Voting Date Incident Response

Sang Young

2012.05.19

One

Category of Attacks - DDoS

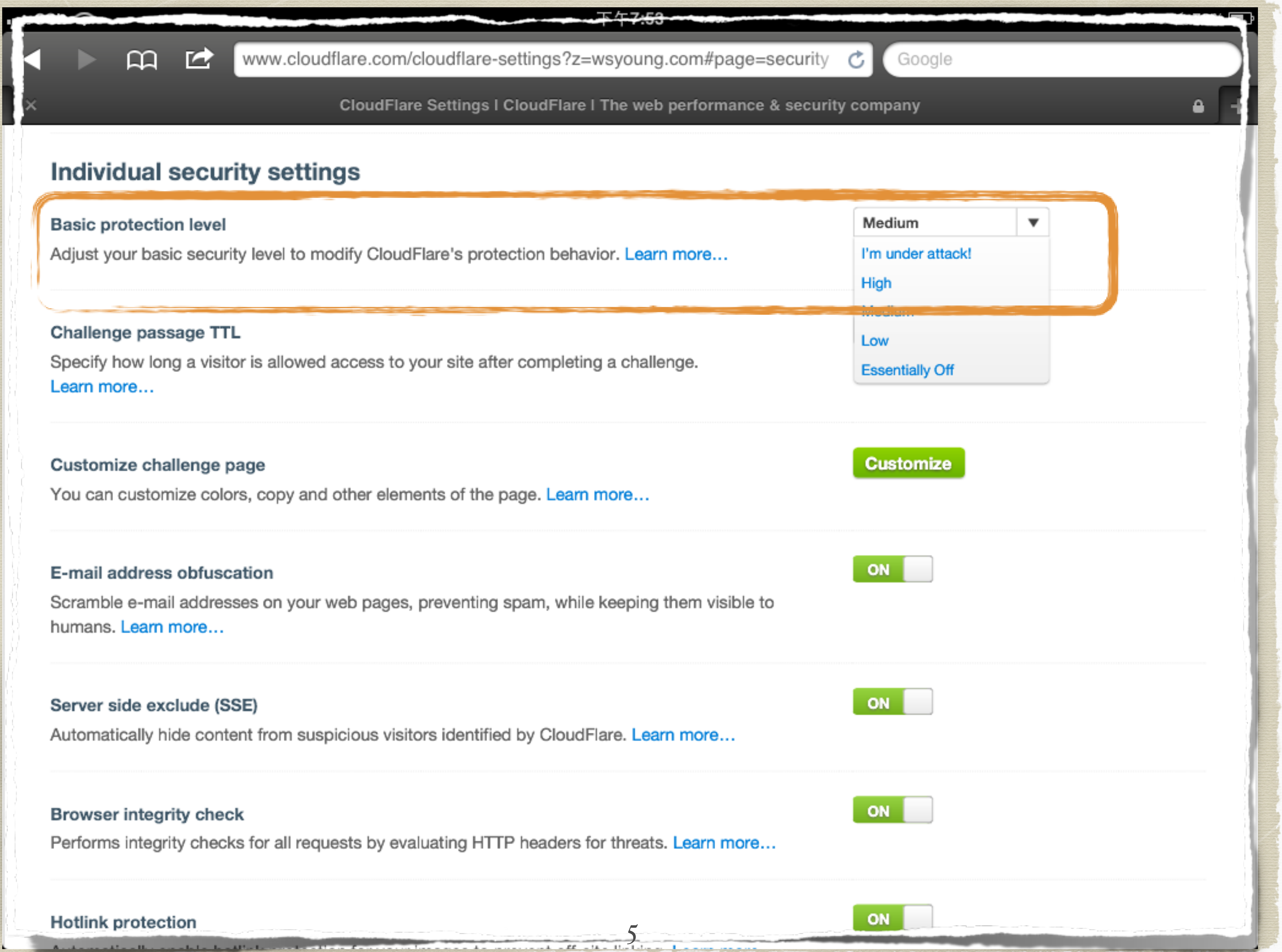
Two

1) Access Violation
2) Hotlink Attack

Access Violation

My observations:

1) malformed network packet
2) from multiple sources
3) from one country
4) network firewall can stop these attacks


下午7:53
www.cloudflare.com/cloudflare-settings?z=wsyoung.com#page=security
Google
CloudFlare Settings | CloudFlare | The web performance & security company

Individual security settings

Basic protection level

Adjust your basic security level to modify CloudFlare's protection behavior. Learn more...

Medium ▼

I'm under attack!
High
Medium
Low
Essentially Off

Challenge passage TTL

Specify how long a visitor is allowed access to your site after completing a challenge. Learn more...

Customize challenge page

You can customize colors, copy and other elements of the page. Learn more...

E-mail address obfuscation

Scramble e-mail addresses on your web pages, preventing spam, while keeping them visible to humans. Learn more...

ON

Server side exclude (SSE)

Automatically hide content from suspicious visitors identified by CloudFlare. Learn more...

ON

Browser integrity check

Performs integrity checks for all requests by evaluating HTTP headers for threats. Learn more...

ON

Hotlink protection

ON

Automatically enable hotlink protection for your images to prevent off-site linking. Learn more...

Hotlink Attack

Without Hotlink Protection, one can

1) access http://vote.pdce-primary.hk/images/logo.jpg directly
2) consume our bandwidth or server resources by creating many requests from multiple sources
3) create spam email with the embedded link of our images, causing same effect as 2)

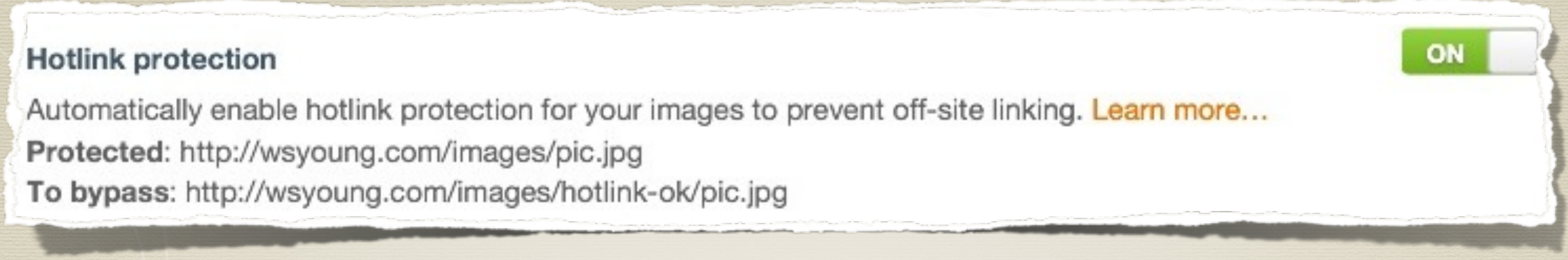
My observations:

1) hotlink attempts
2) from one country
3) network firewall does not help in this case, it is a common URL request

Hotlink Protection

By reconfiguration of the web server.
Apache Example:

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^http(s)?://(www\.)?pdce-primary.hk [NC]
RewriteRule \.(jpg|jpeg|png|gif)$ - [NC,F,L]
```



Hotlink protection ON

Automatically enable hotlink protection for your images to prevent off-site linking. Learn more…

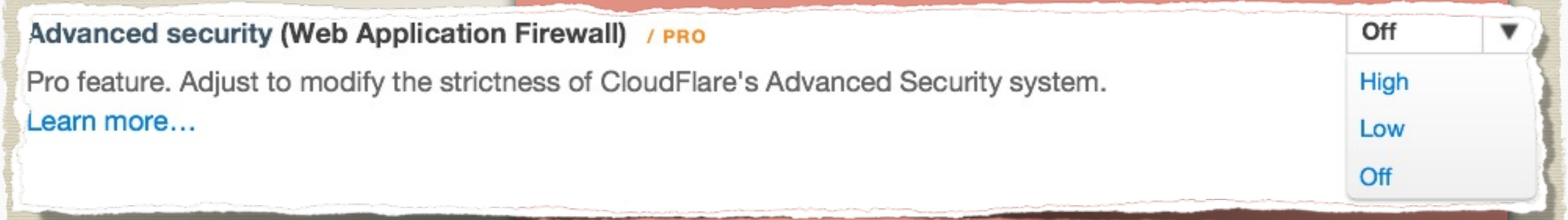
Protected: http://wsyoung.com/images/pic.jpg

To bypass: http://wsyoung.com/images/hotlink-ok/pic.jpg

Application Attacks

1) Web Application Firewall enabled in Cloudflare

2) Why no web application level?



Advanced security (Web Application Firewall) / PRO

Pro feature. Adjust to modify the strictness of CloudFlare's Advanced Security system.

Learn more…

Off ▼

Intrusion Lockout

1) access control includes unique URL, username, and password
2) once logged in, the above elements cannot be used in other terminal
3) we got some calls regarding failed logged in

Performance Tuning

1) encountered system slow down in the morning
2) real time system tuning to improve the response time

Statistical Morning

1) we have a portal https://monitor.pdce-primary.hk
2) check if any terminal adding huge records without short period time

Network Connection

1) voting terminals depends on Wi-Fi, coverage issues
2) voting terminals depends on 3G/ HSPA, operator issues

Privacy Infringement

1) happened in some voting stations

Purge Data

1) make use of secure delete
2) delete the database files in front of voting management team
3) including the resilient systems

Thank You

Sang Young