



# OWASP

Open Web Application  
Security Project

## Lessons from Protecting a Major Conference: What You Do Not Know Will Haunt You

Wong Onn Chee

OWASP Singapore Chapter Lead

# OWASP : Core Mission

- The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit also registered in Europe as a worldwide charitable organization focused on improving the security of software.
- Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks.
- Everyone is welcomed to participate in OWASP and all of our materials are available under free and open software licenses.

# Agenda

- Lessons drawn from protecting a major security conference
- EXTRA lesson arising from a common, major oversight when onboarding CDNs.

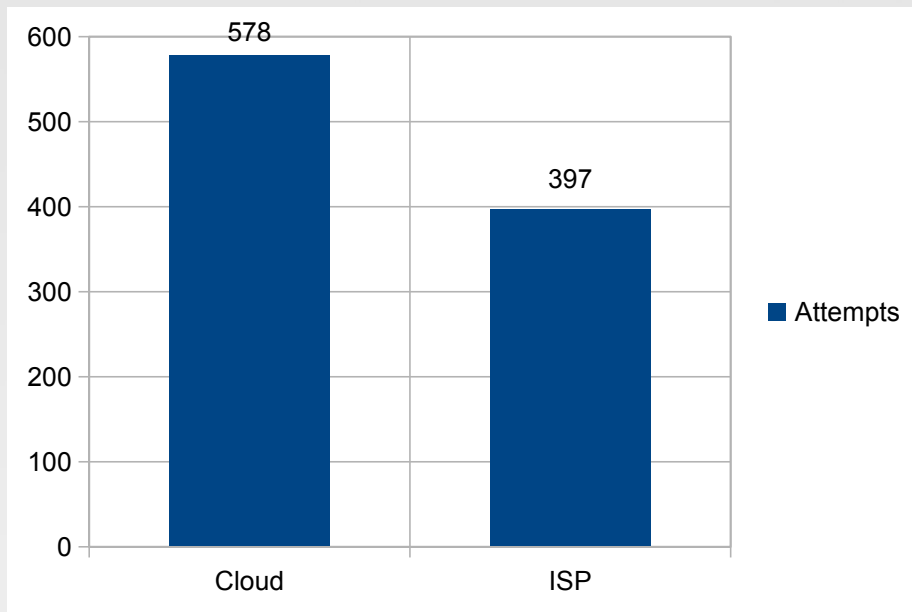
# Background

- A major security conference in 3rd quarter of 2018, with a Taiwanese delegation in the conference.
- Websites were hosted on a major cloud provider, with a separate CDN provider. The CDN provider offers anti-DDoS, WAF and content acceleration services to public.
- My subsidiary outbound security solution was deployed to monitor outbound traffic to provide real-time protection and real-time recovery (not every 5 mins) against web defacement (Not today's focus though).
- No defacement attempt was successful. Website stayed available throughout the conference.

# Findings

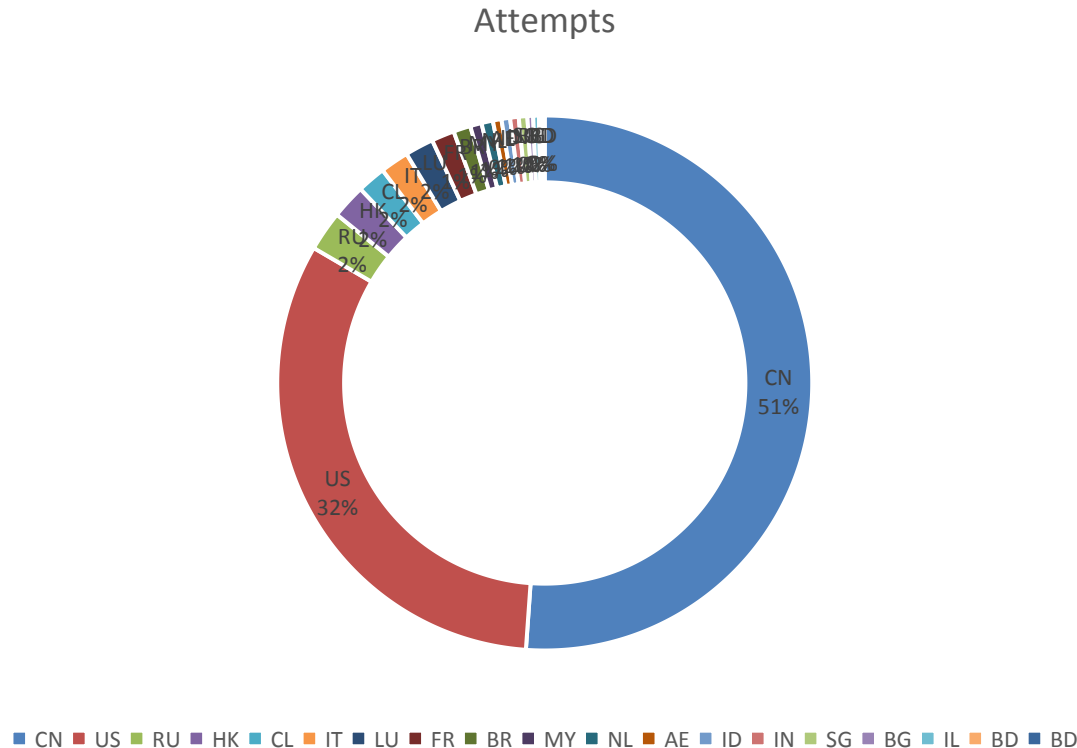
- Findings shared today are related to detected RECONNAISSANCE attempts, which WAF could not block. So using WAF does not mean you can switch off your brains.

## 60% of reconnaissance attempts were from cloud providers

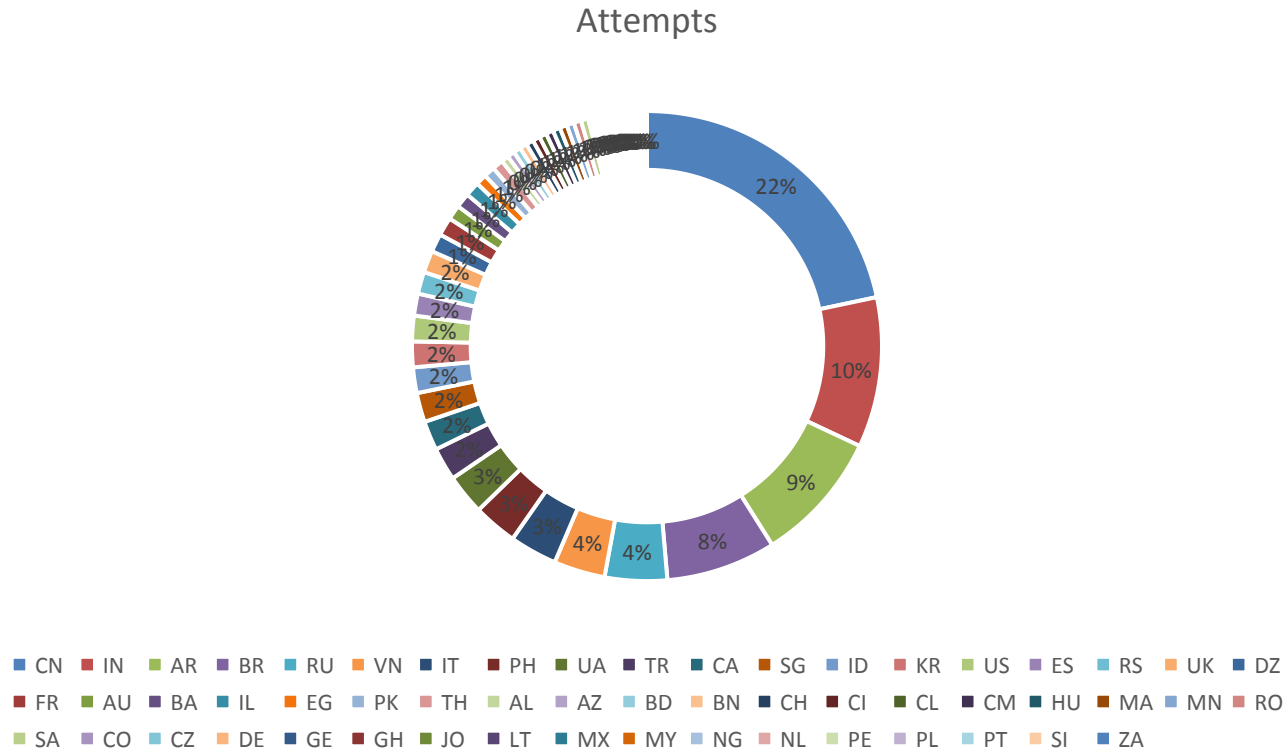


Cloud proportion may be higher as a lot of ISPs also provide hosting services.

# CN and US cloud providers accounted for 83% of recon attempts from cloud providers



# CN and IN ISPs accounted for 32% of recon attempts from ISPs



## More than meets the eyes

- Do note AWS accounted for 26% of recon attempts from US cloud providers . As the actual geo locations of the AWS IP addresses were not known, the recon attempts could have been initiated from within their SG availability zones.

# Map of Amazon's Data Centers

All Data Centers

Northern Virginia

Seattle

California Bay Area

Northeastern Oregon

Dublin

Luxembourg

Frankfurt

Beijing

Ningxia

Tokyo

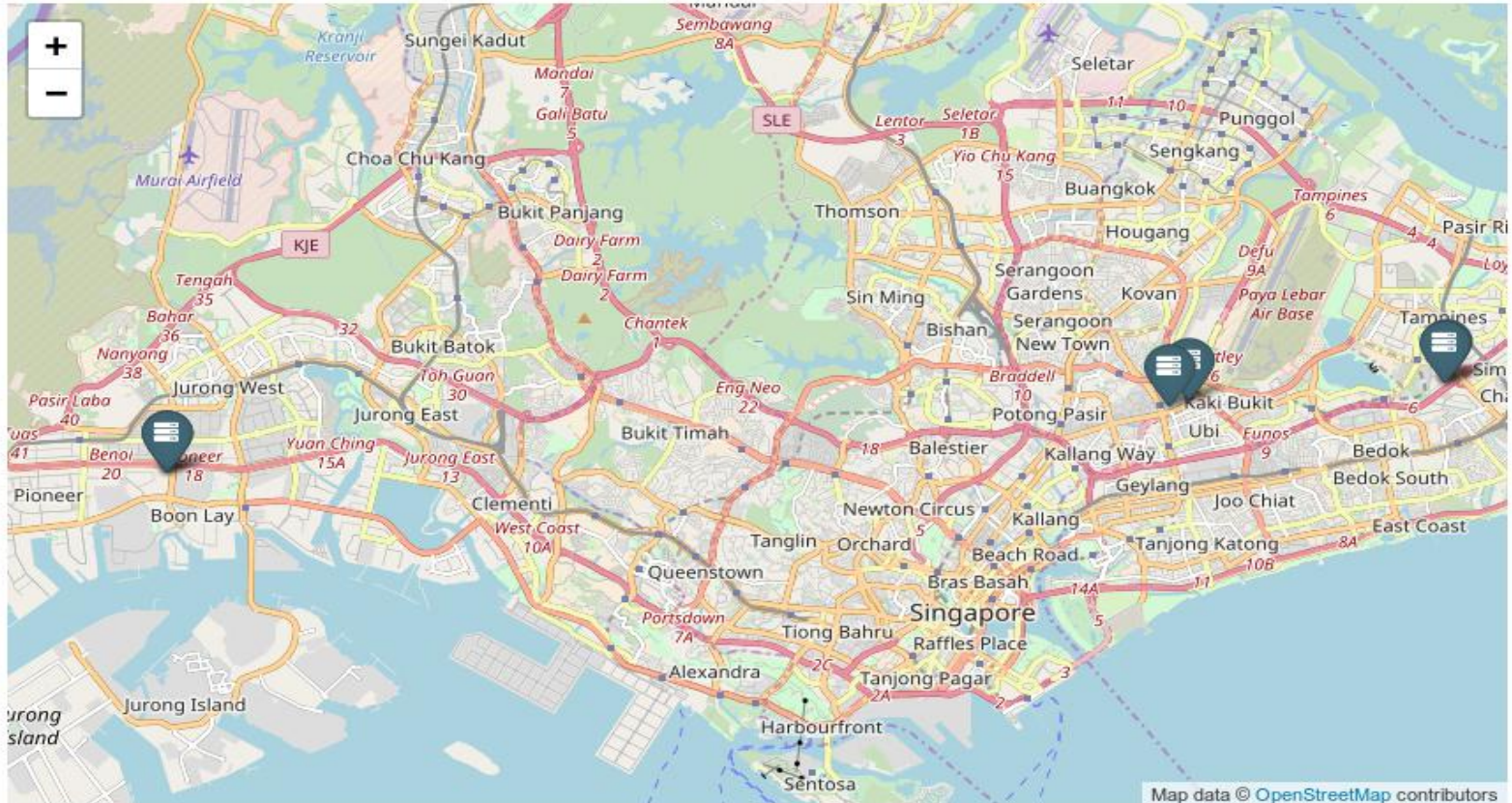
Osaka

Singapore

Sydney

São Paulo

Rio de Janeiro



## Case 1: Adaptive reconnaissance attempts

- Upon detecting recon attempts that from a China cloud IP, changes were made on the CDN to block the entire AS no. where the IP belongs to.
- After the “peace” for a day, the attackers changed the source IP to, perhaps another zone within the cloud, another IP address in another AS no. but still belongs to the same cloud provider.
- Slowly, as more and more of the cloud provider's AS nos. were blocked, the recon attempts from attackers residing in that cloud provider ceased.

## Case 1: Adaptive reconnaissance attempts

- Because we were able to kill the kill chain (pun intended) at it's first phase, there was no progression to the next phases of the kill chain. (Peace be unto Earth?)

# Lesson 1: Block source IPs from cloud providers

- Attacks launched from cloud are gaining popularity as more organisations move their online services to the cloud.
- Ask yourself - if you want to shoot a target, do you prefer to shoot it from across the ocean or from just 1 foot beside the target?



I will follow you to  
the ends of the world.

Khaled Hosseini

## WHOIS LOOKUP



**sg.gov.com is already registered\***

Domain Name: SG-GOV.COM  
Registry Domain ID: 2318916022\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.PublicDomainRegistry.com  
Registrar URL: <http://www.publicdomainregistry.com>  
Updated Date: 2018-10-08T06:49:40Z  
Creation Date: 2018-10-08T06:49:02Z  
Registry Expiry Date: 2019-10-08T06:49:02Z  
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com  
Registrar IANA ID: 303  
Registrar Abuse Contact Email: [abuse-contact@publicdomainregistry.com](mailto:abuse-contact@publicdomainregistry.com)  
~~Registrar Abuse Contact Phone: +1.2013775952~~  
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>  
Name Server: NS1.POLISHNS.RU  
Name Server: NS2.POLISHNS.RU  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>  
>>> Last update of whois database: 2018-10-09T05:18:53Z <<<

For more information on Whois status codes, please visit <https://icann.org/epp>

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information



AbuseIPDB

AbuseIPDB » 149.129.219.138

Enter an IP Address, Domain Name, or Subnet:

e.g. 171.1.234.46, microsoft.com, or 5.188.10.0/23

171.1.234.46

CHECK IP

**149.129.219.138 was found in our database!**

This IP was reported 2 times. Confidence of Abuse is 4%: ?

4%

ISP

Alibaba.com Singapore E-Commerce Private Limited

Usage Type

Commercial

Domain Name

alibaba-inc.com

Country

 Indonesia

City

Jakarta, Jakarta Raya

Spot an error? IP info including ISP, Usage Type, and Location provided by [IP2Location](#).  
[Contact them to update it!](#)

REPORT 149.129.219.138

WHOIS 149.129.219.138

slack

# Lesson 1: Block source IPs from cloud providers

- Cost-free. No need to buy any commercial products.
- Zero impact on 99.99% of human visitors to your websites.
- May impact users of cloud-based security gateway services, such as MessageLabs and Zscaler. (PS: There is a price to pay for mixing end users and cloud.)

# Lesson 1: Block source IPs from cloud providers

- ➊ Similar to typical firewall rules, close first then open access to cloud source IPs upon request:
  - ➋ Block source IP addresses even from the same cloud provider.
  - ➌ Whitelist requests from Search Engines that you allow.
  - ➍ Whitelist requests from Cloud SecaaS providers, such as MessageLabs, Zscaler and etc; known 3rd party service providers, such as SingPass, MyInfo, IRAS, CPF and etc; or authorised B2B partners.
  - ➎ Look at the X-Forwarded-For or X-True-Client-IP if you are behind a CDN.

# Lesson 1: Block source IPs from cloud providers

- Don't forget IPv6 source addresses too! We have seen recon attempts using IPv6 source addresses.

## Lesson 2: Look at Indicators of Reconnaissance for Easy Wins

- Looking at **Indicator of Reconnaissance - IoR**, not IoC or IoA, provided the team advance and ample notice to respond and forestall the actual malicious payloads from even being launched.
- Reconnaissance is the 1st step in the 7-steps kill chain. Stopping attackers at Recon steps will prevent attackers from progressing to the next 6 steps - WEAPONIZATION, DELIVERY, EXPLOITATION, INSTALLATION, COMMAND & CONTROL and ACTIONS ON OBJECTIVE.

## Lesson 2: Look at Indicators of Reconnaissance for Easy Wins

- Honeypot is not necessary for you to look at IoR. Your existing web portals can be a ready source of IoRs.
- Looking at IoR usually provides intelligence even before public disclosure of attacks. For instance, we detected requests to URLs ending with stssys.htm, which belonged to webcams, in July 2016, one month before Mirai was disclosed.

## Lesson 2: Look at Indicators of Reconnaissance for Easy Wins

- Reconnaissance attempts are usually noisy. Even if the attackers use stealth means, aka fly below the radar, you can still catch them even based on a single recon attempt. For instance, if you are running a ASP.Net web portal, any request to a .php URL is prima facie a malicious recon attempt.
- Beware of forwarding all web access logs to your SIEM, as it will blow the costs of your SIEM. This is because recon attempts usually form less than 10% of traffic to your web portal. Which means instead of paying to analyse 1GB of recon attempts, you could be paying to analyse 10GB worth of the entire web traffic.

## Lesson 2: Take note of common false positives

### 🌐 **/.well-known/\* URLs**

Refer to <https://www.iana.org/assignments/well-known-uris/well-known-uris.xhtml>

(Except those openpgpkey URLs)

### 🌐 **/browserconfig.xml**

Refer to <https://realfavicongenerator.net/blog/more-browserconfig-xml-less-html/>

### 🌐 **/cross-platform-app-identifiers**

<https://developer.microsoft.com/en-us/graph/docs/concepts/cross-device-app-configuration>

## Lesson 2: Take note of common false positives

 **/ads.txt**

Refer to <https://iabtechlab.com/ads-txt/>

## Lesson 2: Common true positives

- 🌐 **URLs asking for extensions your portal does not use**

For e.g. requests for .aspx or .php when your portal is built in Java

- 🌐 **/\* URLs (other than .well-known)**

Usually to detect accidental data leakage, such as .git, .filezilla, .vscode and etc

- 🌐 **Configuration files**

Such as deployment-config.json, web.config, web.xml, server.xml, sitemaneger.xml and etc

## Lesson 2: Common true positives

- 🌐 **Admin pages of popular CMS which you are not using**

Such as /users, /wp-admin, /wp-config, /Sitecore, /Sitefinity, /console, phpmyadmin and etc

- 🌐 **Extensions with ~, .save, .bak**

Usually to detect accidental data leakage via backup files

- 🌐 **Others such as /cdn-cgi, /wallet/, /bitcoin/, /backup**

Usually to catch unintentional exposure of sensitive folders.

## Lesson 2: Interesting recon attempts

12 September 2018 21:29:20 +08:00 199.36.244.14 US MCCARRAN INTERNATIONAL AIRPORT

Which famous security conferences are located near this airport?

45.59.88.57 US Marshall Municipal Utilities

45.59.88.57 US Marshall Municipal Utilities

CII/SCADA installation security failures

## Lesson 3: Previous Source IP restrictions NO LONGER work when you onboard CDNs

- Before onboarding CDNs, you may have restricted access to sensitive sections, such as admin console, of your portal to specific source IP addresses. These are usually achieved via simple source IP restrictions on your WAF or URL ACLs on your web server. Good practice as it reduces the exposed attack surface.
- However, when you onboard CDNs, you will need to allow access to ALL sections of your portal from the CDN's IP ranges. Hence, the previous restrictions no longer work.

## Lesson 3: Apply restrictions to X-Forwarded-For or X-True-Client-IP

- You will need to restrict source IPs by looking at the X-Forwarded-For or X-True-Client-IP if you are behind a CDN. These values usually indicate the actual “true” source IP addresses of the visitors.
- Do note that X-Forwarded-For may consists of an array of comma-separated IP addresses. Look at the extreme left or first IP address to identify source IP address of actual client. (Refer to <https://en.wikipedia.org/wiki/X-Forwarded-For>)

# Fun Exercise

- A simple Google Hacking recon exercise to find publicly exposed admin consoles.



# OWASP

Open Web Application  
Security Project

## Lessons from Protecting a Major Conference: What You Do Not Know Will Haunt You