6 Days, 100 Hours, and 1.25 Trillion malicious requests. How a Top UAE Bank Stood Strong Against a Massive Cyber Onslaught

CUSTOMER:
A leading UAE bank with a pan-Middle East presence.

INDUSTRY:
Banking & Finance.

CHALLENGES:

- Extremely intense, high-RPS Web DDoS "Tsunami" attacks persisting in waves lasting for several days at a stretch.
- Encrypted DDoS attack traffic that continuously evolves patterns and vectors to make detection challenging.

Overview

This leading United Arab Emirates bank is a Radware client and provides personal and corporate financial services to customers across the Middle East region. Recently, the bank was confronted with an intense **Web DDoS** (Distributed Denial-of-Service) attack campaign. Over a period of **six days**, the institution endured **100 hours** of continuous attack waves—with some lasting nearly **20 hours**—that were intended to cripple or take down their website and mobile applications.

WHY RADWARE?

Radware's Web DDoS Protection solution, powered by AI-driven, behavioral-based detection and mitigation systems, provides the only effective and proven protection available in the market today against damaging Web DDoS attacks.

Challenges

Unlike conventional DDoS attacks, Web DDoS attacks—also known as "Tsunami" attacks—generate an exceptionally high number of requests per second (RPS) to overwhelm targeted servers and infrastructure. Their attack traffic is often encrypted, making it difficult to discern malicious requests from legitimate ones. Detection of attack is made much more challenging as they continuously evolve to alter their patterns and characteristics to evade conventional security measures. This dynamic behavior prolongs the attack duration and exacerbates downtime.

Key Attack Characteristics:

- **Massive Scale:** The attack peaked at **12.5 million RPS**, with sustained hours-long bursts at 5M–10M RPS.
- **Unrelenting Duration:** 70% of the six-day period was spent under active attack.
- **Sophisticated Tactics:** The attack vectors continuously evolved, rendering traditional rate-limiting and predefined signatures ineffective.

Figure 1:

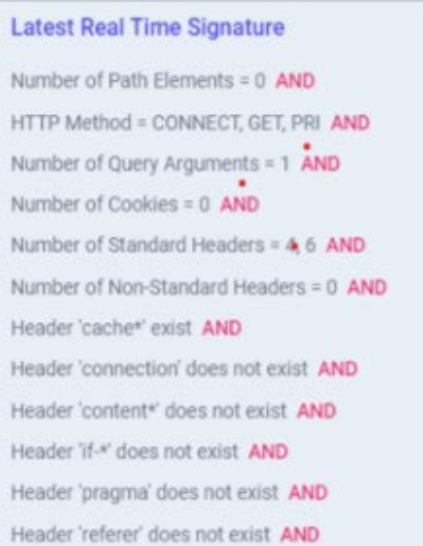
Web DDoS Attack Volume Over Six Days.

Solution

To counteract the scale and persistence of the attack, the bank leveraged Radware's advanced **Web DDoS Protection** solution powered by **AI-driven, behavioral-based detection and mitigation** systems, which provide unique protection not offered by any other security suite in the market.

Figure 2:

Attack Signatures Blocked by Radware Web DDoS Protection.



Key Attack Characteristics:

- **Real-Time Attack Detection:** Radware's AI-based algorithms analyzed attack patterns and created dynamic signatures in real time to effectively mitigate threats without blocking legitimate traffic.
- **Automated Adaptation:** Over 27 different parameters were used to fine-tune the mitigation strategy, ensuring continuous adaptation as attack vectors evolved.
- **Zero Human Intervention:** The system operated autonomously, delivering precision mitigation without manual adjustments.
- **Seamless User Experience:** Throughout the attacks, legitimate users remained unaffected, with zero service disruptions.

Benefits

To counteract the scale and persistence of the attack, the bank leveraged Radware's advanced **Web DDoS Protection** solution powered by **AI-driven, behavioral-based detection and mitigation** systems, which provide unique protection not offered by any other security suite in the market.

- **Unmatched Resilience:** The bank remained **fully operational**, successfully processing all legitimate transactions despite the attack.
- **Uninterrupted Operations:** Despite the relentless assault, all of the bank's 1.5 billion **legitimate requests were seamlessly processed** without downtime or latency—representing only **0.12%** of the overall traffic during the attack.
- **AI-Driven Security:** Real-time behavioral analysis delivered **highly accurate mitigation**, without false positives.
- **Future-Proof Protection:** The system **continuously learns**, strengthening defences against emerging threats.

This attack demonstrated the growing scale and sophistication of Web DDoS threats targeting financial institutions. Traditional defenses are no longer sufficient—**only AI-driven solutions** with real-time adaptive capabilities can effectively counteract modern cyber threats.

With Radware's Web DDoS protection, this UAE bank **prevented a massive cyber-attack from turning into a catastrophe**, ensuring business continuity while reinforcing customer trust.

To learn more about how Radware Web DDoS and other solutions comprehensively protect your organization from sophisticated cyberattacks, contact us now.