Test Results Shock a Major Israeli Bank into Action

RED BUTTON
DDoS Experts

BACKGROUND

The bank is the one of the largest in Israel and a leader among local mortgage lenders. It has over 100 branches and offers a complete range of international, commercial, domestic and personal banking services.

The bank operates traditional security and network operations centers (SOC/NOC) and a dedicated network team as part of its IT ecosystem. Other DDoS mitigation measures include a managed protection service offered by the bank's ISP, which focuses on the provider's infrastructure, and an on-premises WAF for filtering, monitoring and blocking suspect HTTP traffic.

THE CHALLENGE

Banks have good reason to be particularly concerned about DDoS attacks, considering the sensitive nature of the services they provide. In Israel, high profile banks are identified with the state and regularly targeted in cyberattacks.

The client's security and network operations teams need to be able to immediately identify a DDoS attack and trigger a response. Members of both teams should be acquainted with the types of attacks, be able to identify targeted network segments, and understand defense mechanisms.

The CISO decided that the time had come to review the bank's DDoS mitigation capabilities and harden them, if need be. This initiative was undertaken as global DDoS attacks were becoming larger, with higher volumes and greater complexity, and happening more frequently.

THE SOLUTION

The bank's security executive turned to Red Button due to our reputation as a thorough DDoS testing provider.

After reviewing the client's DDoS protection architecture, we ran controlled DDoS attack simulations. This involved resistance and penetration testing that challenged both the network and relevant bank applications.

Network and Application Testing

The three standard infrastructure attack simulations we carried out - SYN, ACK and UDP floods – were only partially resisted. To test the applications, we prepared three mock attacks of increasing severity. However, after the bank's standard protection tools failed to mitigate or resist the first wave, we immediately ended the simulation.

The bank leadership was very surprised at the results. Our DDoS testing had revealed that the bank's ISP protection just did not have the capacity to handle relatively basic attacks, even without any extreme frequency rates.

Next, we provided the bank with recommendations to improve DDoS protection using their current technology. These included: more effective security configurations for the on-premises WAF; options to discuss with the ISP; improvements to the DDoS mitigation layer; migration

to a cloud WAF and scrubbing center; written protocols for DDoS real-time response; and a shortlist for DDoS mitigation technology vendors.

From Complacency to Perpetual Action

The bank was very proactive in their response. While they decided to continue with the technology they were using, they immediately implemented recommended improvements to both their preventative measures and procedural responses to DDoS attack.

As a follow-up step, the bank hired Red Button for guidance in hardening their IT architecture and procedures. We conducted another detailed review and provided further systemic recommendations. This was followed by the bank again calling on Red Button to carry out tests, including a repeat of the simulated network attacks, that would measure the benefits of the various DDoS security optimizations they implemented.

Measurable Results – with More to Come

The last set of tests we carried out for the bank after they implemented our recommendations provided a clear indication of improved protection against DDoS attack. In fact, the bank reached the maximum protection possible with the technology they were using in their IT ecosystem.

The bank's resiliency score in the first Red Button DDoS test was 3.0, which jumped to 4.7 after implementing our recommended measures. We estimate that the bank can further increase its score to 6.5 when it integrates additional technologies and architectural optimizations we suggested.