CLOUDSEC 2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.
Bullet-proofing your Internet applications against the evolving threats

Chris Wang | Cloudflare
@chriswang_tech
If you use the Internet, you already use Cloudflare
Cloudflare's global anycast network

- 8.7M HTTP requests / second on average
- 30Tbps network capacity
- 19M+ Internet properties
- 180+ cities

#cloudsec
In case you haven't heard about Cloudflare...
Cloudflare solves today’s Internet challenges

**PERFORMANCE**
- CDN
- Web optimization
- Mobile optimization
- WAN optimization

**SECURITY**
- DDoS
- SSL
- WAF
- Rate limiting

**RELIABILITY**
- DNS
- Anycast network
- Load balancing
- Always online

**INSIGHTS**
- Threat analytics
- Enterprise logs
- Apps platform
- Traffic monitoring

**PLATFORM**
- Workers
- Access
- Stream
- Mobile SDK

#cloudsec
Defining security threats

1 - DDoS attacks
2 - Web application attacks
Defense against DDoS requires scalable solutions
DDoS aims to make your internet service unavailable.

Up to 600,000 devices (Mirai 2016)
DDoS attacks are getting more "affordable"
DDoS attacks are getting larger

- 2012: 300Gbps // Volumetric Layer 3/4
- 2013: 400Gbps // NTP Reflection
- 2016: 1Tbps // IoT Botnet Layer 7 Attack
- 2018: 1.7 Tbps // Memcached reflection/amplification Attack
IP addresses coming mostly from China. Historically, all state actor-sized DDoS (200-400 Gb/s of junk) we experienced coincided in time with protests in Hong Kong (coordinated on @telegram). This case was not an exception.

6:54 PM - 12 Jun 2019

Source: https://twitter.com/durov/status/1138942773430804480
Put numbers in scale

942 Gbps
Largest DDoS attack mitigated by Cloudflare

30 Tbps
Cloudflare Network Capacity
"Always-On" = No slowing down

Industry Legacy Scrubbing
- Long propagation times (up to 300 sec)
- Adds significant latency
- Typically requires manual intervention

Always-On
- Zero propagation time
- No added latency
- Immediate, automated mitigation, with no “cut over” required
Defense against web application attacks require fast actions on large dataset
Web app attacks aim to gain unauthorized access by exploiting vulnerabilities in web apps

<table>
<thead>
<tr>
<th>OWASP Top 10 - 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1:2017-Injection</td>
</tr>
<tr>
<td>A2:2017-Broken Authentication</td>
</tr>
<tr>
<td>A3:2017-Sensitive Data Exposure</td>
</tr>
<tr>
<td>A4:2017-XML External Entities (XXE)</td>
</tr>
<tr>
<td>A5:2017-Broken Access Control</td>
</tr>
<tr>
<td>A6:2017-Security Misconfiguration</td>
</tr>
<tr>
<td>A7:2017-Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>A8:2017-Insecure Deserialization</td>
</tr>
<tr>
<td>A9:2017-Using Components with Known Vulnerabilities</td>
</tr>
<tr>
<td>A10:2017-Insufficient Logging &amp; Monitoring</td>
</tr>
</tbody>
</table>

Check if you have an account that has been compromised in a data breach

email address

Generate secure, unique passwords for every account

Largest breaches
- Collection #1 accounts: 772,906,991 accounts
- Verifications.io accounts: 763,117,241 accounts
- OnlineSpambot accounts: 711,477,622 accounts
- Exploit.in accounts: 593,427,119 accounts
- Anti Publico Combo List accounts: 467,962,538 accounts
- River City Media Spam List accounts: 363,430,369 accounts

Recently added breaches
- CafePress accounts: 23,205,230 accounts
- Club Penguin Rewritten (July 2019) accounts: 4,007,909 accounts
- Anime-Planet accounts: 388,507 accounts
- EpicNPC accounts: 408,795 accounts
- Clash of Kings accounts: 1,604,657 accounts
- Snail accounts: 1,410,899 accounts
- Xiaomi accounts: 7,088,010 accounts
- Flash Flash Revolution (2019 breach) accounts: 1,858,124 accounts
- Stronghold Kingdoms accounts: 5,187,305 accounts
- GameGadgets accounts: 1,506,242 accounts

Source: https://haveibeenpwned.com/
Web app attacks still follow the old cycles

#1 Discovery of a new vulnerability (0-day)

#2 Exploit attempts by attackers

#3 Fixes / patches issued by vendor

#4 Fixes / patches deployed by the user
WAF "as a service" means faster response to new vulnerabilities

1. Discovery of a new vulnerability (0-day)
2. Exploit attempts by attackers
3. Fixes / patches issued by vendor
4. Fixes / patches deployed by the user
Stopping CVE-2019-0604 (1/2)

2019-05-11 9:33AM: CVE-2019-0604, a Remote Code Execution vulnerability in Microsoft SharePoint Servers which was not previously known to be exploitable via the web. CVSS v3 rating = 8.8

2019-05-11 2:45PM: Cloudflare internal vulnerability score = 9.8
Cloudflare WAF Rule 100157 deployed in Log mode


timestamps in UTC; source: https://blog.cloudflare.com/stopping-cve-2019-0604/
Stopping CVE-2019-0604 (2/2)

2019-05-13 2:13PM: Cloudflare WAF Rule 100157 deployed in **Block** mode

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Group</th>
<th>Default mode</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>100157</td>
<td>Microsoft SharePoint - Deserialization - CVE:CVE-2019-0604</td>
<td>Cloudflare Specials</td>
<td>Block</td>
<td></td>
</tr>
</tbody>
</table>

2019-05-16: UK’s NCSC's [alert](#) of highly successful exploitation attempts against UK organisations. On the same day, ~7000 malicious requests blocked by Cloudflare WAF Rule 100157
Some best practices we find useful ....
How to prepare against DDoS attacks

Choose a DDoS solution that's scalable, always-on & cost-effective

Ensure it doesn't slow down your visitors (or make it even faster)
How to prepare against web app attacks

- Choose a cloud managed WAF with a large user base
- Patch the applications (eventually)
Lucky Draw
Main stage 4:50-5:00pm

Remember visit us at booth 黄2!
THANK YOU