Service Provider Overcomes Application-Layer Attacks and Bot Assaults to Restore Services and Customer Trust

OVERVIEW

This global service provider delivers services such as internet access, cloud hosting, phone lines, cellular communication, streaming TV, and more, to 250 million wireless subscribers and 80 million subscribers using non-wireless services.

CHALLENGES

This service provider found itself in the middle of a massive brute force bot attack using log-in credentials. The security operations team (SOC) assumed they were protected by their DDoS protection service, but this proved incapable of stopping these automated attacks. The assault lasted several weeks.

The attacks impacted website availability, resulting in a poor digital experience and brand reputation loss. Low application performance impacted new service activations and reduced

revenue. In addition, the service provider had to deal with the threat of account takeover, fraud and free use of services.

The first targeted application was the portal where customers can login from the webpage and activate, remove and edit services. The attacker created a largescale bot attack on this login service, peaking at ~27 million HTTP request per day, which dramatically reduced the availability and performance of the service. Customers complained about poor service availability and performance, which generated bad relations for the service provider.

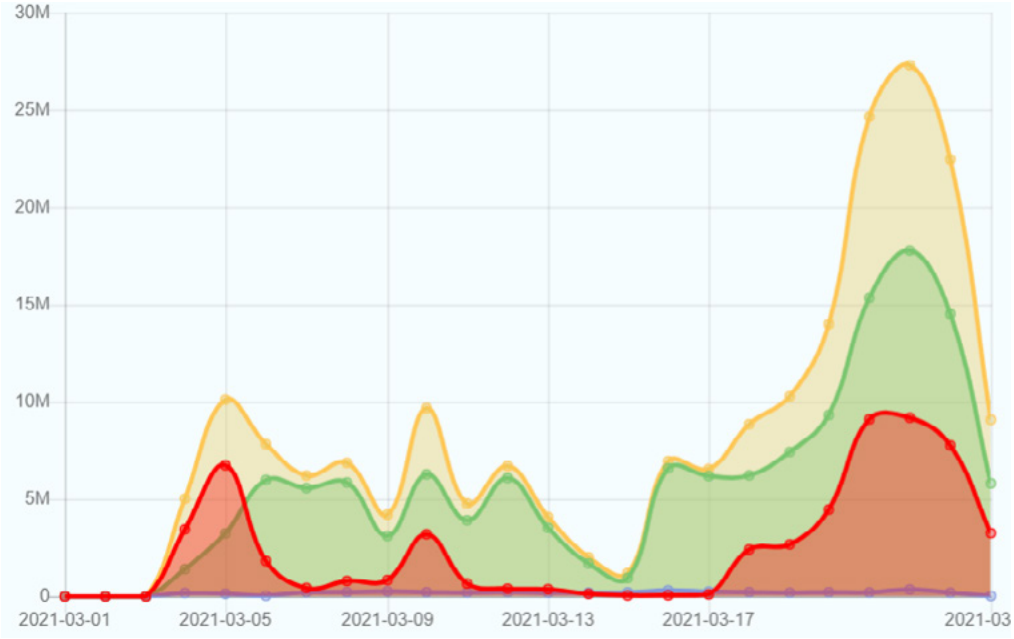

Figure 1: ~27 million HTTP requests per day

In an attempt to mitigate the attack, the service provider tried to use rate limiting and geo blocking. This did not solve the problem since both are largely useless against dynamic attacks and generate high false positives.

By this time, the service provider had been overwhelmed by attacks for weeks. Its SOC team was exhausted, its fraud department didn't understand the threat and the company began experiencing criticism from its customer base.

SOLUTION

The service provider turned to Radware and its cloud protection services, including Bot Manager, Cloud WAF Service and Cloud DDoS Protection Service. Since these are cloud services, implementation and set up was accomplished via a simple DNS redirection.

An important key for success was Radware's customer service support team and Emergency Response Team (ERT). They provided timely and accurate best practices within a few hours of the request for assistance.

The account takeover attacks began with up to 19,500 login attempts per username and it was reduced to only 51 login attempts with the help of Radware Bot Manager (see image below).

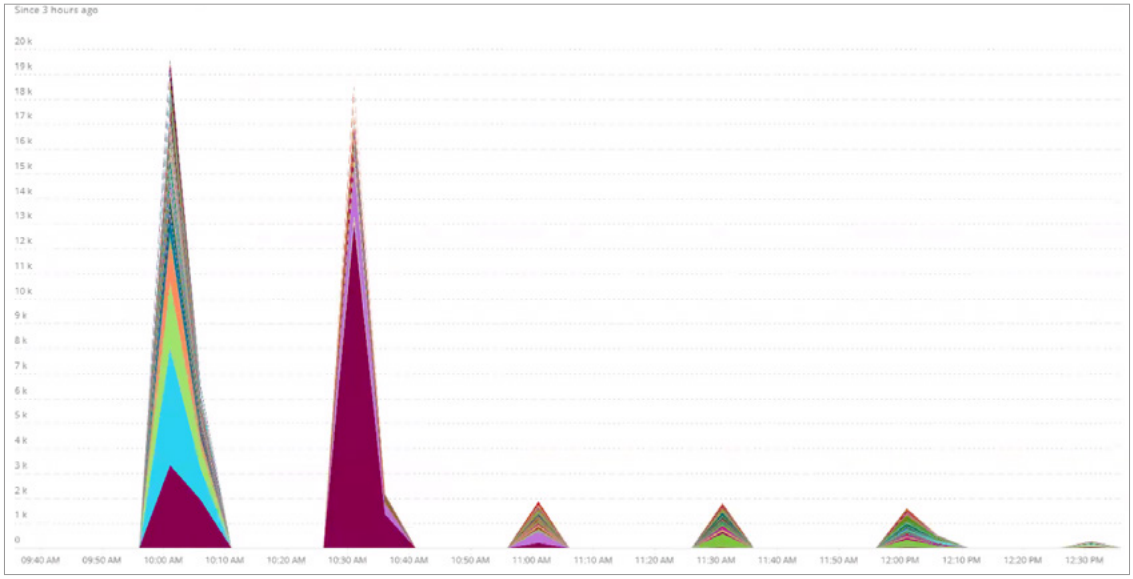

Figure 2

The bot campaign ran for several weeks and would adapt to try and bypass Radware's application protection.

- Brute force bot attack that began with account takeover attempts
- Changed method from hundreds of requests per IP to one request per IP to overcome the bot manager policy
- After being successfully mitigated again, the focus of attacks shifted to a new customer-facing application and switched attack vectors to form fills.
- A new target was selected: the service provider's mobile application
- Attack vectors changed to Layer 7 DDOS – 10Gbps

All attacks were mitigated by Radware Bot Manager, while the Layer 7 DDoS attack was mitigated by Radware's Cloud DDoS Protection Service.

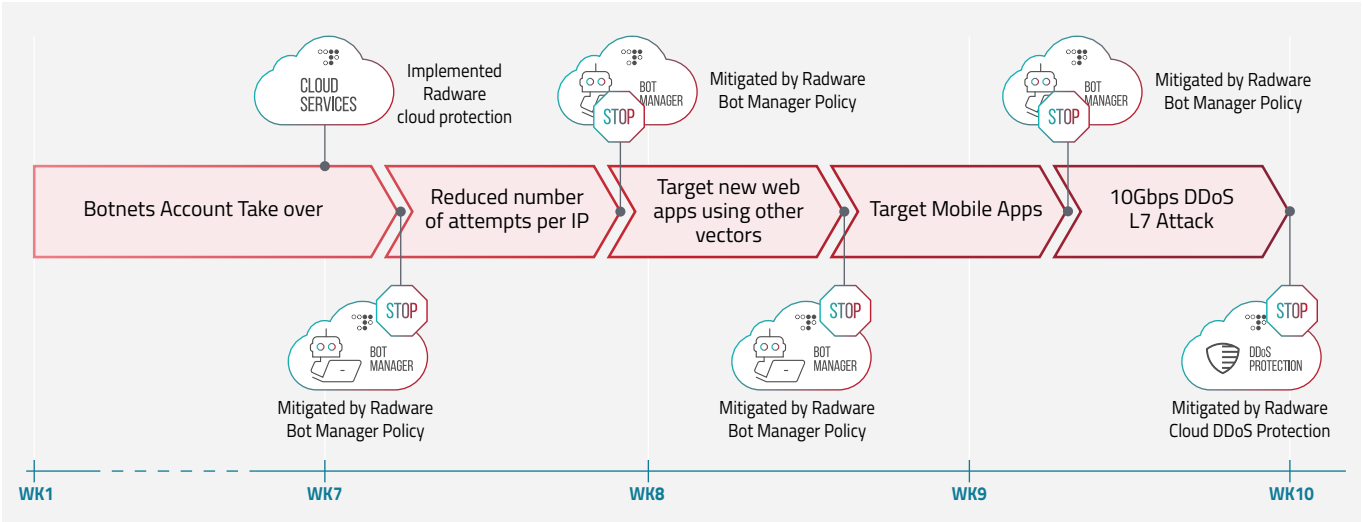

Figure 3: Attack evolution mapped to the solution used to mitigate the threat

BENEFITS

Radware successfully protected the service provider's applications and services from a series of high-volume bot and DDoS attacks. Radware's automation and behavioral learning capabilities allowed the service provider's SOC team to focus on implementing new security strategies and policies.