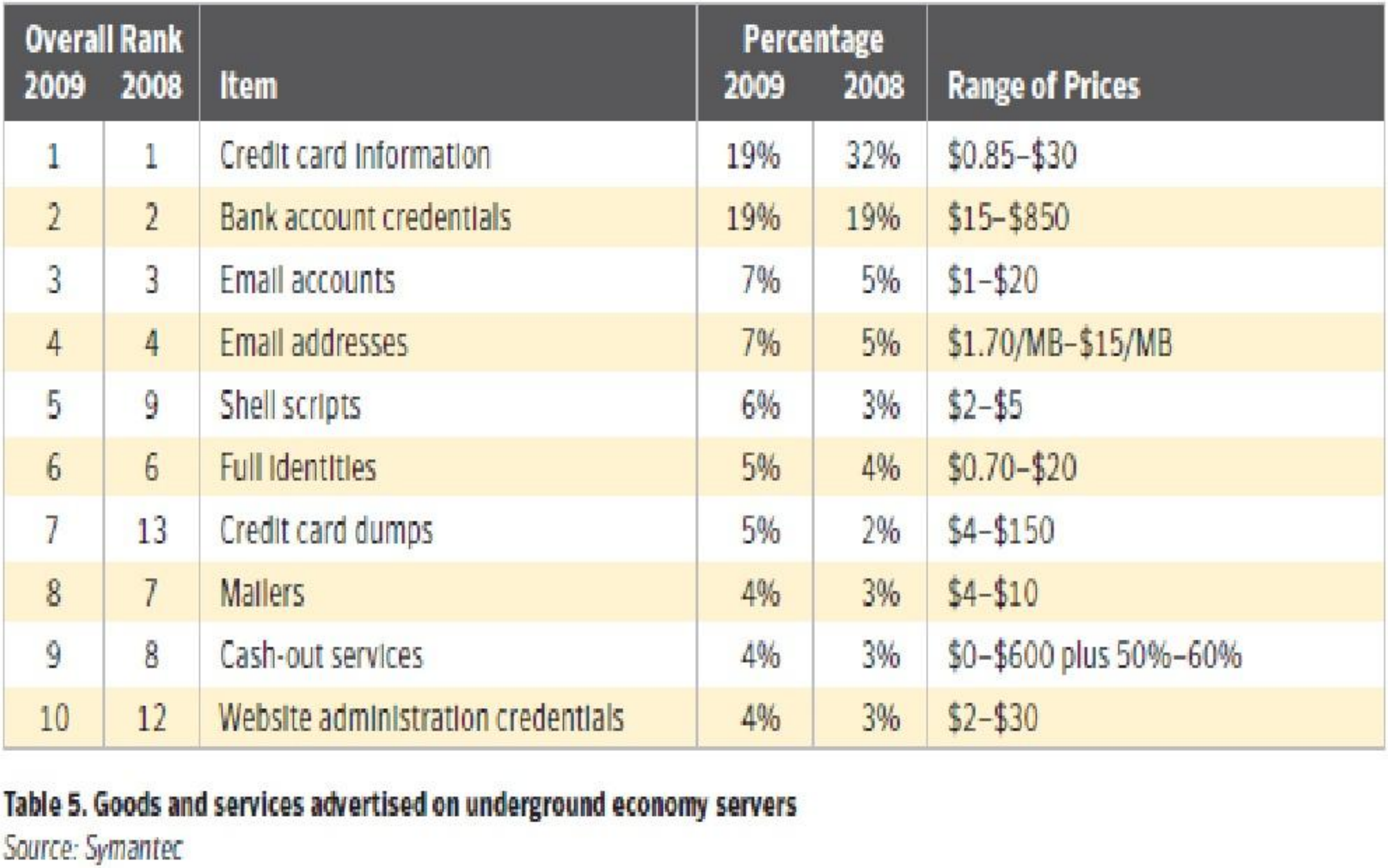
Agenda

- 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

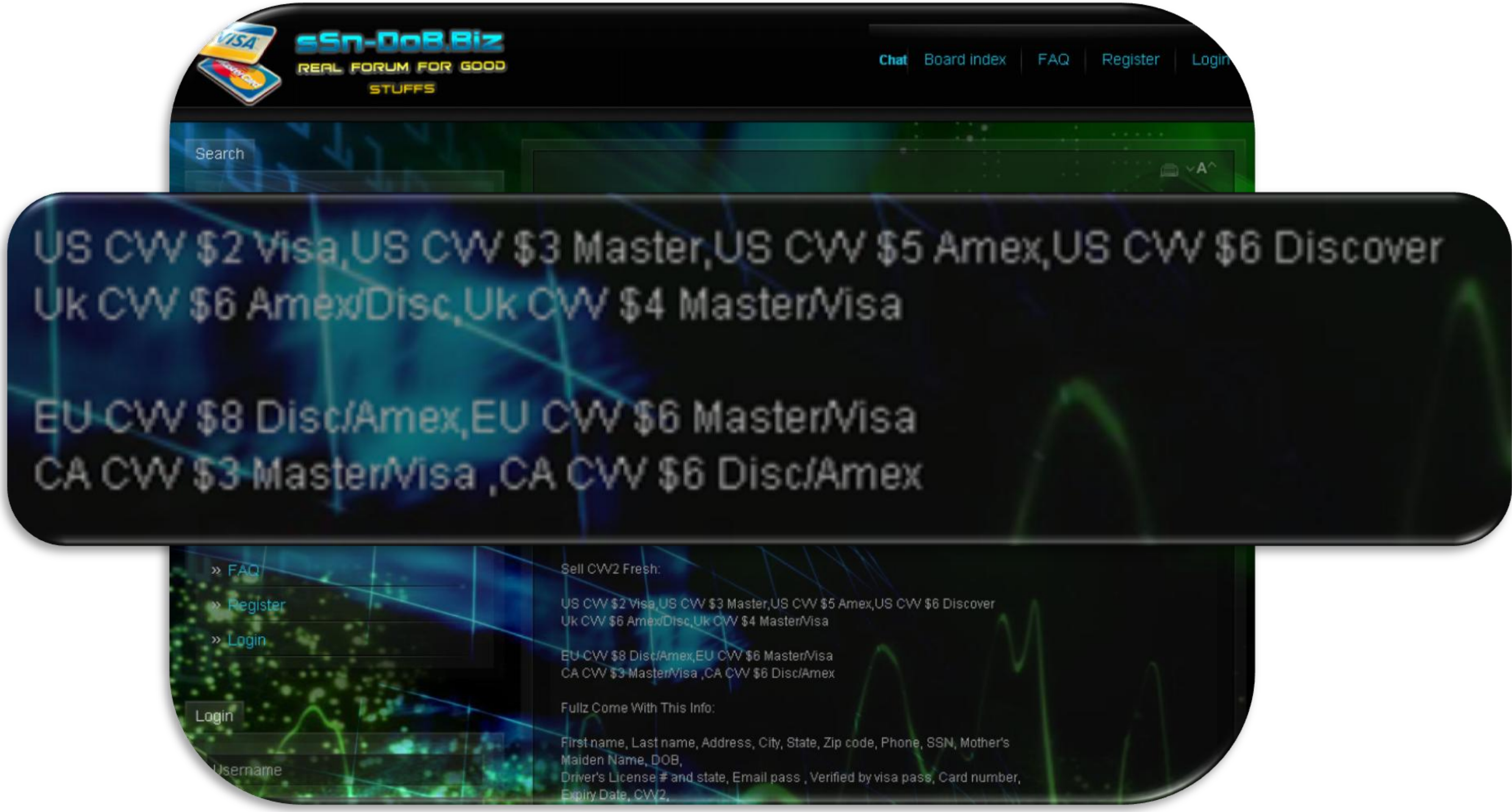


Overall Rank		Item	Percentage		Range of Prices
2009	2008		2009	2008	
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
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

The Underground Markets



Sell CVV2 Fresh:

US CVV $2 Visa,US CVV $3 Master,US CVV $5 Amex,US CVV $6 Discover
Uk CVV $6 Amex/Disc,Uk CVV $4 Master/Visa

EU CVV $8 Disc/Amex,EU CVV $6 Master/Visa
CA CVV $3 Master/Visa ,CA CVV $6 Disc/Amex

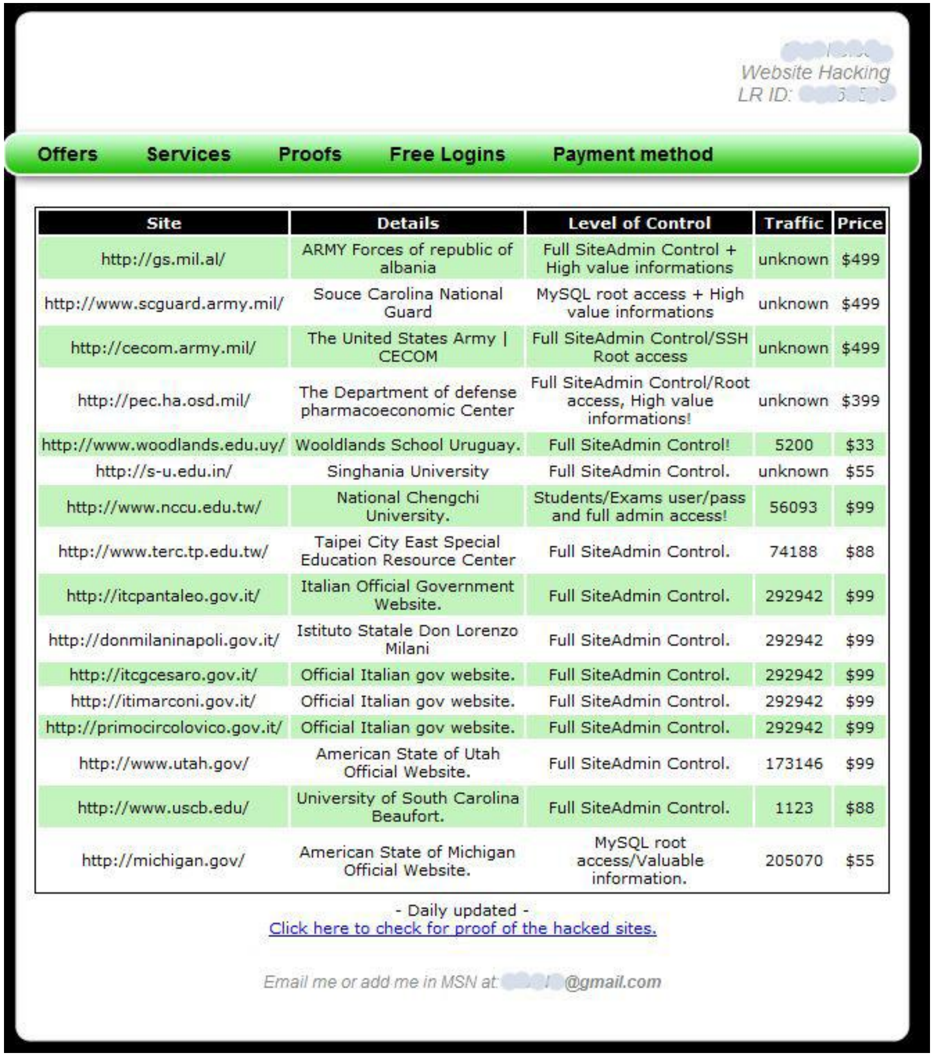
Fullz Come With This Info:

First name, Last name, Address, City, State, Zip code, Phone, SSN, Mother's Maiden Name, DOB,
Driver's License # and state, Email pass , Verified by visa pass, Card number, Expiry Date, CVV2,

US CVV $2 Visa,US CVV $3 Master,US CVV $5 Amex,US CVV $6 Discover
Uk CVV $6 Amex/Disc,Uk CVV $4 Master/Visa

EU CVV $8 Disc/Amex,EU CVV $6 Master/Visa
CA CVV $3 Master/Visa ,CA CVV $6 Disc/Amex

Website Access Up for Sale



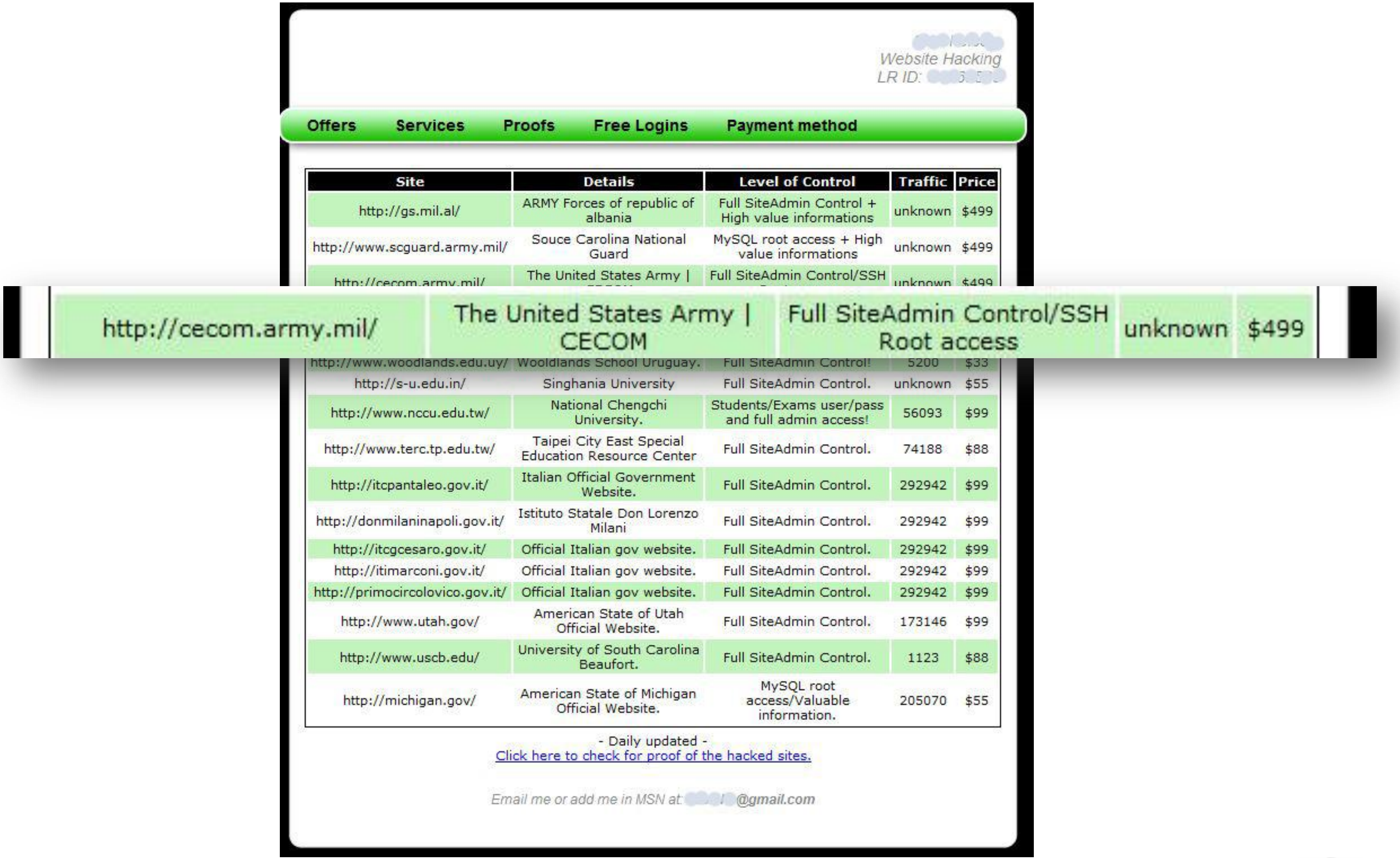
[redacted]
Website Hacking
LR ID: [redacted]

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/	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**

Website Access Up for Sale



[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://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

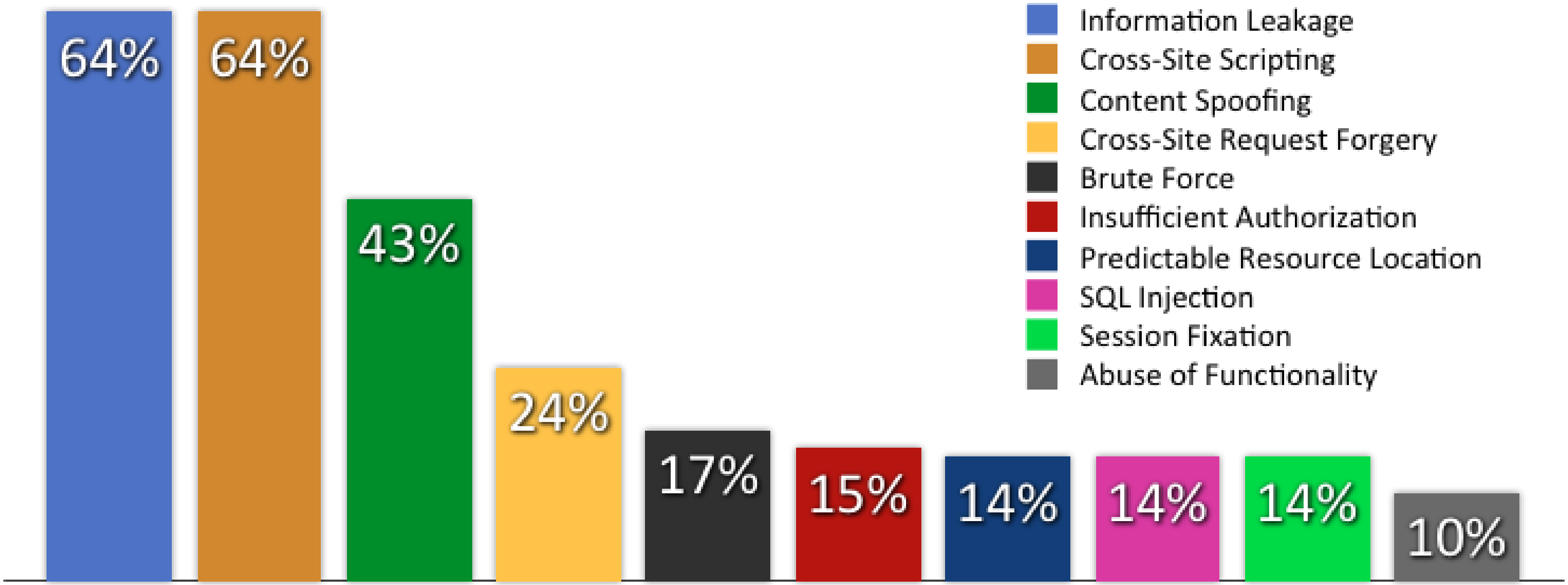
- Daily updated -
Click here to check for proof of the hacked sites.

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

OWASP

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

x

of

But which will be exploited?

821,771,600

vulnerabilities in active circulation

OWASP

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 forum

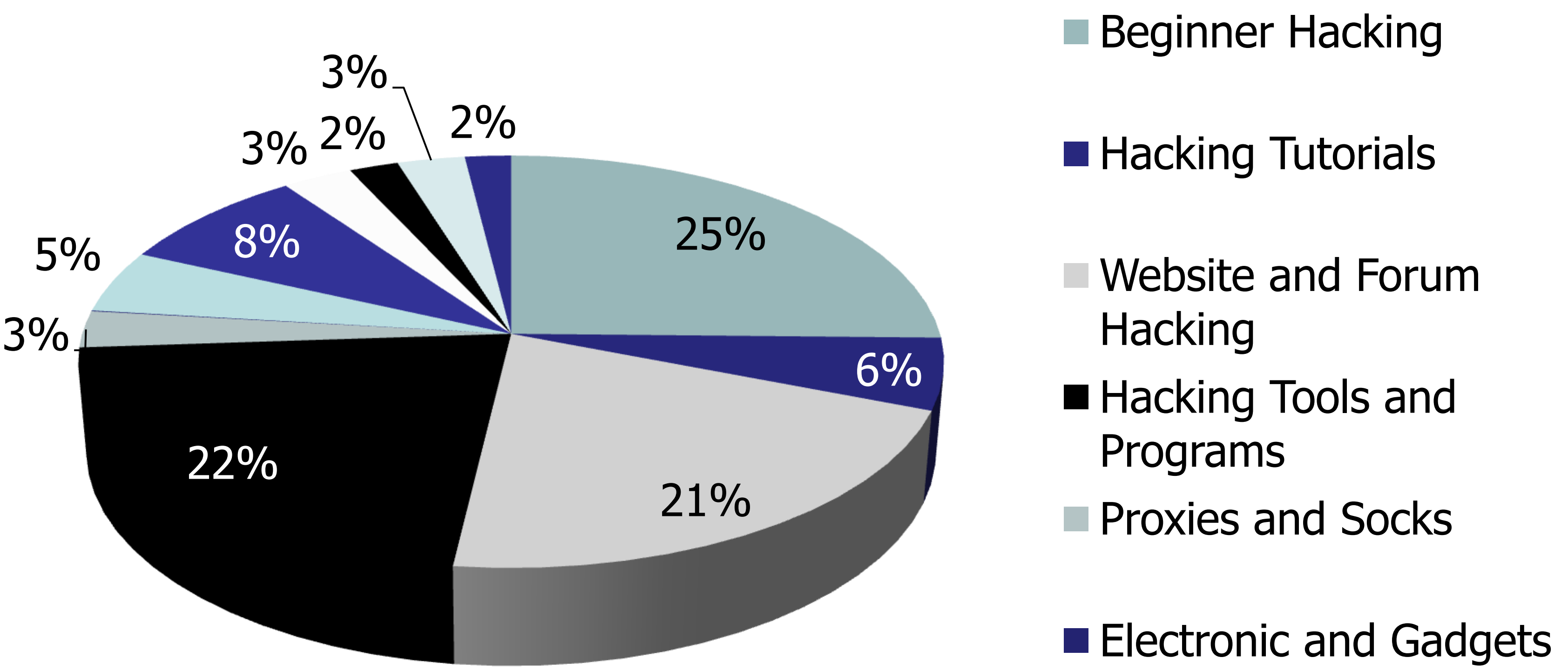
2. Analyze hacker tools and activity

3. Record and monitor hacker activity

What are Hackers Hacking?

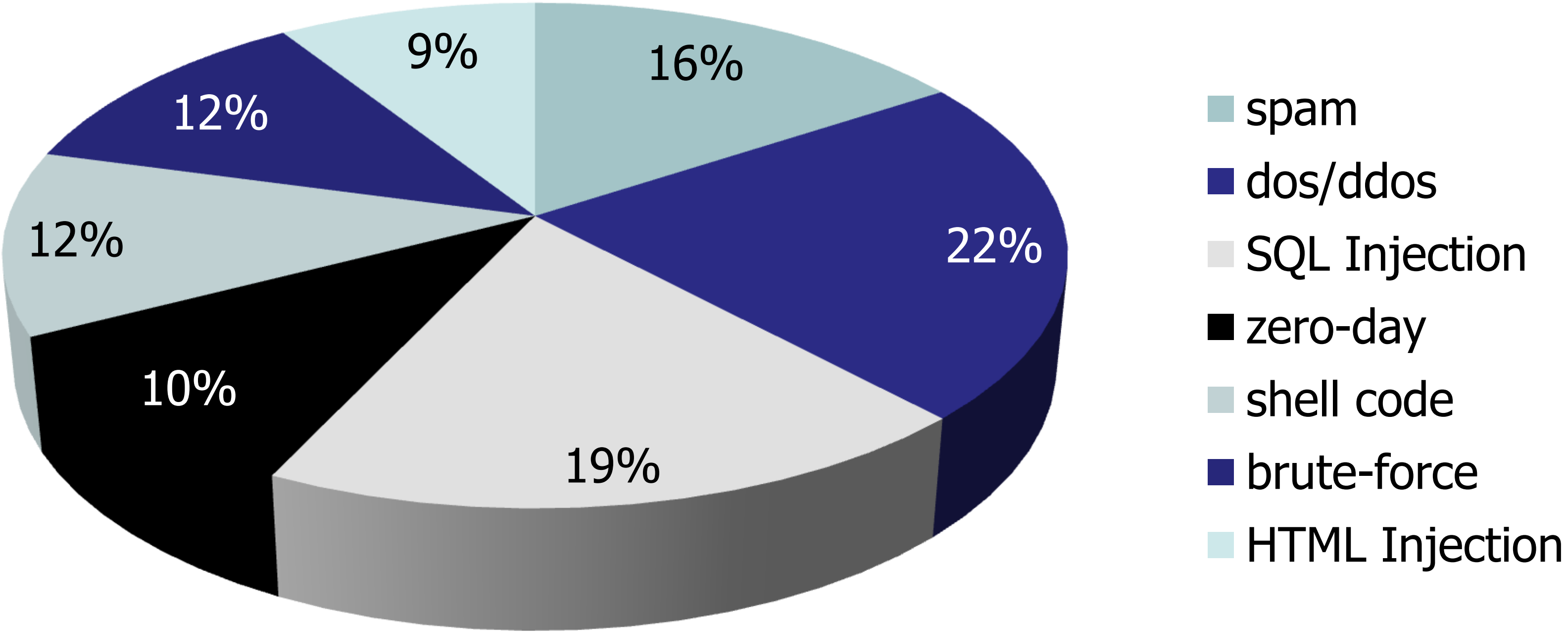
PART I: HACKER FORUMS

General Topics: Hacker Forum Analysis



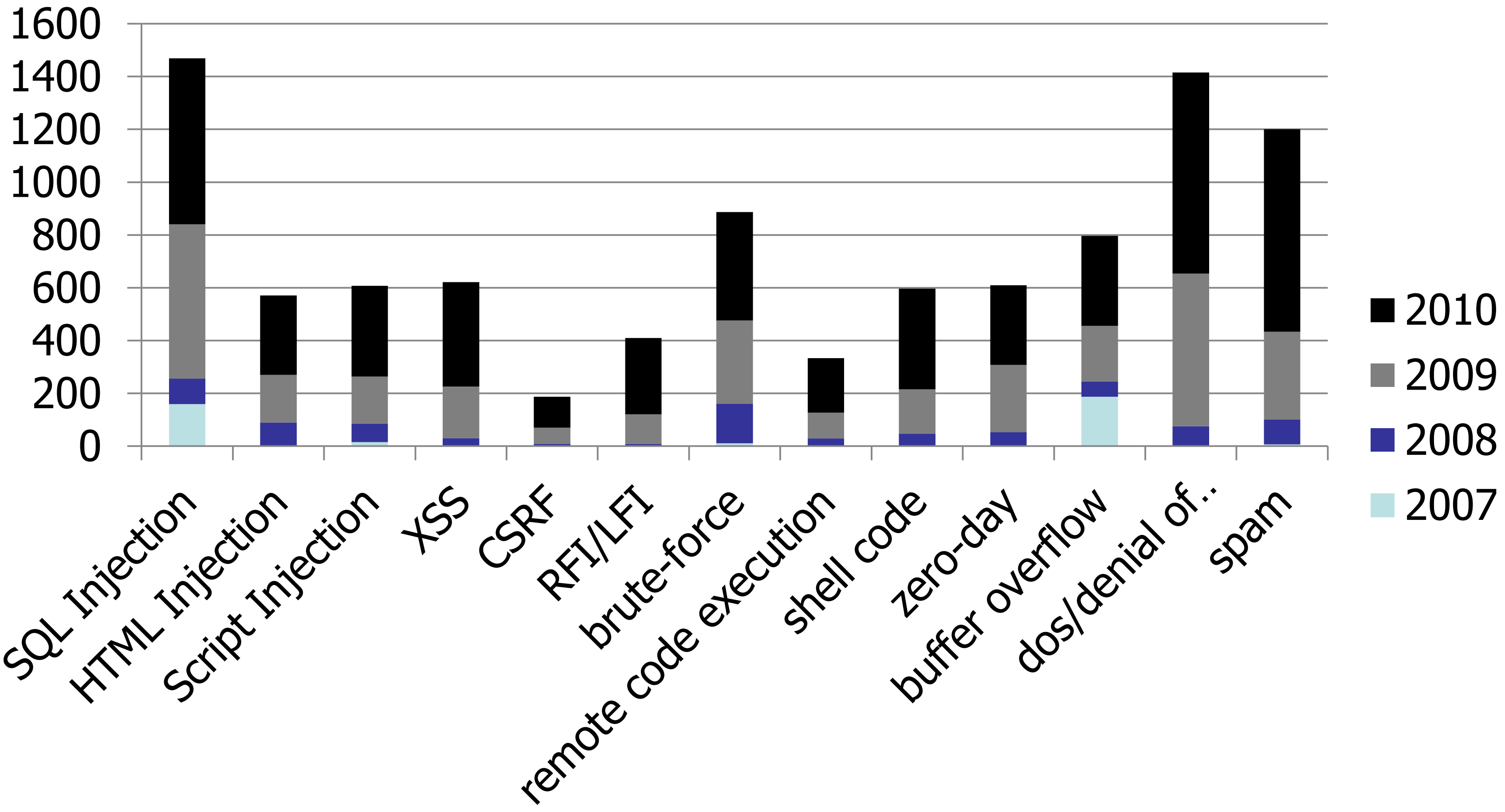
Dates: 2007- 2011

Top 7 Attack Techniques: Hacker Forum Analysis



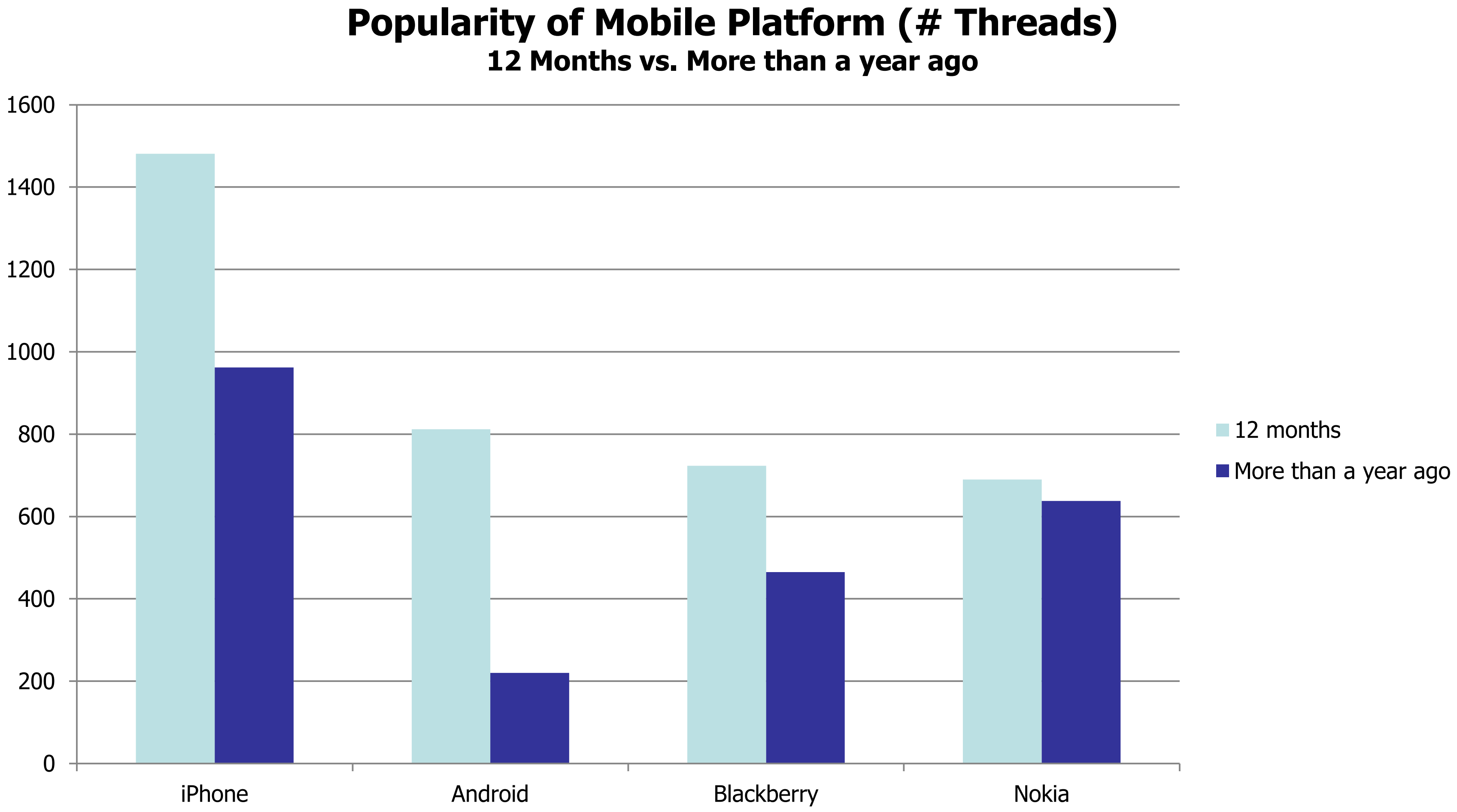
Dates: July 2010 -July 2011

Growth of Discussion Topics by Year



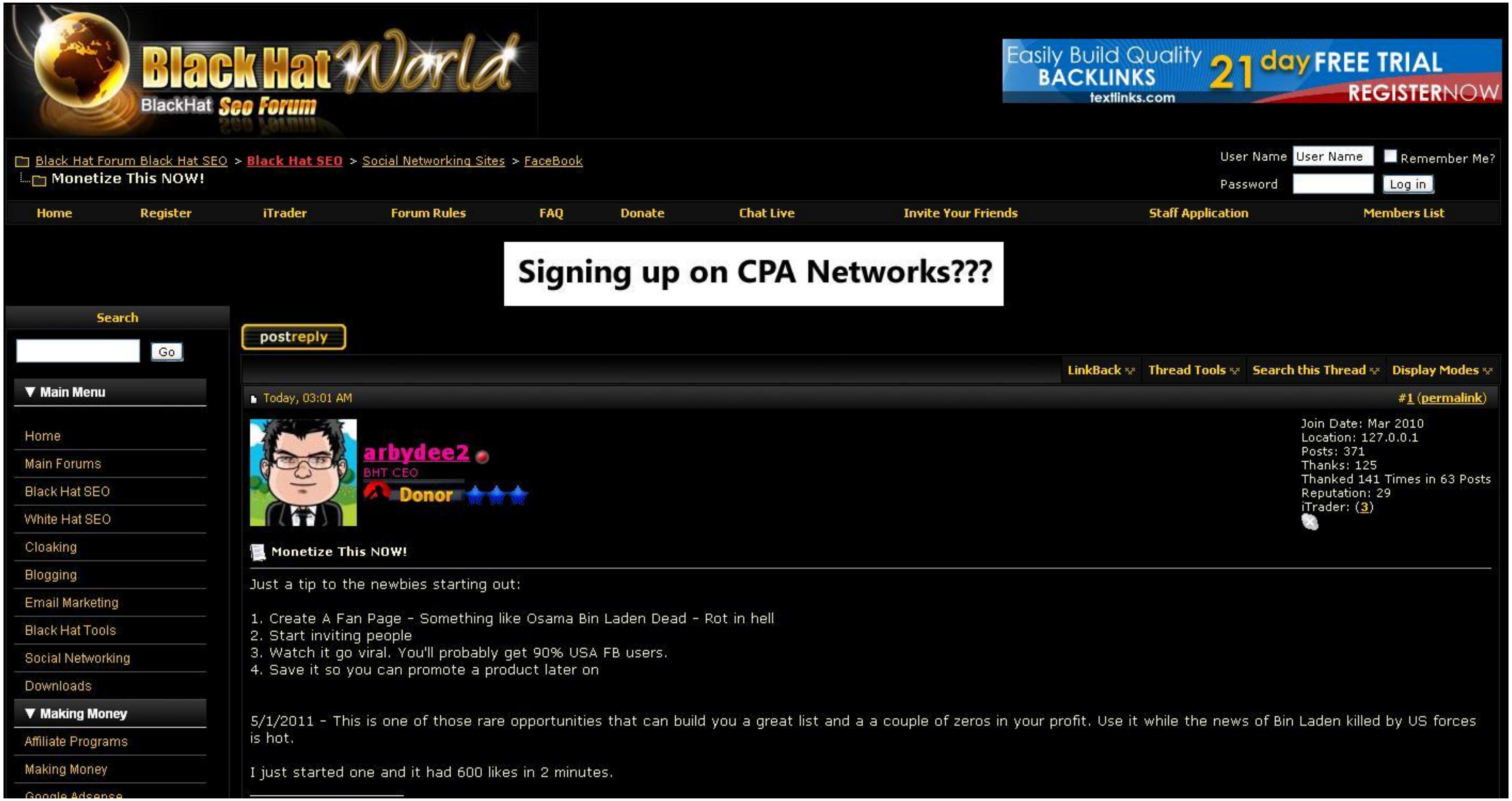
Dates: 2007- July 2010

Mobile (in)Security



Dates: July 2010-July 2011

Qualitative Analysis



Signing up on CPA Networks???

Today, 03:01 AM #1 (permalink)

arbydee2
BHT CEO
Donor

Join Date: Mar 2010
Location: 127.0.0.1
Posts: 371
Thanks: 125
Thanked 141 Times in 63 Posts
Reputation: 29
iTrader: (3)

Monetize This NOW!

Just a tip to the newbies starting out:

1. Create A Fan Page - Something like Osama Bin Laden Dead - Rot in hell
2. Start inviting people
3. Watch it go viral. You'll probably get 90% USA FB users.
4. Save it so you can promote a product later on

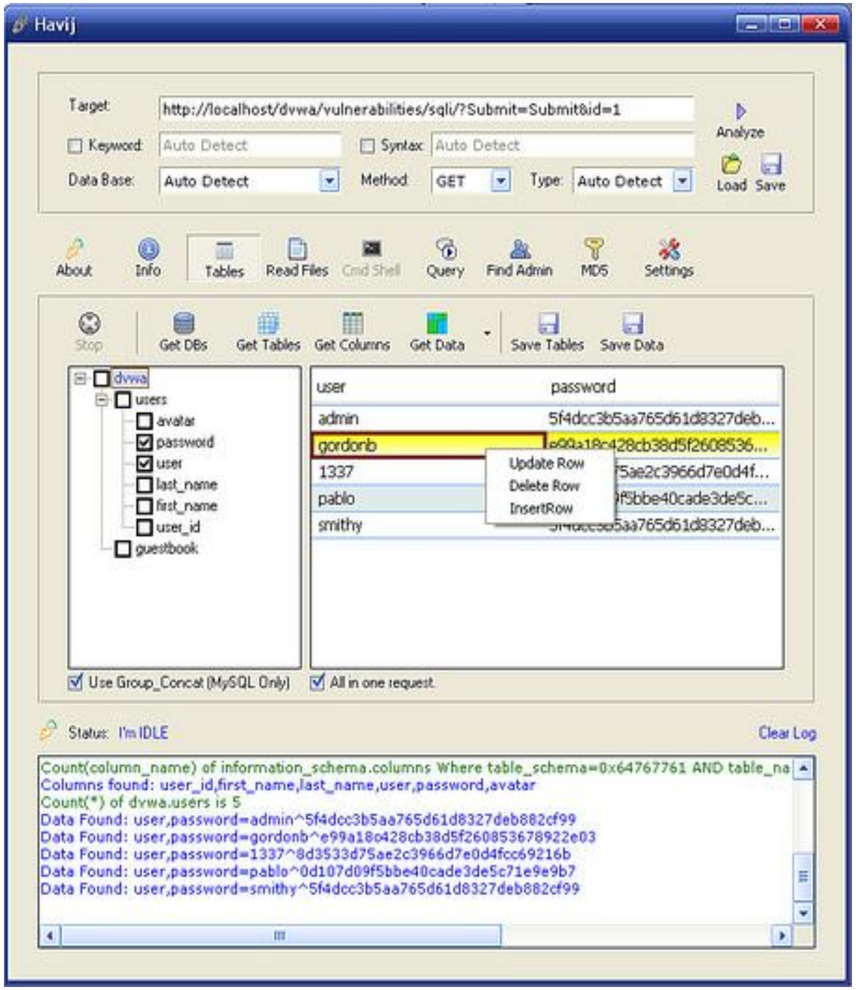
5/1/2011 - This is one of those rare opportunities that can build you a great list and a a couple of zeros in your profit. Use it while the news of Bin Laden killed by US forces is hot.

I just started one and it had 600 likes in 2 minutes.

What are Hackers Hacking?

PART II: ATTACK TECHNOLOGIES

Example: SQL Injection Attack Tools



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

□ Keyword: Auto Detect □ Syntax: Auto Detect

Data Base: Auto Detect Method: GET Type: Auto Detect

- □ dvwa
  - □ users
    - □ avatar
    - ☑ password
    - ☑ user
    - □ last_name
    - □ first_name
    - □ user_id
  - □ guestbook

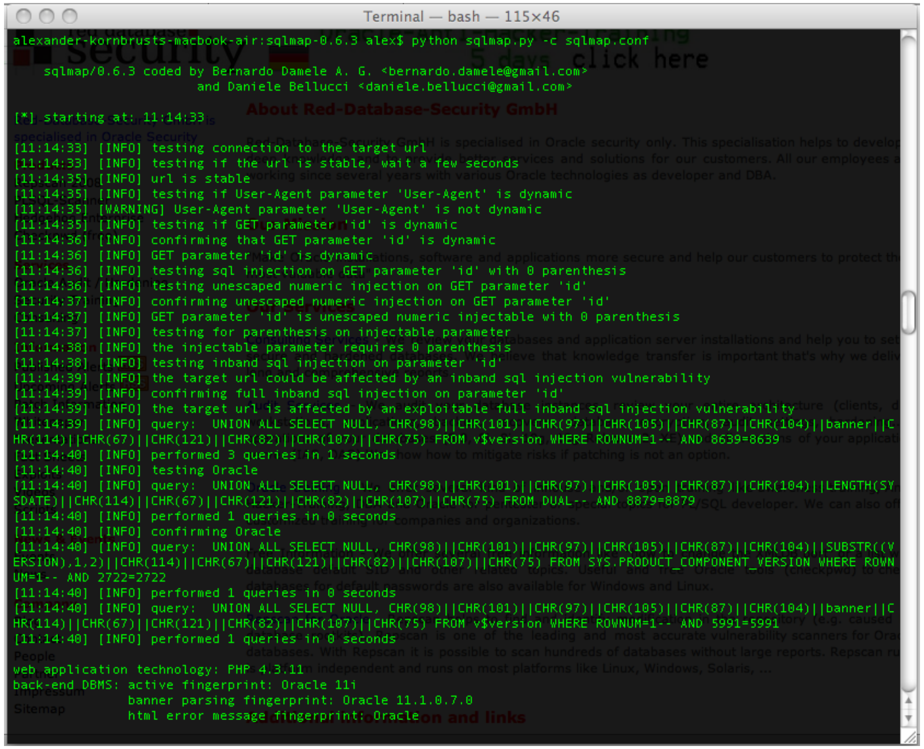
user	password
admin	5f4dcc3b5aa765d61d8327deb...
gordonb	e99a18c428cb38d5f2608536...
1337	f5ae2c3966d7e0d4f...
pablo	9f5bbe40cade3de5c...
smithy	5f4dcc3b5aa765d61d8327deb...

☑ Use Group_Concat (MySQL Only) ☑ All in one request

Status: I'm IDLE

```
Count(column_name) of information_schema.columns Where table_schema=0x64767761 AND table_na
Columns found: user_id,first_name,last_name,user,password,avatar
Count(*) of dvwa.users is 5
Data Found: user,password=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
```

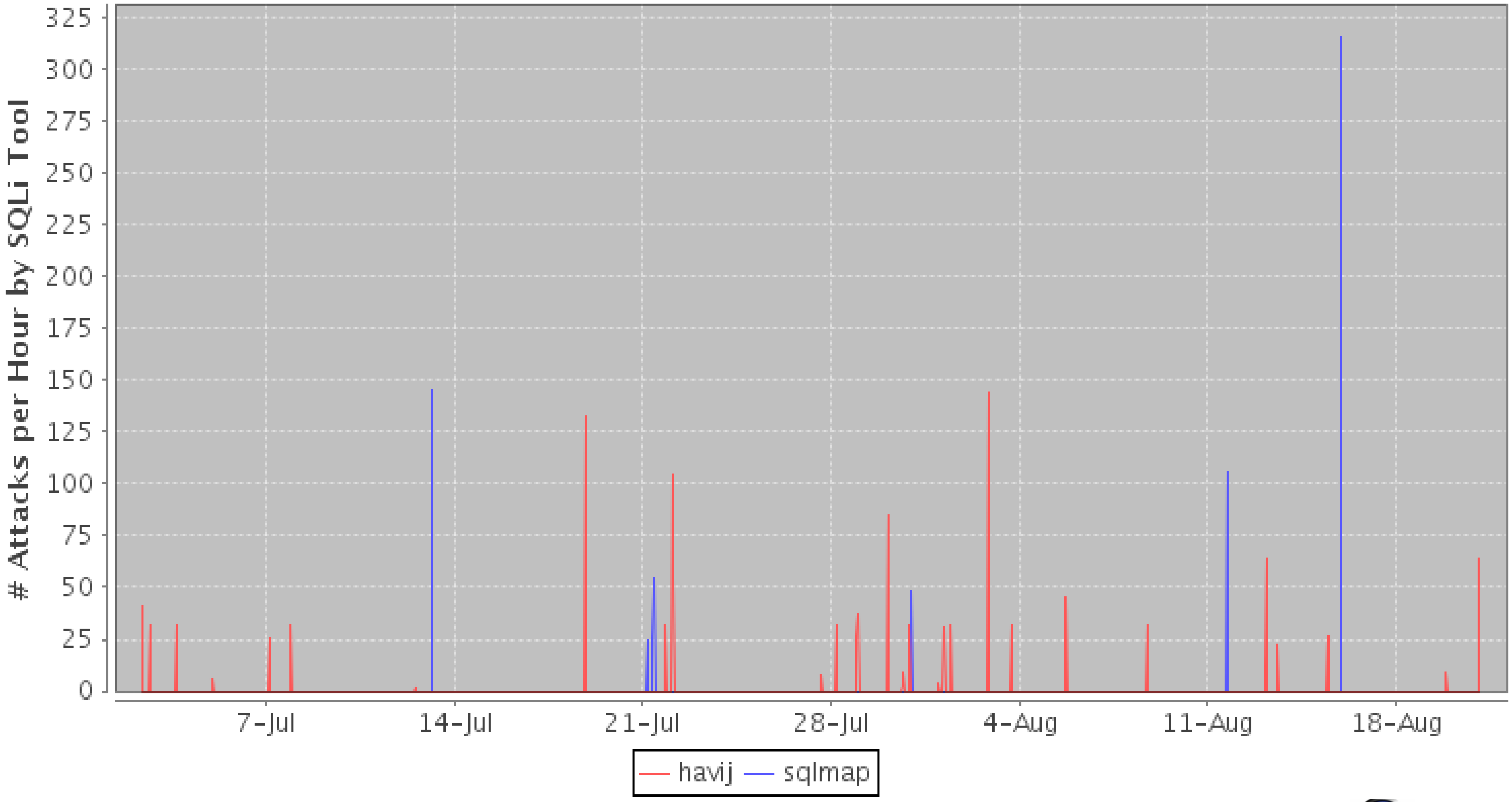
Havij



```
alexander-kornbrusts-macbook-air:sqlmap-0.6.3 alex$ python sqlmap.py -c sqlmap.conf

    sqlmap/0.6.3 coded by Bernardo Damele A. G. <bernardo.damele@gmail.com>
                          and Daniele Bellucci <daniele.bellucci@gmail.com>

[*] starting at: 11:14:33

[11:14:33] [INFO] testing connection to the target url
[11:14:33] [INFO] testing if the url is stable, wait a few seconds
[11:14:35] [INFO] url is stable
[11:14:35] [INFO] testing if User-Agent parameter 'User-Agent' is dynamic
[11:14:35] [WARNING] User-Agent parameter 'User-Agent' is not dynamic
[11:14:35] [INFO] testing if GET parameter 'id' is dynamic
[11:14:36] [INFO] confirming that GET parameter 'id' is dynamic
[11:14:36] [INFO] GET parameter 'id' is dynamic
[11:14:36] [INFO] testing sql injection on GET parameter 'id' with 0 parenthesis
[11:14:36] [INFO] testing unescaped numeric injection on GET parameter 'id'
[11:14:37] [INFO] confirming unescaped numeric injection on GET parameter 'id'
[11:14:37] [INFO] GET parameter 'id' is unescaped numeric injectable with 0 parenthesis
[11:14:37] [INFO] testing for parenthesis on injectable parameter
[11:14:38] [INFO] the injectable parameter requires 0 parenthesis
[11:14:38] [INFO] testing inband sql injection on parameter 'id'
[11:14:39] [INFO] the target url could be affected by an inband sql injection vulnerability
[11:14:39] [INFO] confirming full inband sql injection on parameter 'id'
[11:14:39] [INFO] the target url is affected by an exploitable full inband sql injection vulnerability
[11:14:39] [INFO] query:  UNION ALL SELECT NULL, CHR(98)||CHR(101)||CHR(97)||CHR(105)||CHR(87)||CHR(104)||banner||C
HR(114)||CHR(67)||CHR(121)||CHR(82)||CHR(107)||CHR(75) FROM v$version WHERE ROWNUM=1-- AND 8639=8639
[11:14:40] [INFO] performed 3 queries in 1 seconds
[11:14:40] [INFO] testing Oracle
[11:14:40] [INFO] query:  UNION ALL SELECT NULL, CHR(98)||CHR(101)||CHR(97)||CHR(105)||CHR(87)||CHR(104)||LENGTH(SY
SDATE)||CHR(114)||CHR(67)||CHR(121)||CHR(82)||CHR(107)||CHR(75) FROM DUAL-- AND 8879=8879
[11:14:40] [INFO] performed 1 queries in 0 seconds
[11:14:40] [INFO] confirming Oracle
[11:14:40] [INFO] query:  UNION ALL SELECT NULL, CHR(98)||CHR(101)||CHR(97)||CHR(105)||CHR(87)||CHR(104)||SUBSTR((V
ERSION),1,2)||CHR(114)||CHR(67)||CHR(121)||CHR(82)||CHR(107)||CHR(75) FROM SYS.PRODUCT_COMPONENT_VERSION WHERE ROWN
UM=1-- AND 2722=2722
[11:14:40] [INFO] performed 1 queries in 0 seconds
[11:14:40] [INFO] query:  UNION ALL SELECT NULL, CHR(98)||CHR(101)||CHR(97)||CHR(105)||CHR(87)||CHR(104)||banner||C
HR(114)||CHR(67)||CHR(121)||CHR(82)||CHR(107)||CHR(75) FROM v$version WHERE ROWNUM=1-- AND 5991=5991
[11:14:40] [INFO] performed 1 queries in 0 seconds

web application technology: PHP 4.3.11
back-end DBMS: active fingerprint: Oracle 11i
               banner parsing fingerprint: Oracle 11.1.0.7.0
               html error message fingerprint: Oracle
```

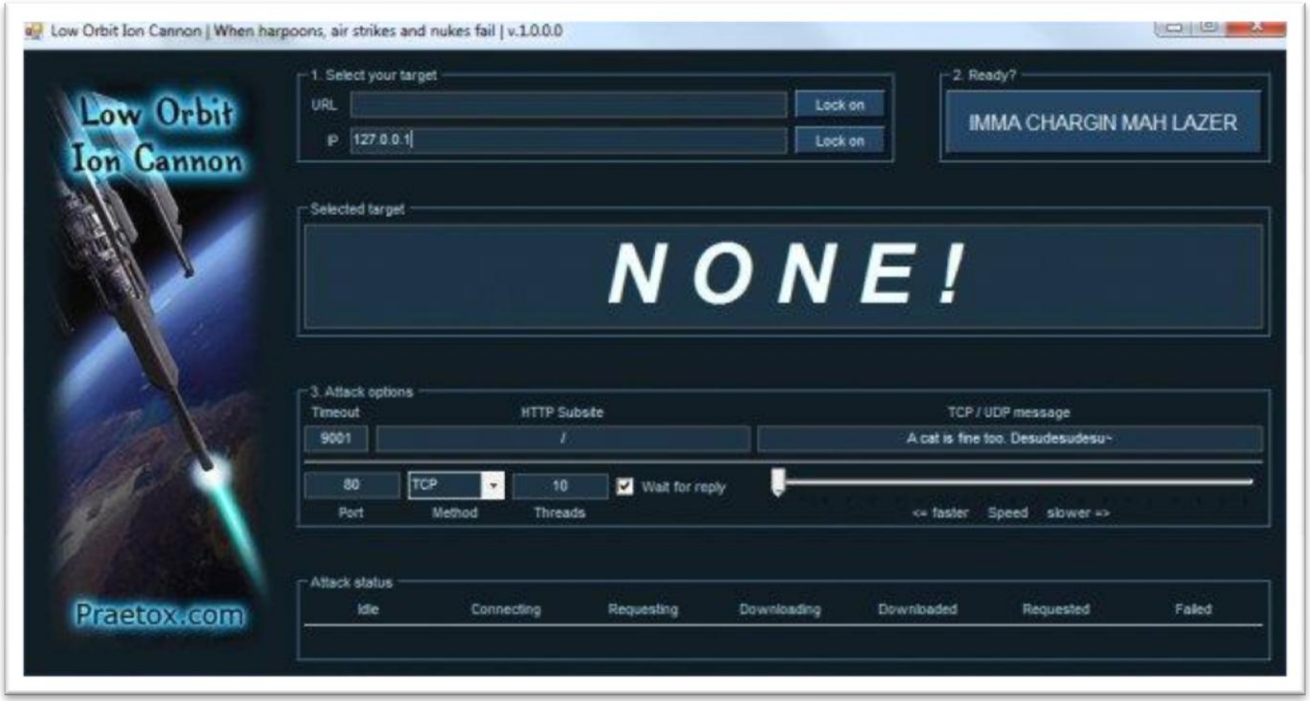
SQLMap

Attacks from Automated Tools



OWASP

Low Orbit Ion Cannon



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fail | v.1.0.0.0

1. Select your target

URL

IP 127.0.0.1

2. Ready?

Selected target

NONE!

3. Attack options

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: A cat is fine too. Desudesudesu~

Port: 80

Method: TCP

Threads: 10

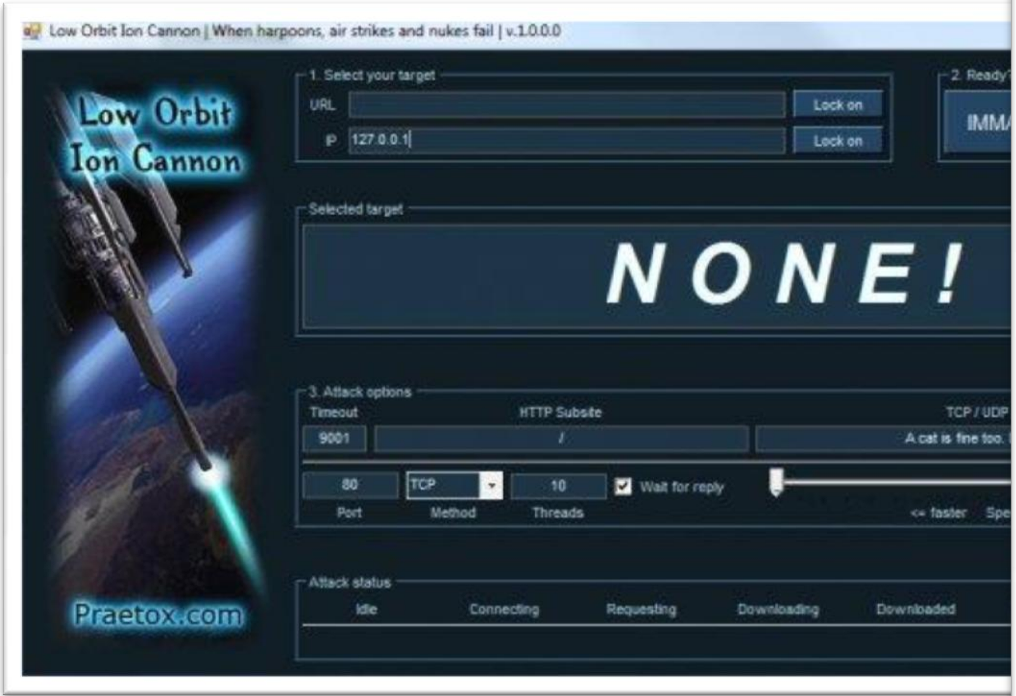
☑ Wait for reply

<= faster Speed slower =>

Attack status

Idle Connecting Requesting Downloading Downloaded Requested Failed

Low Orbit Ion Cannon

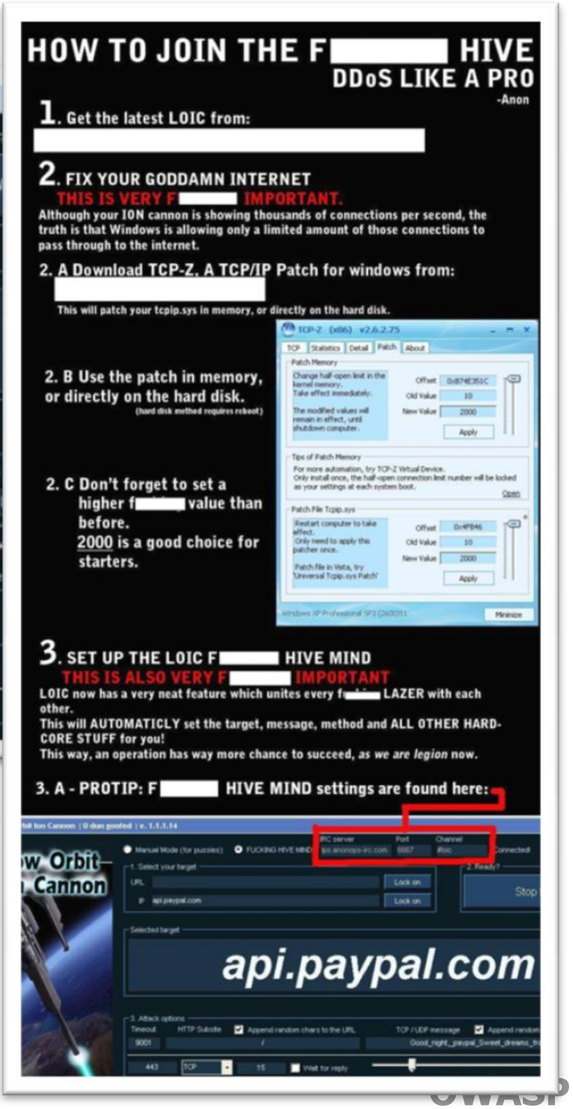

Low Orbit Ion Cannon | When harpoons, air strikes and nukes fail | v.1.0.0.0

1. Select your target
URL
IP 127.0.0.1

Selected target
NONE!

3. Attack options
Timeout 9001
HTTP Subsite /
TCP / UDP message: A cat is fine too.
Port 80
Method TCP
Threads 10
☑ Wait for reply

Attack status
Idle Connecting Requesting Downloading Downloaded


HOW TO JOIN THE F[redacted] HIVE

DDoS LIKE A PRO

-Anon

1. Get the latest LOIC from:
[redacted]

2. FIX YOUR GODDAMN INTERNET

THIS IS VERY F[redacted] IMPORTANT.

Although your ION cannon is showing thousands of connections per second, the truth is that Windows is allowing only a limited amount of those connections to pass through to the internet.

2. A Download TCP-Z, A TCP/IP Patch for windows from:
[redacted]

This will patch your tcpip.sys in memory, or directly on the hard disk.

2. B Use the patch in memory, or directly on the hard disk.
(hard disk method requires reboot)

2. C Don't forget to set a higher f[redacted] value than before.
2000 is a good choice for starters.

TCP-Z (x86) v2.6.2.75

Patch Memory
Change half-open limit in the kernel memory.
Take effect immediately.
The modified values will remain in effect, until shutdown computer.
Offset 0x874E351C
Old Value 10
New Value 2000

Tips of Patch Memory
For more automation, try TCP-Z Virtual Device.
Only install once, the half-open connection limit number will be locked as your settings at each system boot.

Patch File Tcpip.sys
Restart computer to take effect.
Only need to apply this patcher once.
Patch file in Vista, try 'Universal Tcpip.sys Patch'
Offset 0x4F846
Old Value 10
New Value 2000

Windows XP Professional SP3 (2600)

3. SET UP THE LOIC F[redacted] HIVE MIND

THIS IS ALSO VERY F[redacted] IMPORTANT

LOIC now has a very neat feature which unites every f[redacted] LAZER with each other.
This will AUTOMATICLY set the target, message, method and ALL OTHER HARD-CORE STUFF for you!
This way, an operation has way more chance to succeed, *as we are legion* now.

3. A - PROTIP: F[redacted] HIVE MIND settings are found here:

...bit Ion Cannon | U dun goofed | v. 1.1.1.14

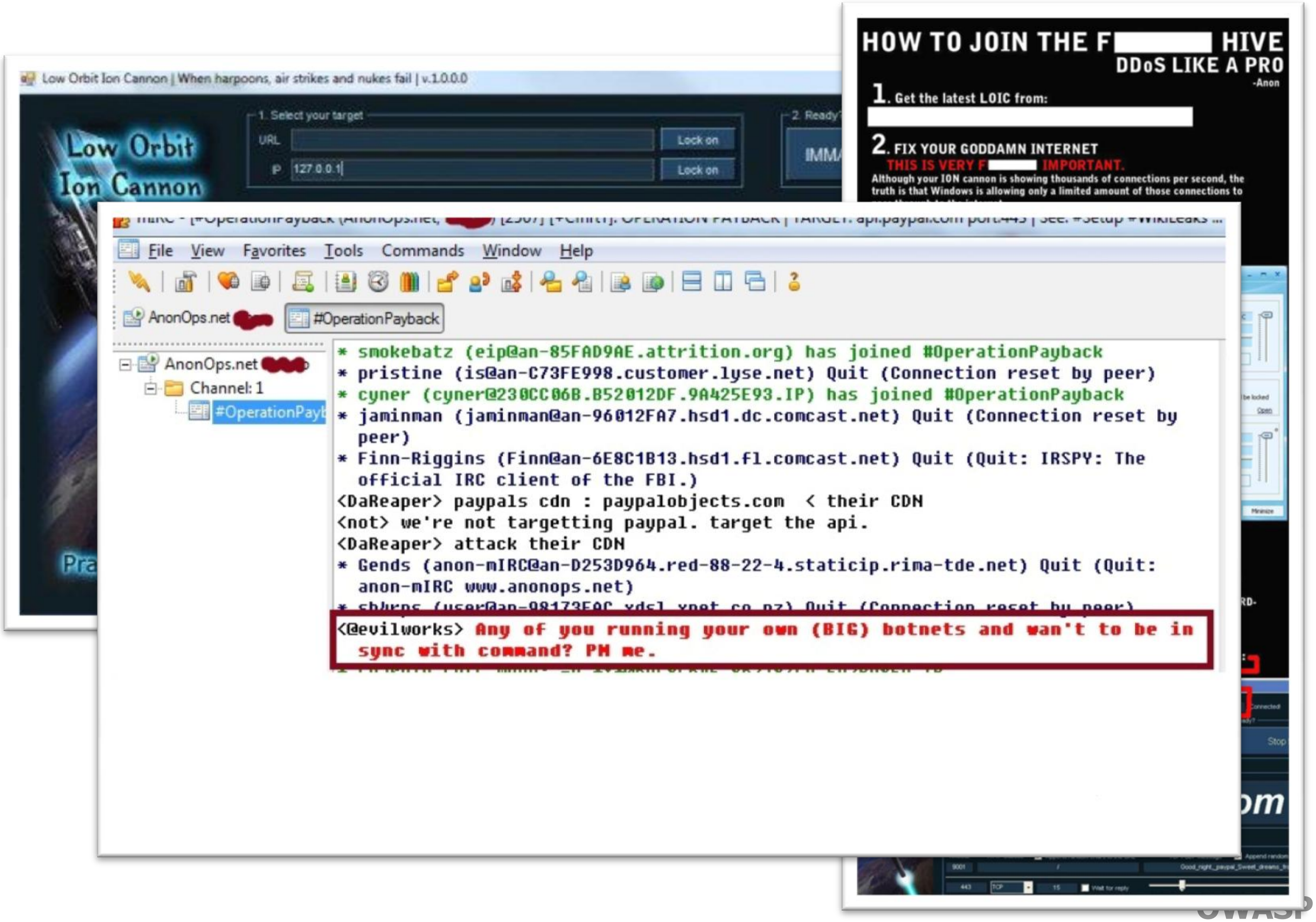
○ Manual Mode (for pussies) ● FUCKING HIVE MIND
IRC server irc.anonops-irc.com
Port 6667
Channel #loic
Connected

1. Select your target
URL
IP api.paypal.com

Selected target
api.paypal.com

3. Attack options
Timeout 9001
HTTP Subsite /
☑ Append random chars to the URL
TCP / UDP message Good_night_paypal_Sweet_dreams_fr...
☑ Append random
Port 443
Method TCP
Threads 15
□ Wait for reply

Low Orbit Ion Cannon



HOW TO JOIN THE F[redacted] HIVE
DDoS LIKE A PRO
-Anon

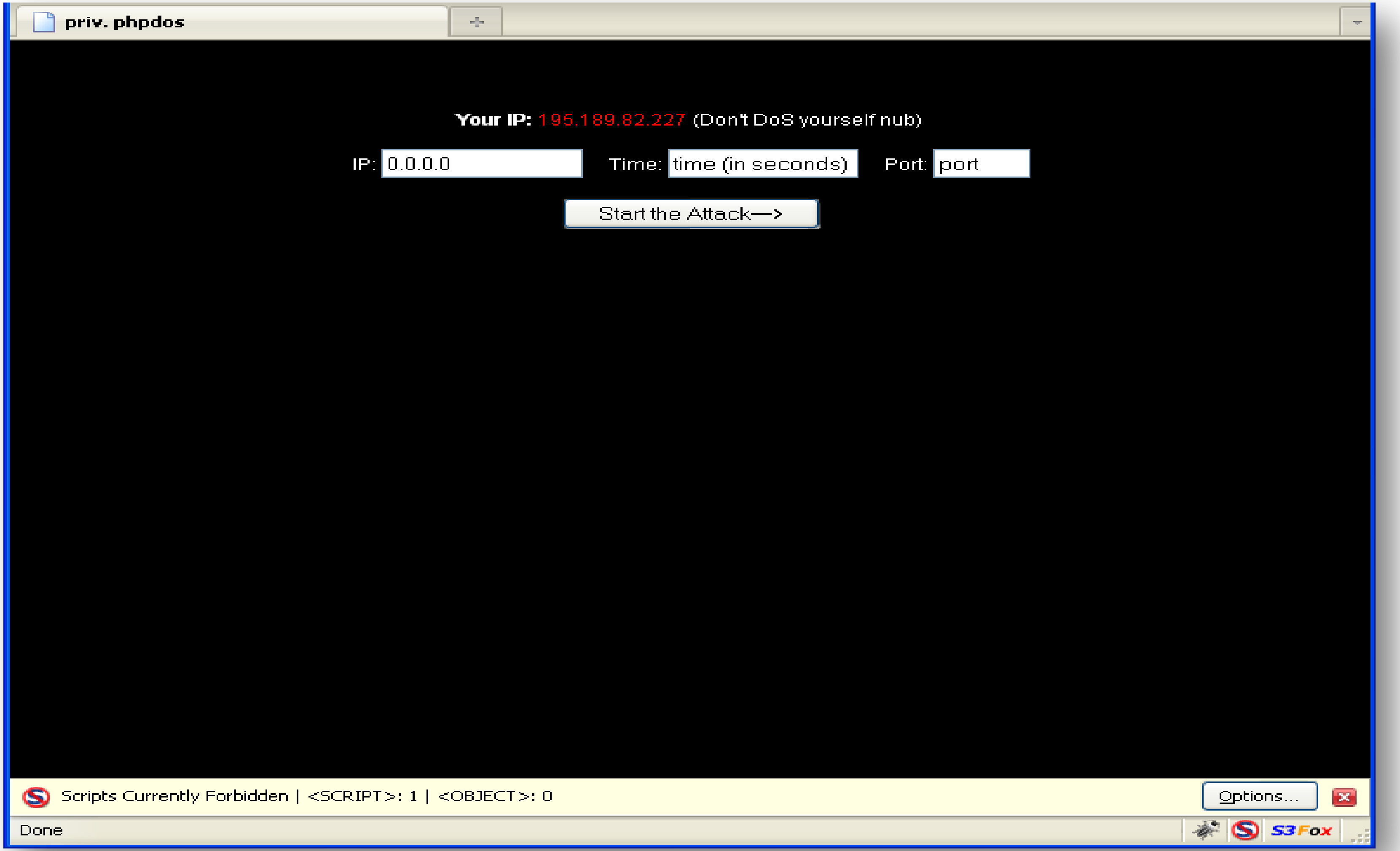
1. Get the latest LOIC from:
[redacted]

2. FIX YOUR GODDAMN INTERNET
THIS IS VERY F[redacted] IMPORTANT.
Although your ION cannon is showing thousands of connections per second, the truth is that Windows is allowing only a limited amount of those connections to

mIRC - [#OperationPayback (AnonOps.net, [redacted]) [2367] [+Cmnt]: OPERATION PAYBACK | TARGET: api.paypal.com port:443 | See: #setup #WikiLeaks ...

```
* smokebatz (eip@an-85FAD9AE.attrition.org) has joined #OperationPayback
* pristine (is@an-C73FE998.customer.lyse.net) Quit (Connection reset by peer)
* cyner (cyner@230CC06B.B52012DF.9A425E93.IP) has joined #OperationPayback
* jaminman (jaminman@an-96012FA7.hsd1.dc.comcast.net) Quit (Connection reset by
  peer)
* Finn-Riggins (Finn@an-6E8C1B13.hsd1.fl.comcast.net) Quit (Quit: IRSPY: The
  official IRC client of the FBI.)
<DaReaper> paypals cdn : paypalobjects.com  < their CDN
<not> we're not targetting paypal. target the api.
<DaReaper> attack their CDN
* Gends (anon-mIRC@an-D253D964.red-88-22-4.staticip.rima-tde.net) Quit (Quit:
  anon-mIRC www.anonops.net)
* sh/rps (user@an-98173FAC.xdsl.xnet.co.nz) Quit (Connection reset by peer)
<@evilworks> Any of you running your own (BIG) botnets and wan't to be in
  sync with command? PM me.
```

DDoS 2.0



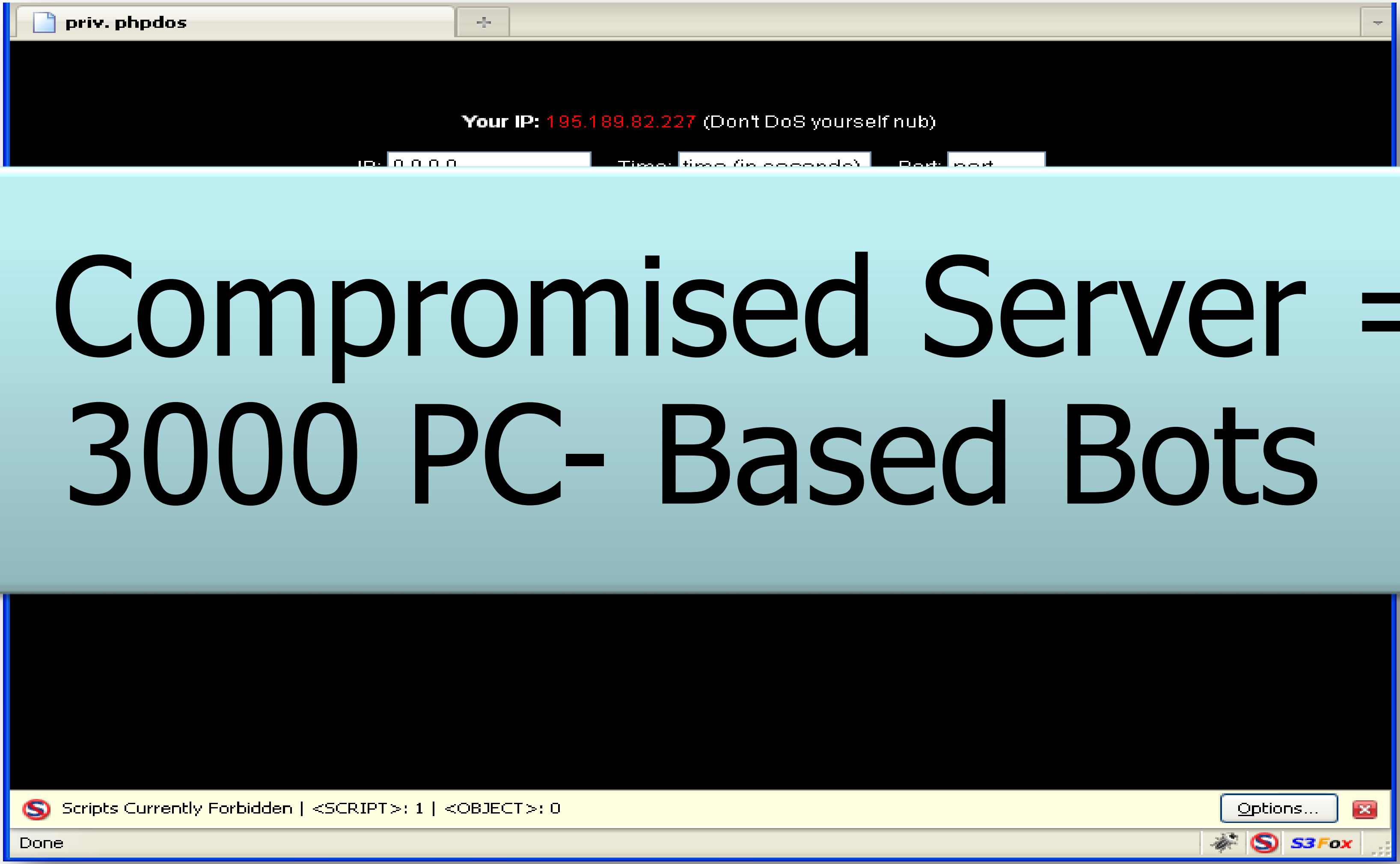
Your IP: 195.189.82.227 (Don't DoS yourself nub)

IP: 0.0.0.0 Time: time (in seconds) Port: port

Scripts Currently Forbidden | <SCRIPT>: 1 | <OBJECT>: 0

Done

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

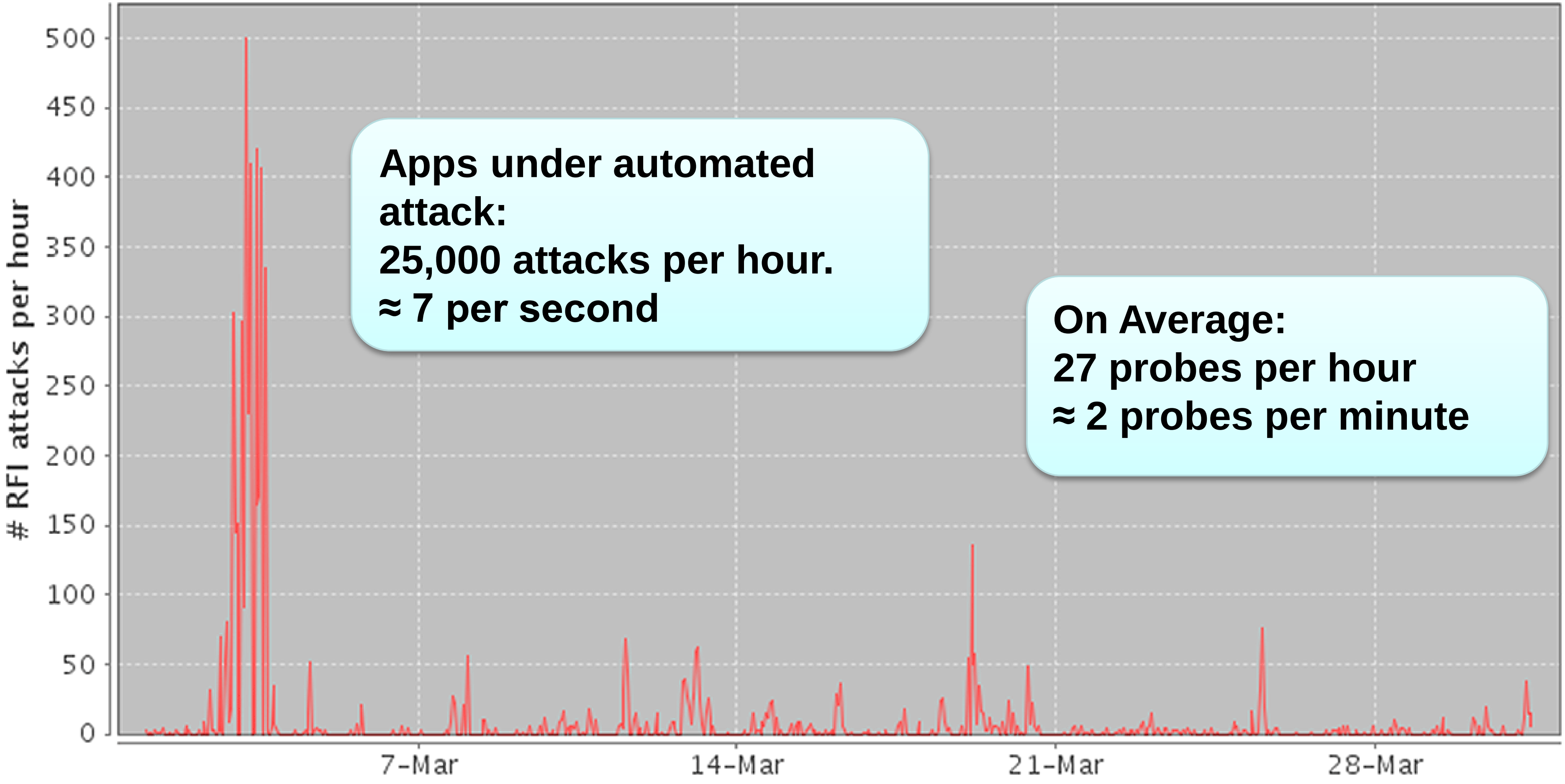
Scripts Currently Forbidden | <SCRIPT>: 1 | <OBJECT>: 0

1 Compromised Server = 3000 PC- Based Bots

What are Hackers Hacking?

PART III: MONITORING TRAFFIC

Lesson #1: Automation is Prevailing

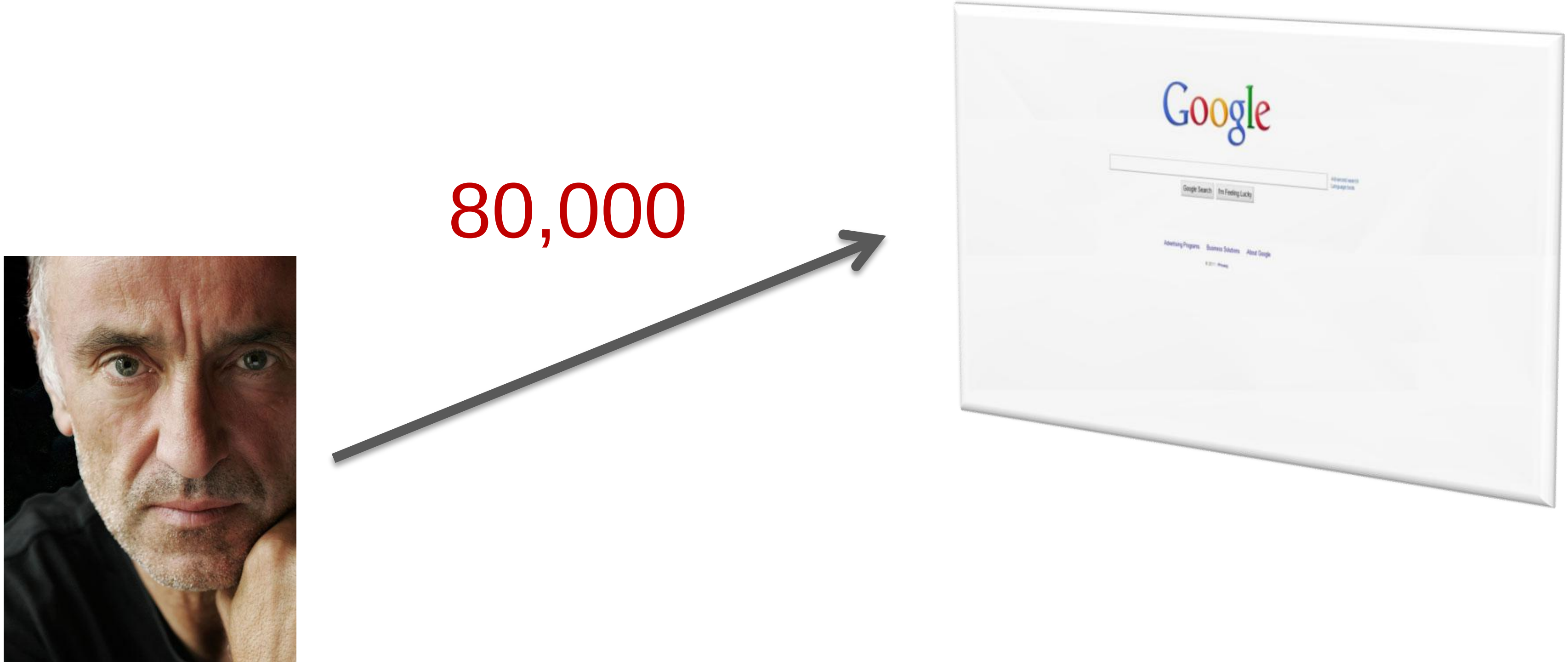


Apps under automated attack:
25,000 attacks per hour.
≈ 7 per second

On Average:
27 probes per hour
≈ 2 probes per minute

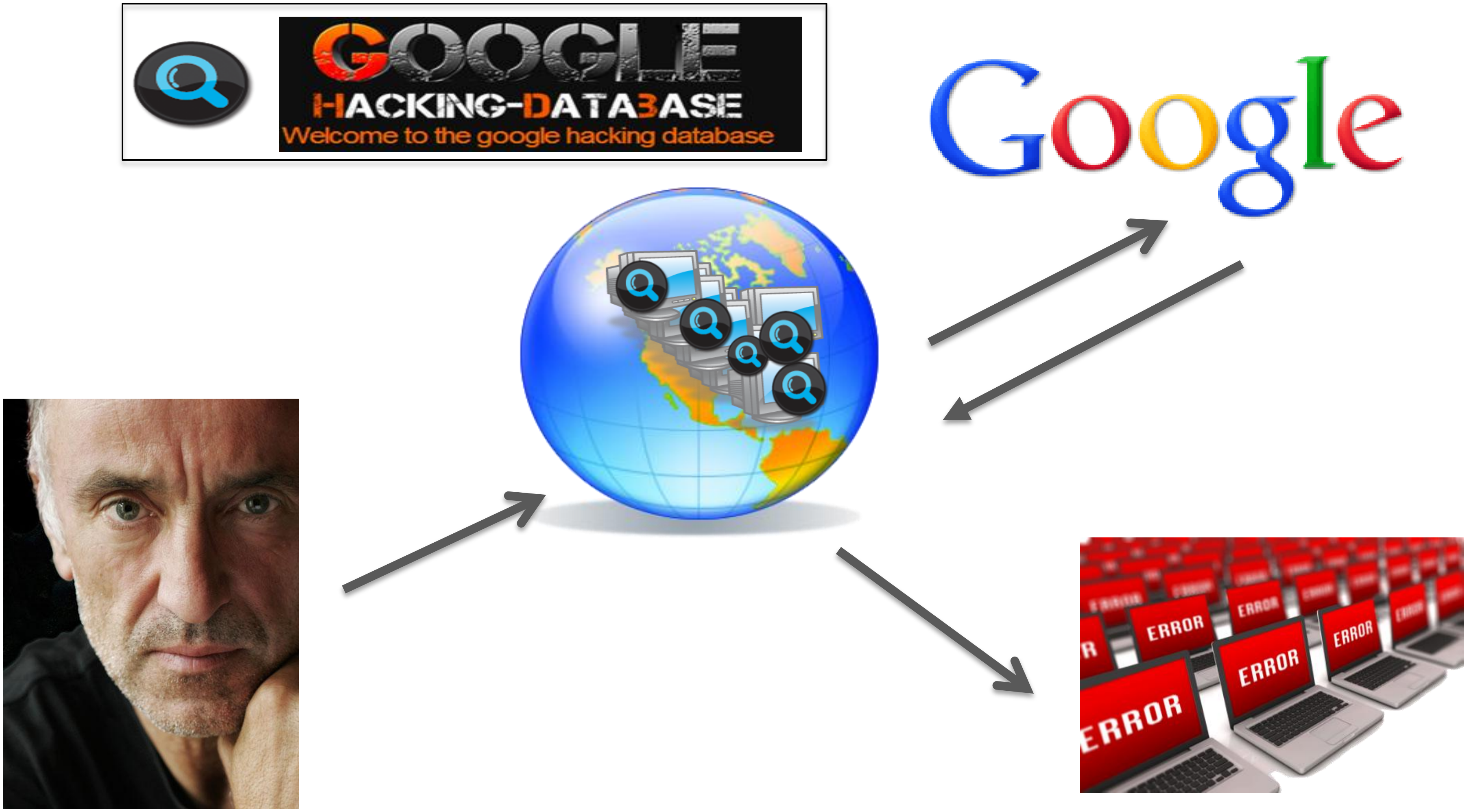
Lesson #1: Automation is Prevailing

- Example: Google Dorks Campaign

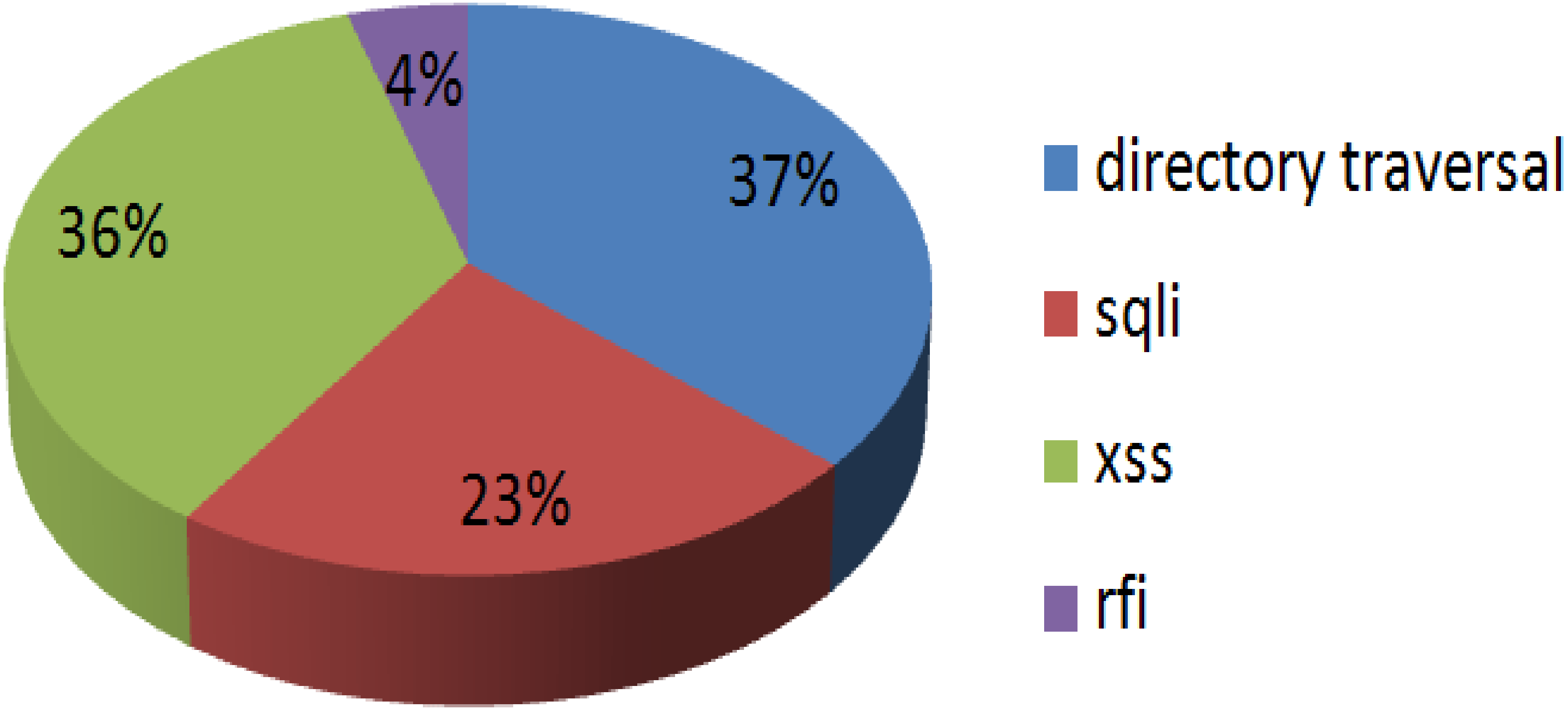


80,000

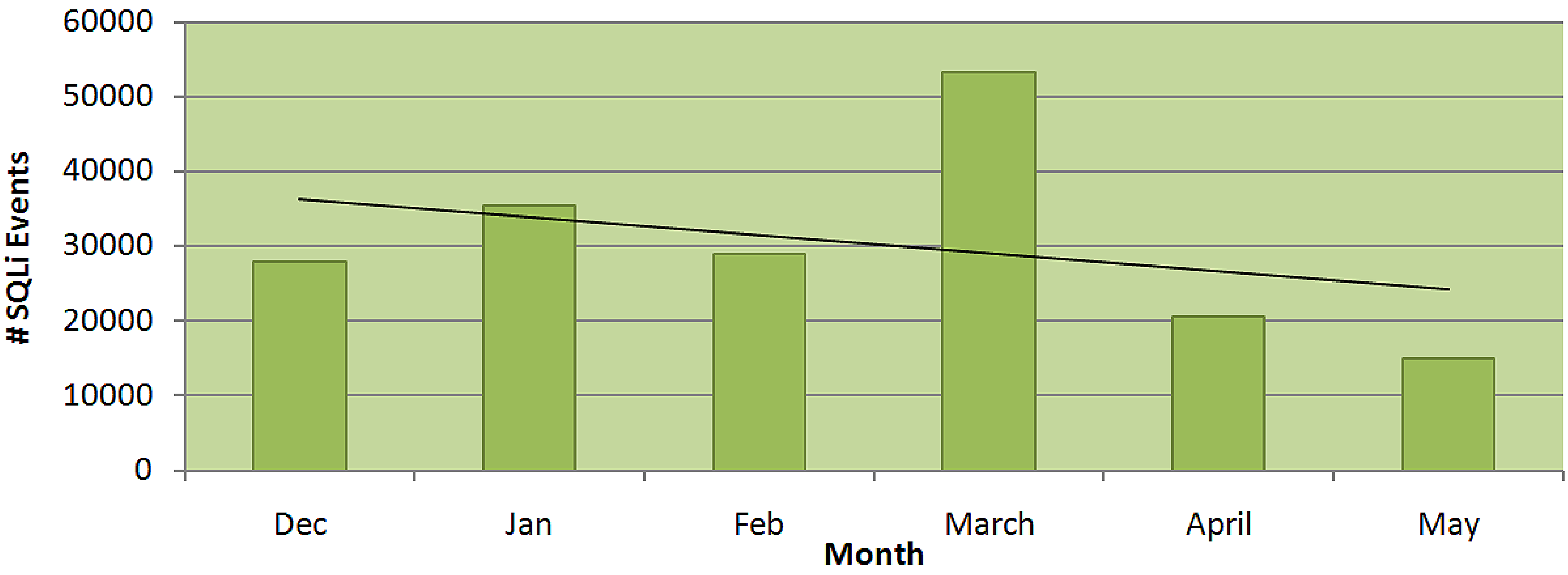
Lesson #1: Automation is Prevailing



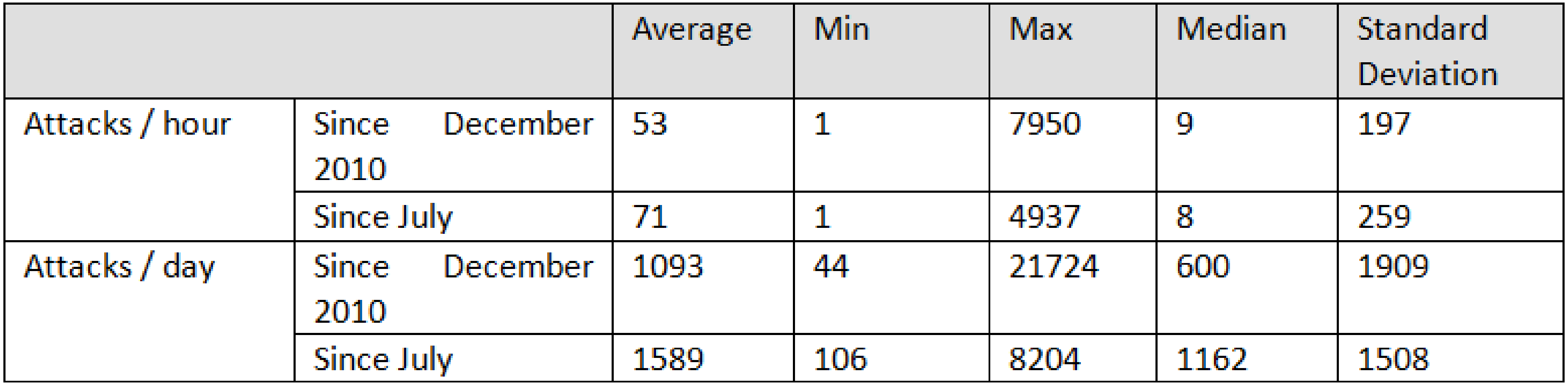
Lesson #2: The Unfab Four



Lesson #2A: The Unfab Four, SQL Injection



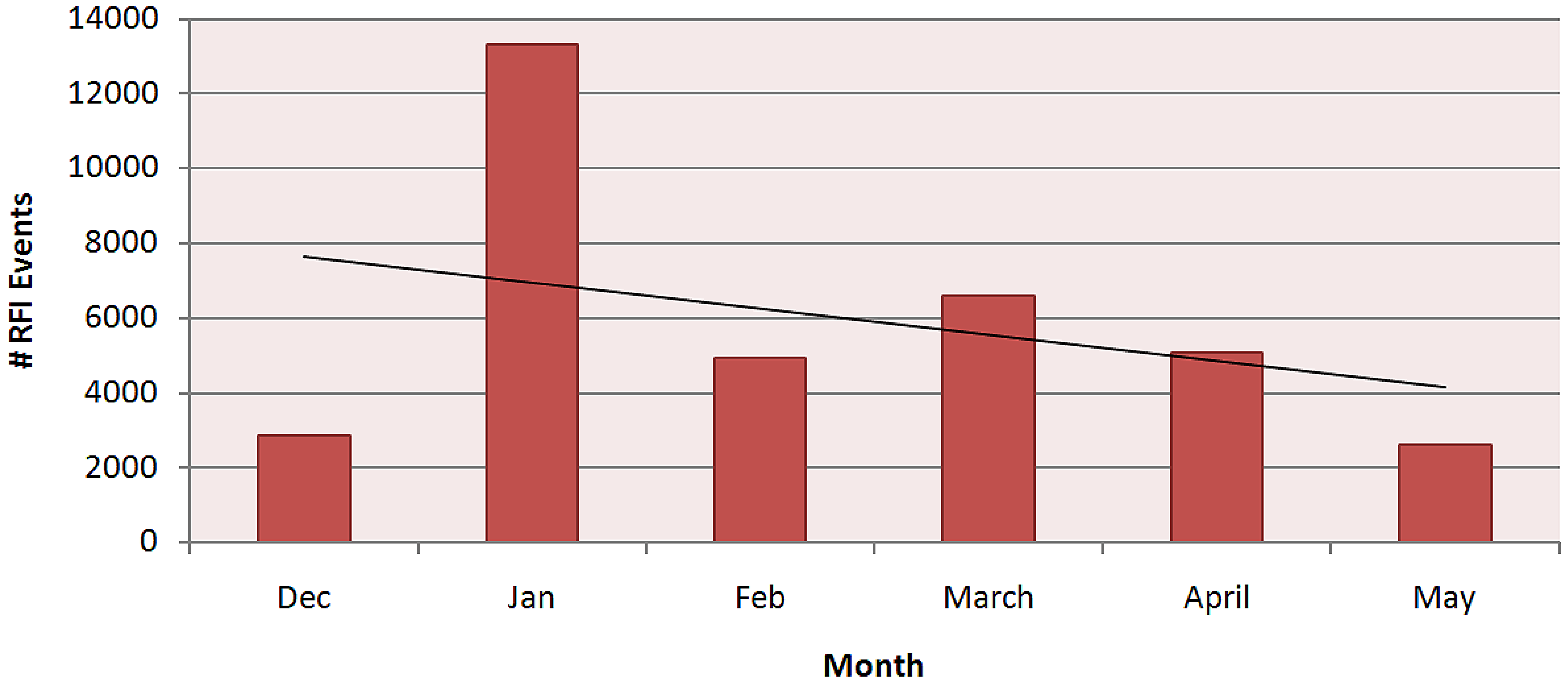
Lesson #2A: The Unfab Four, SQL Injection



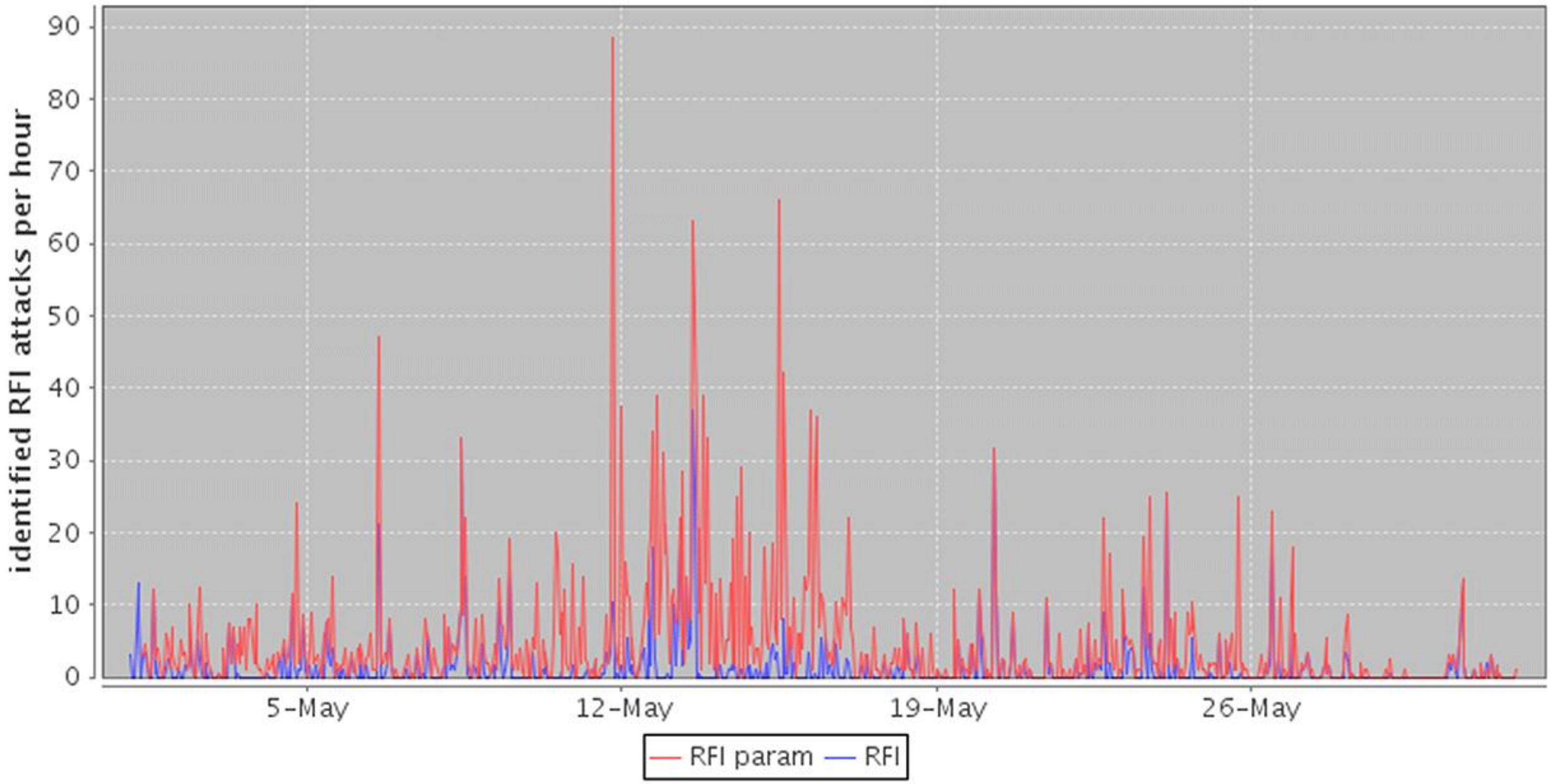
		Average	Min	Max	Median	Standard Deviation
Attacks / hour	Since December 2010	53	1	7950	9	197
	Since July	71	1	4937	8	259
Attacks / day	Since December 2010	1093	44	21724	600	1909
	Since July	1589	106	8204	1162	1508

Table 1 : Statistics of SQLi occurrences

Lesson #2B: The Unfab Four, RFI

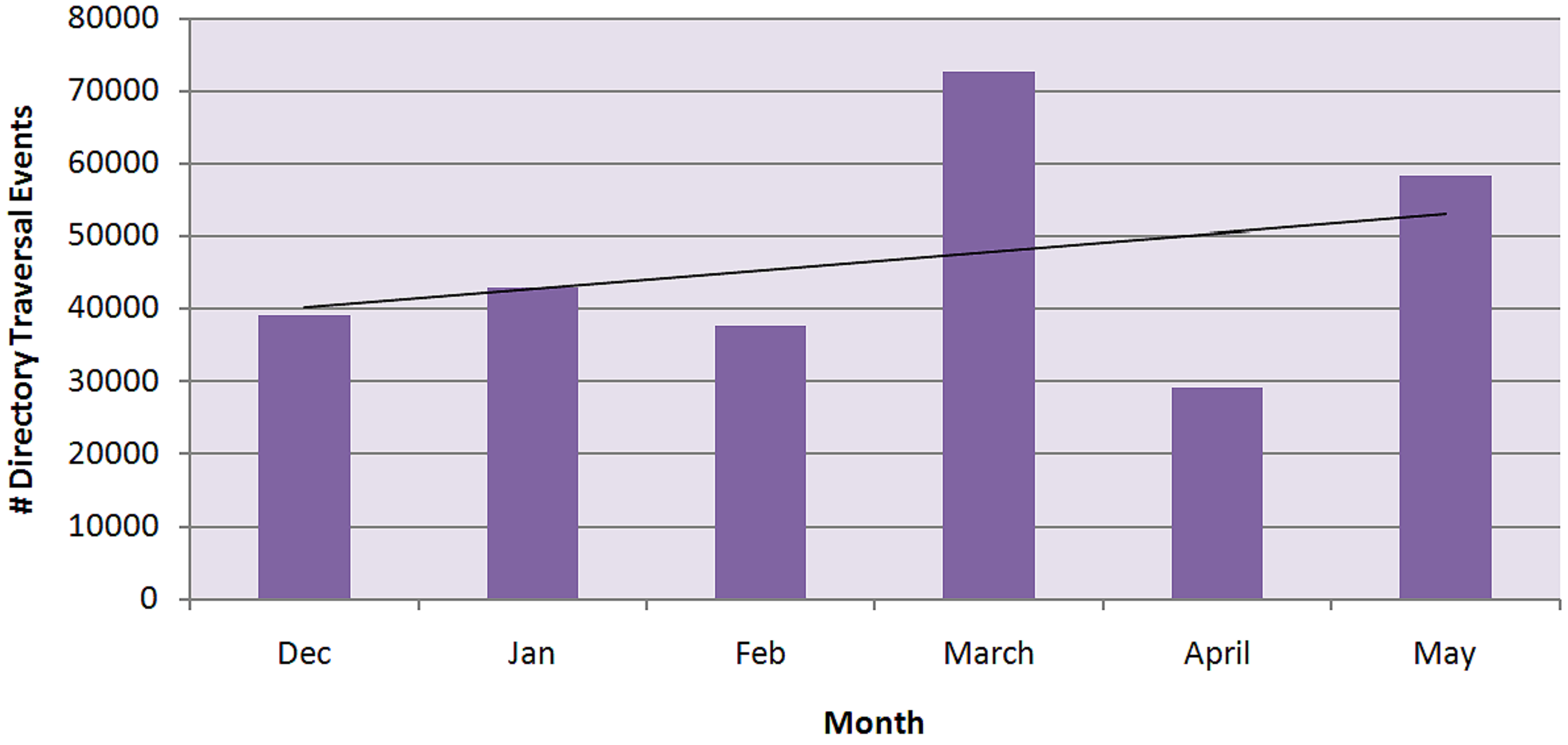


Lesson #2B: The Unfab Four, RFI

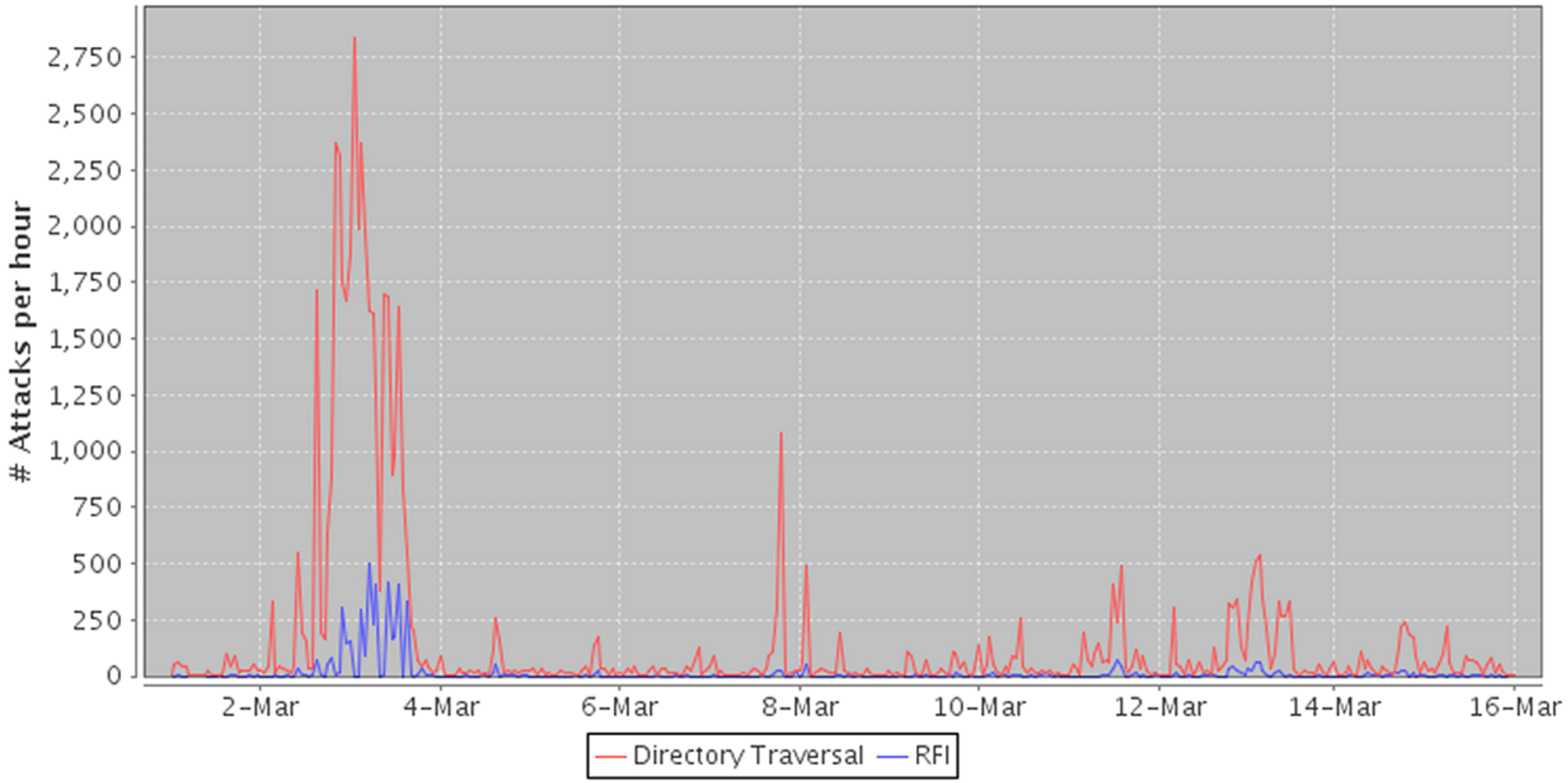


Analyzing the parameters and source of an RFI attack enhances common signature-based attack detection.

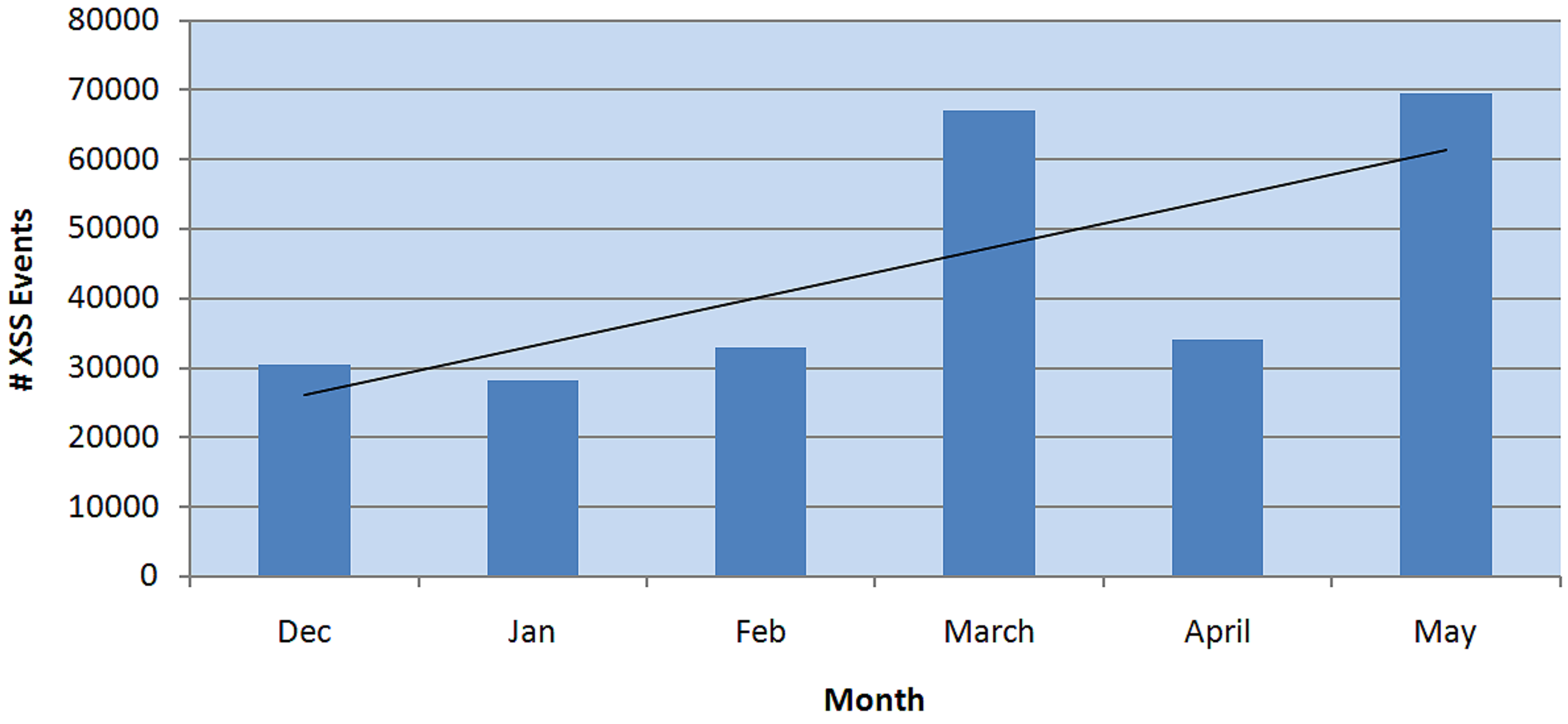
Lesson #2C: The Unfab Four, Directory Traversal



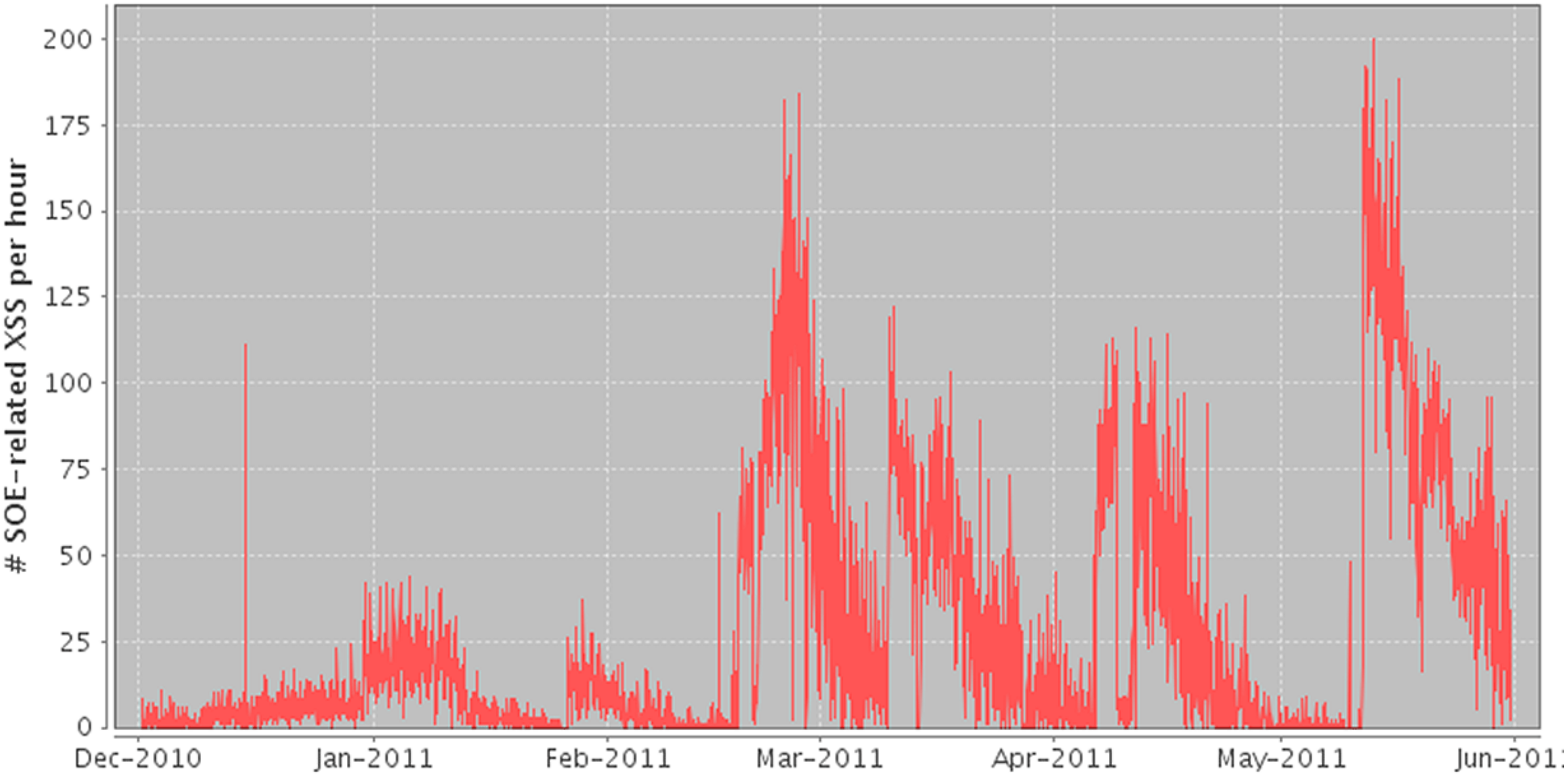
Lesson #2C: The Unfab Four, Directory Traversal



Lesson #2D: The Unfab Four, XSS

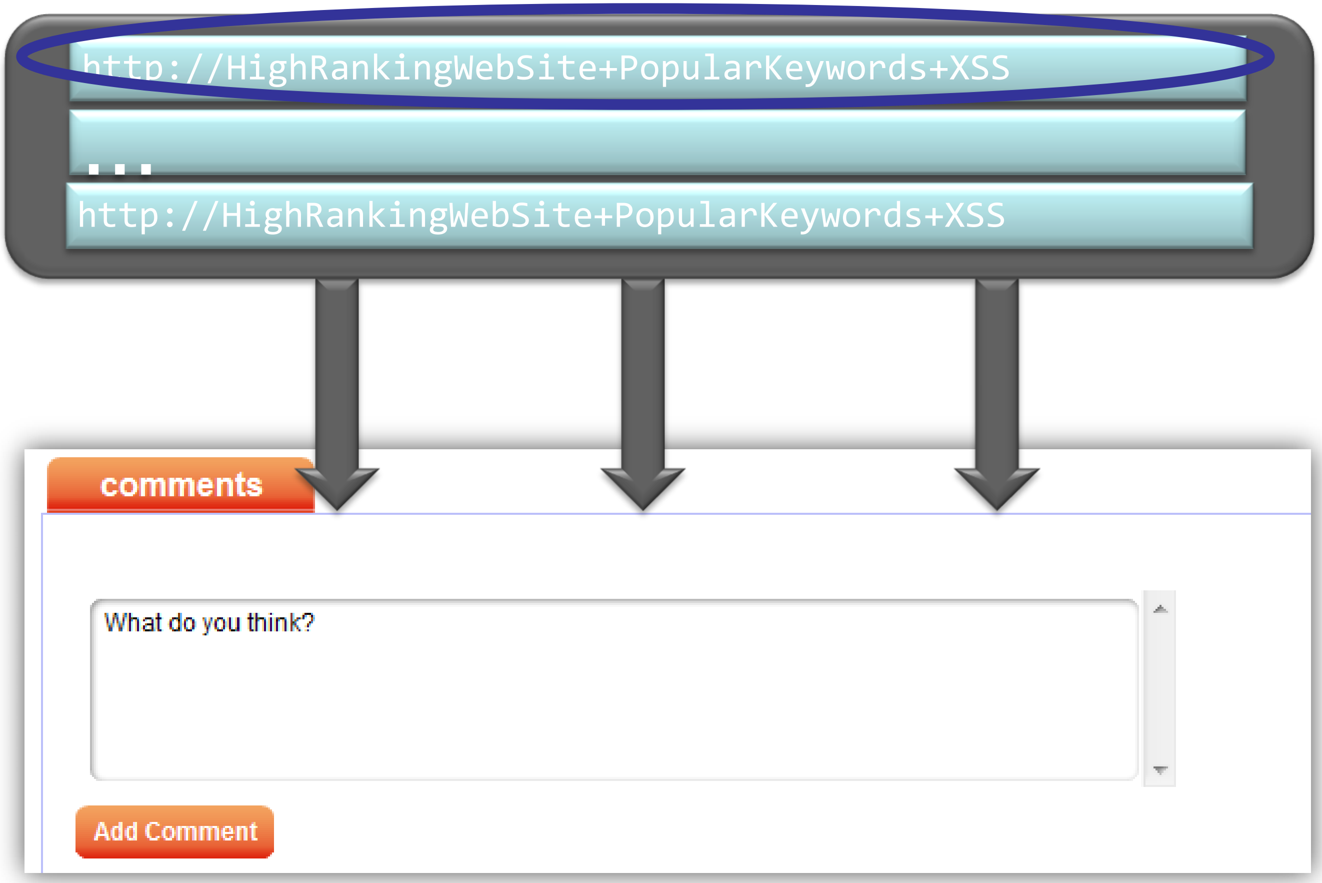


Lesson #2D: The Unfab Four, XSS

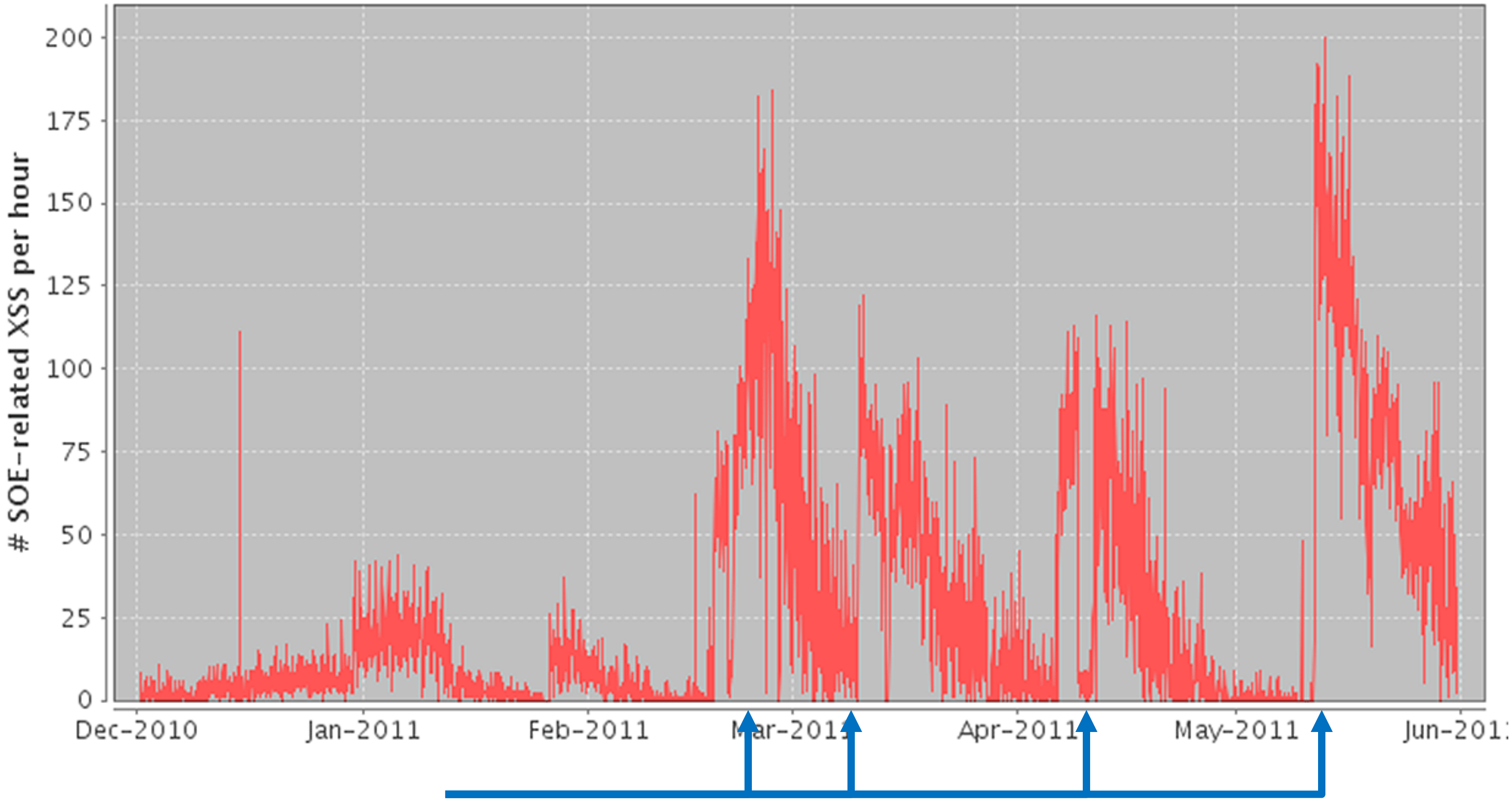


Lesson #2D: The Unfab Four

XSS: Zooming into Search Engine Poisoning

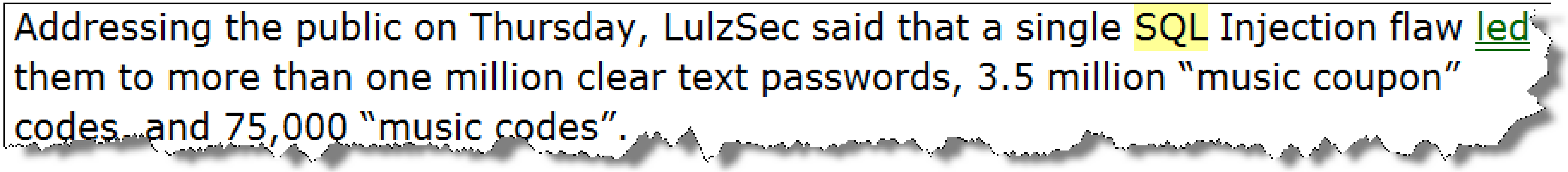

http://HighRankingWebSite+PopularKeywords+XSS
...
http://HighRankingWebSite+PopularKeywords+XSS
comments
What do you think?
Add Comment

Lesson #2D: The Unfab Four, XSS

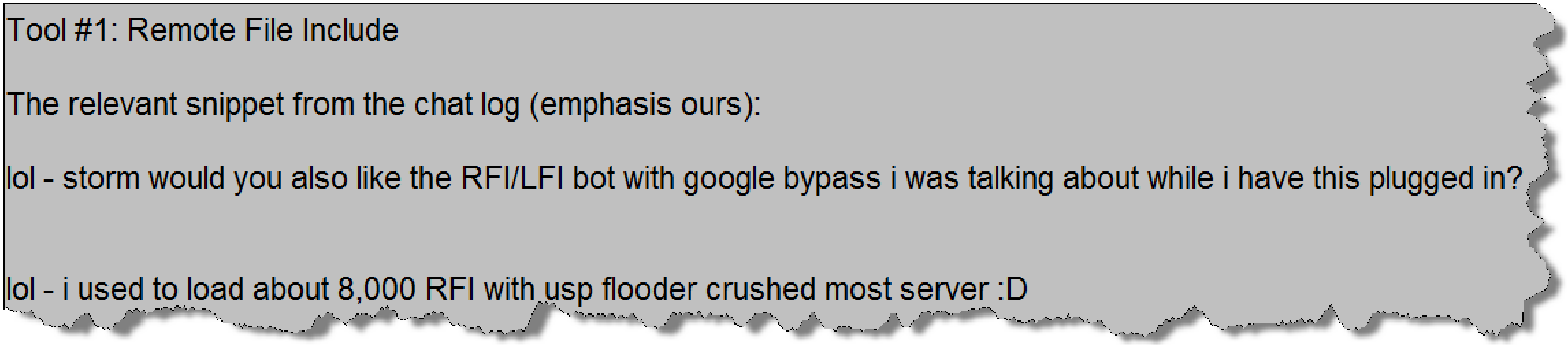


New Search Engine Indexing Cycle

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”.

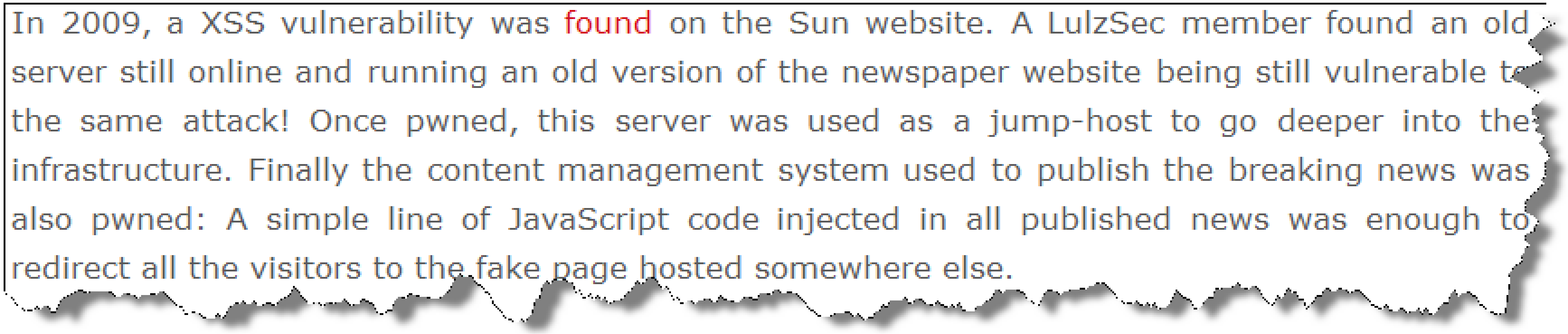


Tool #1: Remote File Include

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?

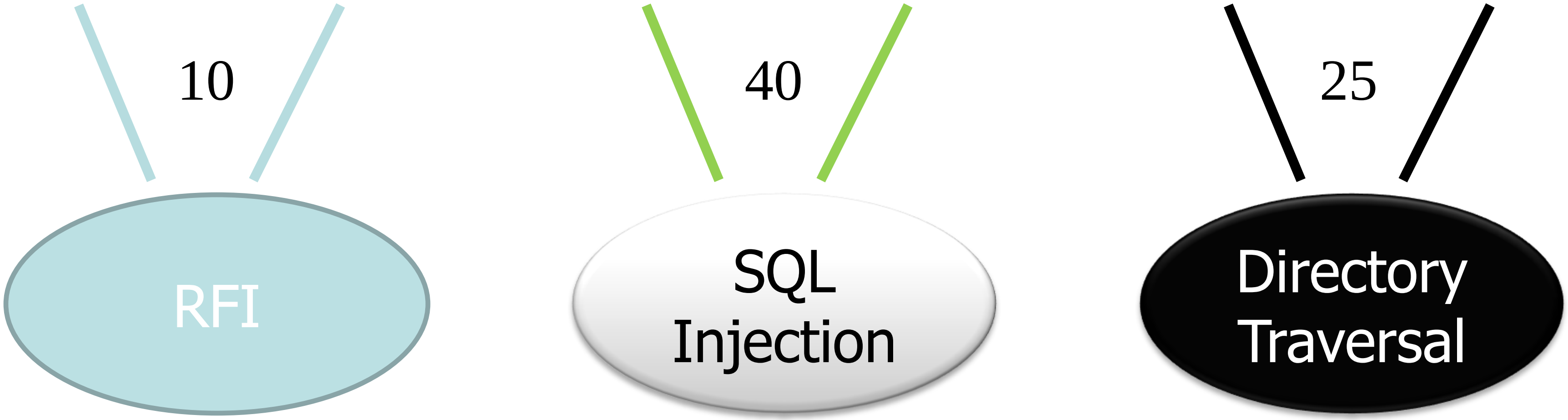
lol - i used to load about 8,000 RFI with usp flooder crushed most server :D



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



10

RFI

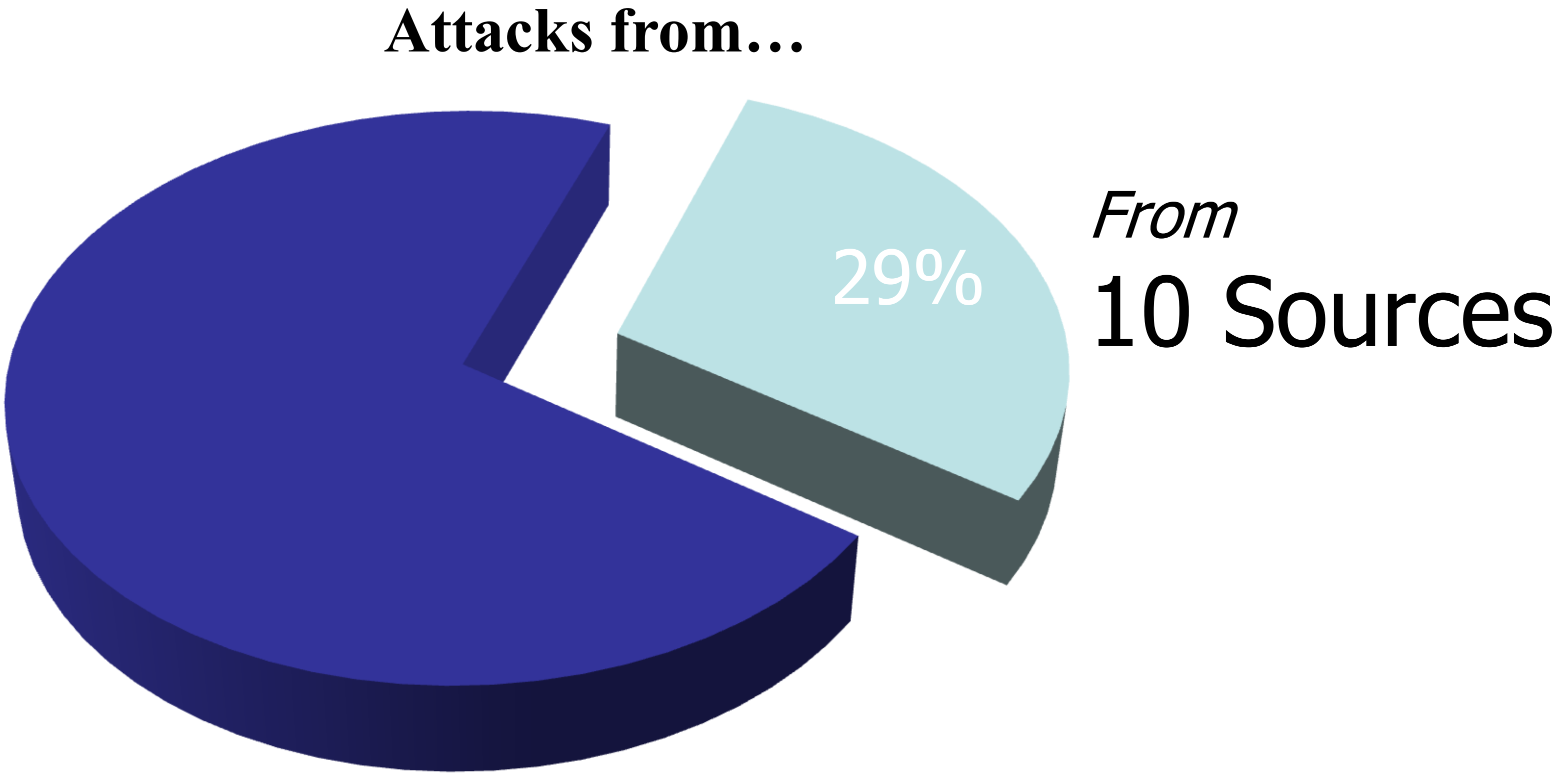
40

SQL Injection

25

Directory Traversal

Lesson #3: Repeating Offenders

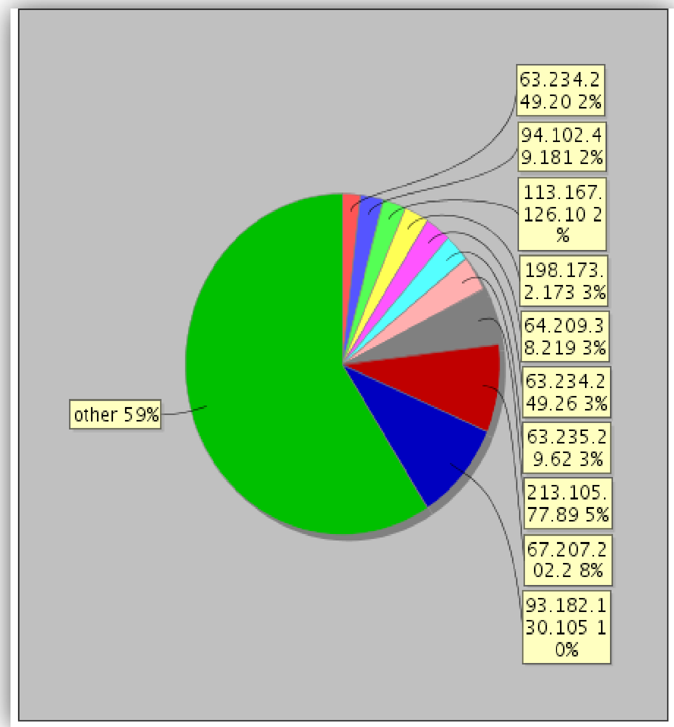


MITIGATION

Step 1: Dork Yourself (for SQL injection)

- Put detection policies in place (using the data source monitoring solution) to depict move of sensitive data to public facing servers.
- Regularly schedule “clean ups”. Every once in a while, a clean-up should be scheduled in order to verify that no sensitive data resides in these publicly accessible servers.
- Periodically look for new data stores that hold sensitive data. Tools exist today to assist in the task of detecting database servers in the network and classifying their contents.

Step 2: Create and deploy a blacklist of hosts that initiated attacks

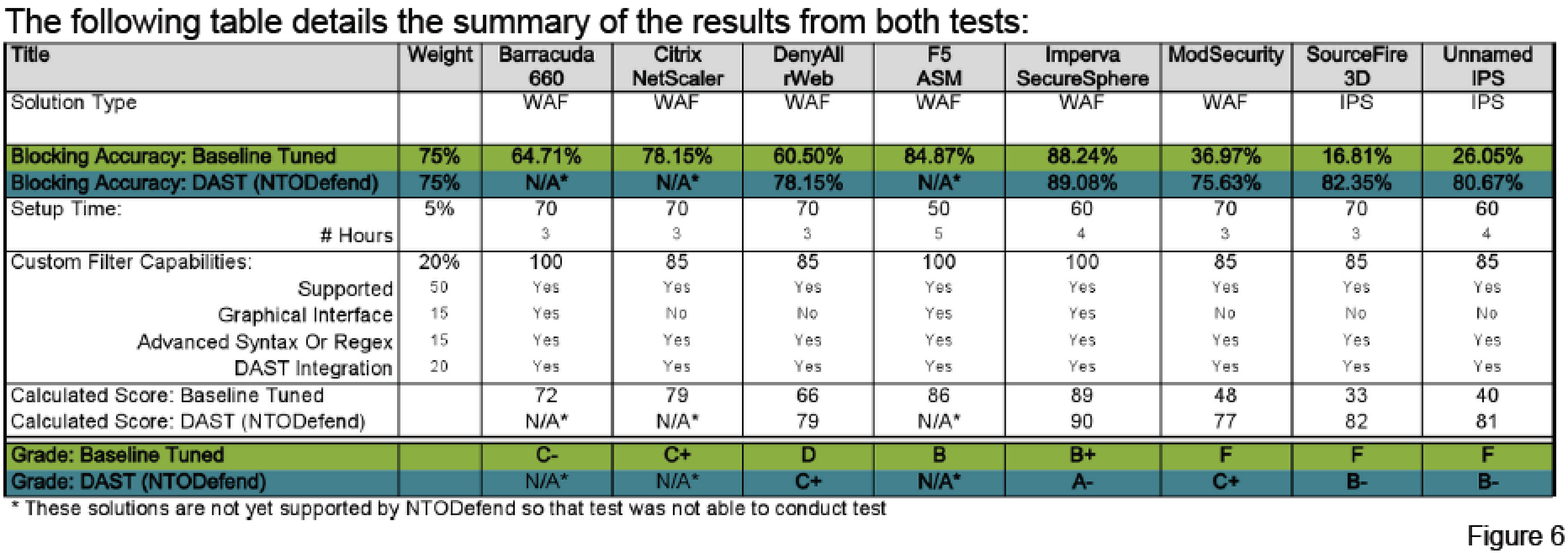


- Blacklisting of: compromised servers, botnet Command and Control (C&C) servers, infected devices, active spam sources, crawlers to acquire intelligence on malicious sources and apply it in real time
- Participate in a security community and share data on attacks
  - Some of the attacks' scanning is horizontal across similar applications on the internet.
- Sort traffic based on reputation
- Whitelisting of: legitimate search engine bots, aggregators

Step 3: Use a WAF to detect/block attacks

- Can block many attacks
- Relatively easy
- Can accelerate SDLC
- Not all WAFs created equal

WAFs in Reality



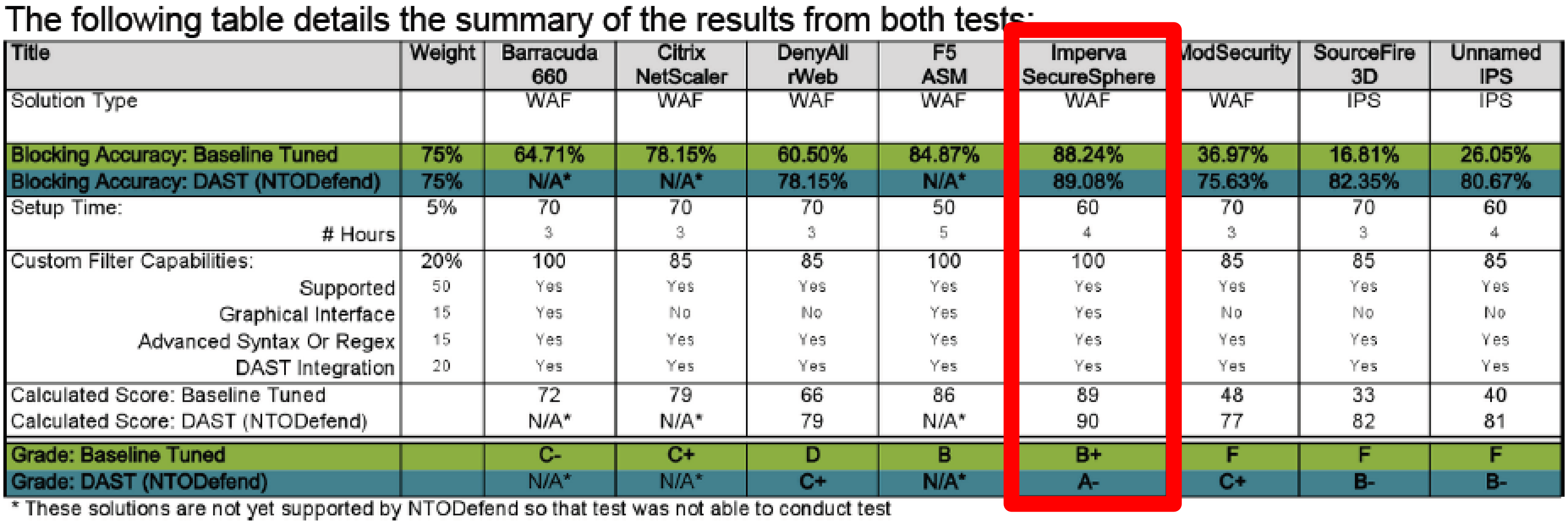
The following table details the summary of the results from both tests:

Title	Weight	Barracuda 660	Citrix NetScaler	DenyAll rWeb	F5 ASM	Imperva SecureSphere	ModSecurity	SourceFire 3D	Unnamed IPS
Solution Type		WAF	WAF	WAF	WAF	WAF	WAF	IPS	IPS
Blocking Accuracy: Baseline Tuned	**75%**	**64.71%**	**78.15%**	**60.50%**	**84.87%**	**88.24%**	**36.97%**	**16.81%**	**26.05%**
Blocking Accuracy: DAST (NTODefend)	**75%**	**N/A***	**N/A***	**78.15%**	**N/A***	**89.08%**	**75.63%**	**82.35%**	**80.67%**
Setup Time:	5%	70	70	70	50	60	70	70	60
# Hours		3	3	3	5	4	3	3	4
Custom Filter Capabilities:	20%	100	85	85	100	100	85	85	85
Supported	50	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Graphical Interface	15	Yes	No	No	Yes	Yes	No	No	No
Advanced Syntax Or Regex	15	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DAST Integration	20	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Calculated Score: Baseline Tuned		72	79	66	86	89	48	33	40
Calculated Score: DAST (NTODefend)		N/A*	N/A*	79	N/A*	90	77	82	81
Grade: Baseline Tuned		C-	C+	D	B	B+	F	F	F
Grade: DAST (NTODefend)		N/A*	N/A*	C+	N/A*	A-	C+	B-	B-

* These solutions are not yet supported by NTODefend so that test was not able to conduct test

Figure 6

WAFs in Reality



The following table details the summary of the results from both tests:

Title	Weight	Barracuda 660	Citrix NetScaler	DenyAll rWeb	F5 ASM	Imperva SecureSphere	ModSecurity	SourceFire 3D	Unnamed IPS
Solution Type		WAF	WAF	WAF	WAF	WAF	WAF	IPS	IPS
Blocking Accuracy: Baseline Tuned	75%	64.71%	78.15%	60.50%	84.87%	88.24%	36.97%	16.81%	26.05%
Blocking Accuracy: DAST (NTODefend)	75%	N/A*	N/A*	78.15%	N/A*	89.08%	75.63%	82.35%	80.67%
Setup Time:	5%	70	70	70	50	60	70	70	60
# Hours		3	3	3	5	4	3	3	4
Custom Filter Capabilities:	20%	100	85	85	100	100	85	85	85
Supported	50	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Graphical Interface	15	Yes	No	No	Yes	Yes	No	No	No
Advanced Syntax Or Regex	15	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DAST Integration	20	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Calculated Score: Baseline Tuned		72	79	66	86	89	48	33	40
Calculated Score: DAST (NTODefend)		N/A*	N/A*	79	N/A*	90	77	82	81
Grade: Baseline Tuned		C-	C+	D	B	B+	F	F	F
Grade: DAST (NTODefend)		N/A*	N/A*	C+	N/A*	A-	C+	B-	B-

* These solutions are not yet supported by NTODefend so that test was not able to conduct test

Figure 6

Step 4: WAF + Vulnerability Scanner

> “Security No-Brainer #9: Application Vulnerability Scanners Should Communicate with Application Firewalls”
>
> *—Neil MacDonald, Gartner*

Source: http://blogs.gartner.com/neil_macdonald/2009/08/19/security-no-brainer-9-application-vulnerability-scanners-should-communicate-with-application-firewalls/

Step 4: WAF + Vulnerability Scanner

- Apply SecureSphere policies based on scan results
- Monitor attempts to exploit known vulnerabilities
- Fix and test vulnerabilities on your schedule

WhiteHat SECURITY

QUALYS

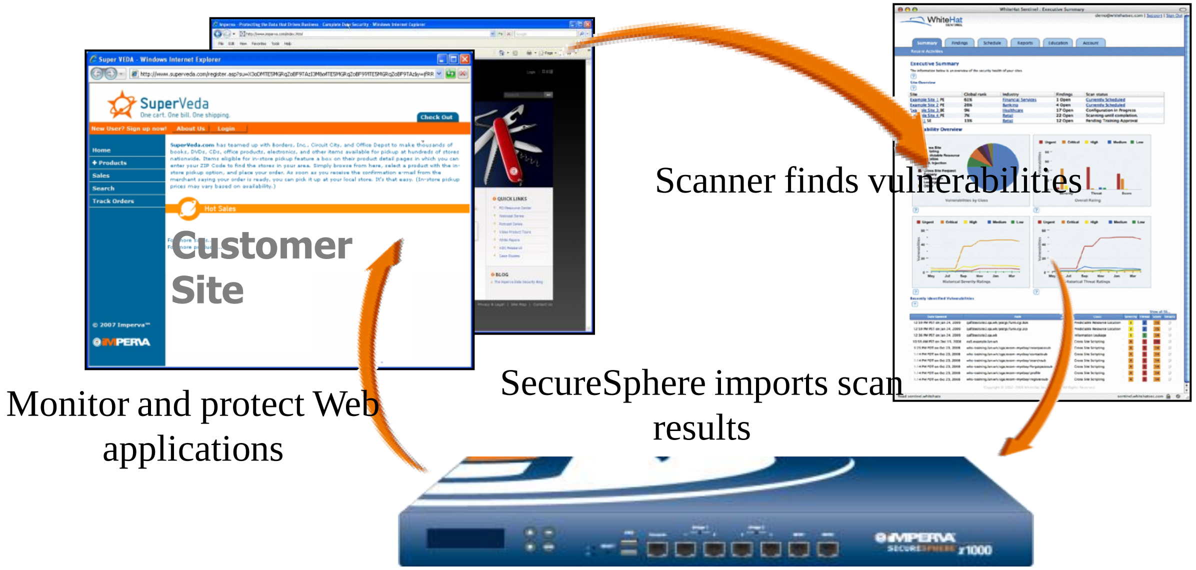
CENZIC Securing Enterprise Applications

hp

IBM

NTO NT OBJECTives, INCORPORATED

OWASP



Scanner finds vulnerabilities

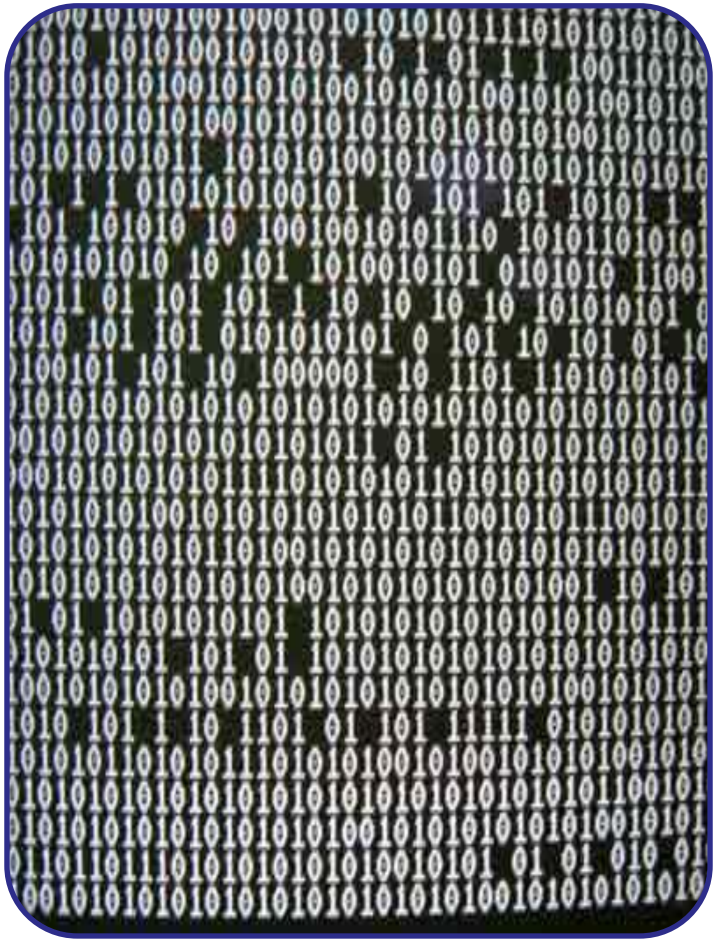
SecureSphere imports scan results

Monitor and protect Web applications

Step 5: Stop Automated Attacks

- Detecting protocol anomalies even if they are not considered malicious
- Slowing down an attack is most often the best way to make it ineffective (e.g. CAPTCHA, computational challenges)
- Feed the client with bogus information (e.g hidden links)

Step 6: Code Fixing



- Positives:
  - Root cause fixed
  - Earlier is cheaper
- Issues
  - Expensive, time consuming.
  - Never-ending process.

Summary: The Anti-Hack Stack

Dork Yourself

Blacklist

WAF

WAF + VA

Stop Automated Attacks

Code Fixing

QUESTIONS?

THANK YOU!