MAZEBOLT

Case Study: Financial Services

European Bank chooses RADAR™ to prevent damaging DDoS attacks

Overview:

A European bank with over 4 million customers and average yearly revenues of €1.5 billion was recently hit by another DDoS attack. The bank has over 10,000 employees and places significant emphasis on open banking initiatives. Following the attack, it became clear that critical online banking and third-party financial services were at a high risk.

The Challenge:

The bank has always been a target for DDoS attacks, and in recent years, political hacktivist groups have made it a prime target, successfully causing significant downtime and damages. Every time a DDoS attack penetrated the bank's defenses, the following services were affected: online and mobile banking, proprietary trading platform, VPN services, and centralized security management systems.

The bank couldn't afford any more disruption to services and transactions, as they caused financial losses, higher cyber insurance costs, and harming its reputation. Additionally, the primary Security Operations Center (SOC) team were concerned about the lack of real-time management of security systems from.

The bank heavily invested in a hybrid DDoS protection strategy, including Scrubbing Centres, on-premises equipment, and WAF, but still suffered downtime; They decided to optimize its mitigation stack and contacted MazeBolt.

The Banking DDoS Threat

- Unavailability of critical online banking services for customers, including online banking, mobile banking, and trading platforms
- Inaccessibility of third-party connected applications.
- Inability to connect remotely: Employees and branches.
- Lack of visibility to DDoS vulnerability for the bank's online environment

THE SOLUTION:

Following a short POC, RADAR uncovered DDoS misconfiguration vulnerabilities in layers 3,4, and 7 - while keeping online services operational with no disruption and no maintenance periods. The bank's cybersecurity team realized that these vulnerabilities would again lead to damaging attacks and bring critical services down when attacked again.

RADAR was deployed in two of the bank's primary data centers and uncovered the following:

> Over 1,500 DDoS vulnerabilities > 57% of DDoS vulnerability level across layers 3, 4, and 7 > Automated DDoS protection was only 43% effective > DDoS protection policies were not customized, leaving the bank highly vulnerable to future DDoS attacks

MAZEBOLT

RADAR provided a prioritized configuration vulnerability report with a roadmap to remediate and close risks. Working with MazeBolt's Professional Services (PS) team, the bank was able to gain critical visibility into its DDoS protection misconfigurations and vulnerabilities, per security layer - Scrubbing Center, CPE, and WAF.

The actionable remediation plan, generated automatically after each cycle of RADAR testing, enabled MazeBolt's PS team to continuously focus on attack vectors that affected the majority of the bank's external facing targets: sophisticated Layer 7 attacks, Slowloris, UDP, and DNS attack vectors - all presenting the greatest risk to the bank's environment and critical services' uptime.

THE BENEFITS:

RADAR delivered the following results:

- Automated DDoS protection was improved by over 120%: from 43% to over 95%.
- The bank has eliminated operational downtime and the need for damaging time-to-mitigation (TTM) SLAs and emergency response scenarios
- The bank received a reduction in cyber insurance
- Over 1500 DDoS vulnerabilities were identified and more than 1100 were eliminated (79%) in less than three months - without maintenance periods.
- Currently, the DDoS vulnerability level has dropped from 57% to less than 5%

The bank continues to be targeted by threat actors, but all DDoS attacks have been mitigated automatically without any damaging downtime since RADAR was deployed.

Continuous RADAR testing and remediation provide the bank with the necessary insight and data to protect new services and block DDoS attacks automatically. The bank has adopted the new approach to DDoS security with RADAR: Preventative, Proactive, Automated Protection.

> MazeBolt RADAR helped us ensure business continuity, through identifying and remediating vulnerabilities. We have gained ongoing insight into our automated DDoS protection. RADAR has enabled us to reliably provide online banking services to our customers even when under attack.
>
> CISO, European Bank

MazeBolt is pioneering a new standard in DDoS security. RADAR™, an industry-first patented solution, empowers organizations to identify and remediate vulnerabilities in every layer of DDoS protection. Global enterprises, including financial services, insurance, gaming, and high-security government environments, rely on MazeBolt to prevent damaging DDoS attacks.