An HR Company's DDoS Protection Gets a Major Promotion

RED BUTTON
DDoS Experts

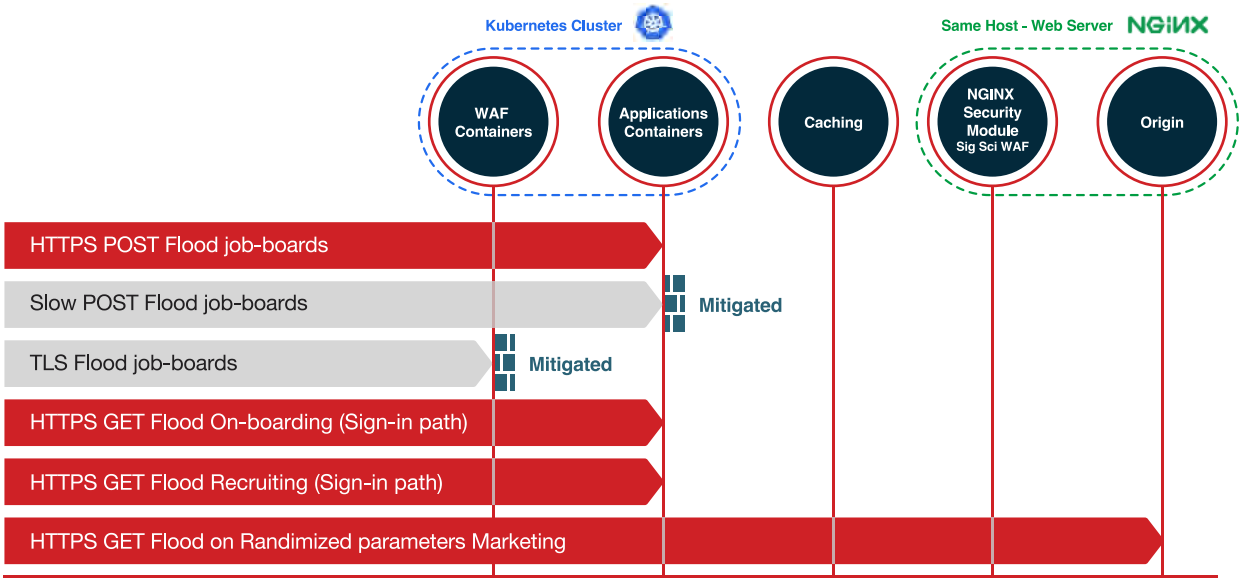
The HR services company provides innovative SaaS technology and know-how for recruiting, hiring and onboarding top talent. After their services experienced high loads that appeared to have malicious intent, the company turned to Red Button to examine and test their protection against potential DDoS attacks.

WHEN THE DEFENDER IS ALSO UNDER ATTACK

The company uses a cloud protection service provided by AWS to protect against network layer DDoS attacks. For defense of the web application layer, the company uses a host-based WAF provided by Signal Sciences. However, this is not in line with best practices in the industry, as both the WAF and the potential target of a DDoS attack are on the same company web server. That is, the targeted server would simultaneously attempt to provide a defense relying on the very same resources that are currently under DDoS attack.

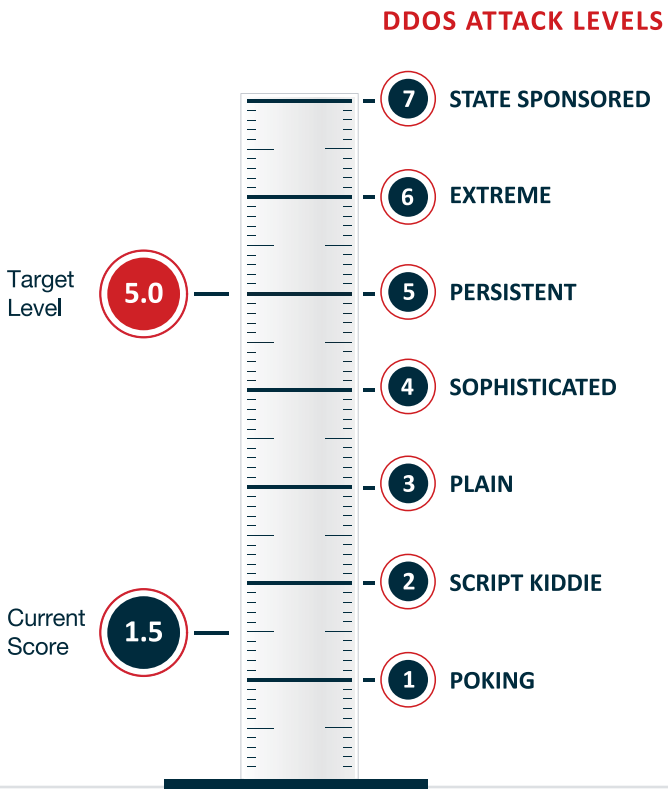
In light of the company's infrastructure, architecture and assets, we designed a tiered simulation to challenge their WAF protection against DDoS attacks. The simulation included six application-level attack scenarios. Five attacks targeted three web applications in the AWS environment, protected by the hosted WAF containers, while a sixth attack focused on a marketing website, which also included a hosted WAF (the attack was meant to bypass the caching mechanism).

The Initial Failure



All but two of the simulated attacks completely crashed the company's online services, indicating that such attacks would result in a significant denial of service to the company's customers. The only two attack vectors that were mitigated, without impacting service, were a slow-moving POST flood and a targeted TLS flood.

The simulated attacks indicated a DDoS Resiliency Score (DRS) level of 1.5, which is very far below both the minimal necessary protection level of 4.5 and the recommended target DRS of 5.0.



Recommendations

Urgent steps were clearly needed to change the situation:

- First and foremost, Red Button recommended deploying a cloud-based WAF, which is highly available, scalable, and not subject to the resource limitations of host-based WAFs.
- Also recommended was a CDN service for the web applications, as it is highly effective in mitigating various DDoS attack vectors with configurable traffic-routing that allows for better risk management.
- Finally, we advised the company to investigate the mitigation failures of the Signal Sciences WAF, which will provide insight into how best to tweak its configuration.

We noted that implementing these recommendations will align the organization's resiliency level with the threat level we initially identified.

EXCEEDING EXPECTATIONS WITH RED BUTTON

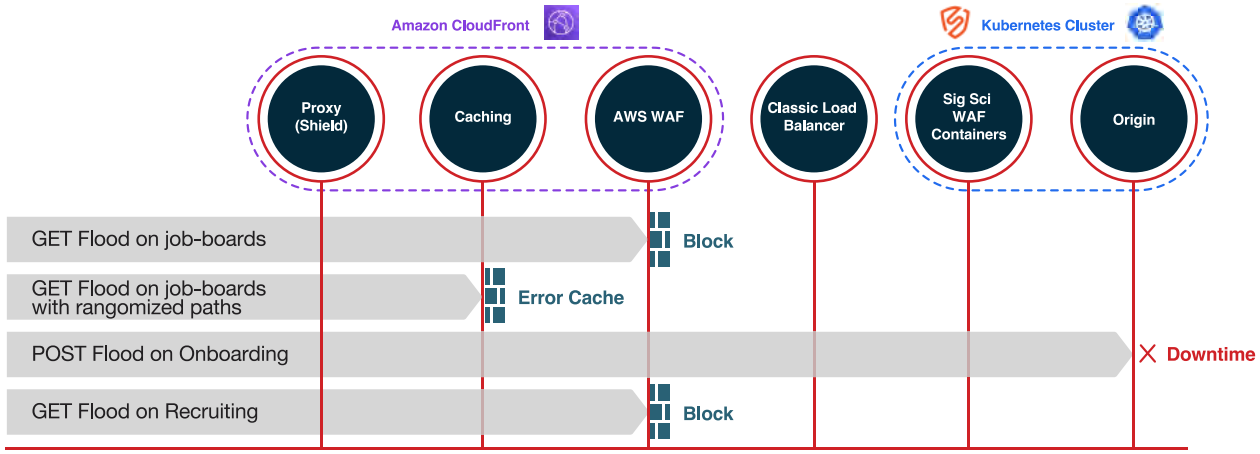
Faced with the disturbing news, the HR services company asked for guidance from Red Button as to hardening their defenses. We explained several architecture and configuration options in detail, including the costs, required resources, and expected DRS improvement.

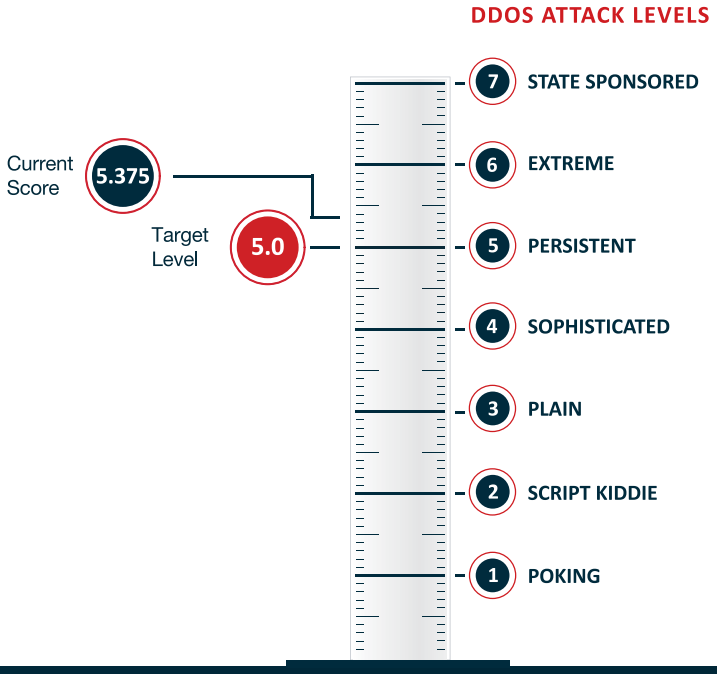
They undertook the project with enthusiasm. The company implemented Amazon CloudFront CDN and a cloud-based AWS WAF for their web application layer and made several configuration changes as recommended. These steps added several additional layers of protection, which were proven highly effective in follow-up Red Button DDoS simulations.

THE UNDENIABLE RESULTS

Red Button's simulation to test the migration to the AWS cloud-based DDoS defenses consisted of four web application layer attacks.

The results were night-and-day in comparison to the DDoS simulation carried out prior to the recommended changes. Three scenarios were fully mitigated with fine-tuned rate-limit rules and the one successful DDoS attack was merely the result of an easily corrected misconfiguration.





The follow-up DDoS simulation indicated a DRS score of 5.375. This is not just well above the threat level typically faced by such companies, it is also above the target score we suggested for them.

For this HR services company, the resounding success is a job well done.