EMEA Multinational Banking Group Turns to Radware to Stop Ransom, Burst and Encrypted Attacks in Their Tracks

CHALLENGES

This financial services company became the target of an increasing array of Burst attacks, multivector campaigns and ransom-based attacks following rapid growth.

SOLUTION

Radware DefensePro was implemented, in addition to Cloud DDoS Protection Service, DefenseSSL and ERT Active Attackers Feed.

WHY RADWARE

Radware was primarily selected for its machine-learning capabilities that allow attack signatures and security policies to be automatically created and because it offered a fully integrated hybrid offering for on-premise and cloud-based protection.

Overview

This EMEA-based financial services company is the oldest bank in its respective country and a leading provider of financial services to organizations of all sizes throughout the region. Because of its success, public visibility and growth, in recent years, this banking conglomerate has become the target of an increasing array of cyberattacks and ransom threats.

Challenges

Ransom-based attacks have been a growing threat targeting the financial services industry for some time, and this company was no exception. The company was receiving ransom threats from both the Armada Collective and Lizard Squad. Most ransom notes would be followed by a teaser flood attack to validate and underscore the threat.

In addition, attackers were relying increasingly on “hit and run” Burst assaults that included UDP fragmented and DNS reflective attacks as well as longer multivector attack campaigns that would start relatively small (only 2–3 Gbps) but would last hours and gradually evolve across multiple vectors.

Finally, the geographic location of this financial services organization has implications on both the organization's ability to protect itself from cyberattacks (in terms of latency in times of diversion) and the hackers' ability to use volumetric attacks. Hackers are unable to force large volumes of attack traffic through local networks due to limited bandwidth.

The Solution: Radware Tailors a Bespoke Solution

The bank went to market and evaluated a number of DDoS mitigation vendors, but ultimately Radware's on-premise DDoS mitigation appliance, DefensePro, was selected for a multitude of reasons, in addition to a series of other products and services.

- While testing a DDoS mitigation solution that leveraged rate-limiting technology, the bank discovered that using behavioral analysis provided a significant advantage since it doesn't block legitimate traffic, allowing the bank to maintain service levels and business continuity even during an attack.
- The ability to develop attack signatures in real time allows Radware to mitigate attacks in as little as 20 seconds. Traffic patterns during the day are heavier, which limit the time allowed to analyze and adjust behavioral traffic patterns throughout the day.
- Tight integration between Radware's on-premise appliances and cloud-based scrubbing centers. This allows the bank to maintain identical baselines between its perimeter defenses and Radware's scrubbing centers, so attacks are mitigated faster than other solutions that must reanalyze traffic once it is redirected to the cloud, require additional manual tuning, or both.
- Support by cybersecurity experts in the form of Radware's Emergency Response Team (ERT). This allows the bank's network team to focus on daily tasks and doesn't require the bank to have in-depth expertise. The ERT's level of expertise of various attack vectors and strategies was considered critical to maintaining business continuity.

The bank's network team preferred not to employ any form of Border Gateway Protocol on-ramping or off-ramping. This was supported by Radware and was a key competitive differentiator. Radware's Cloud DDoS Protection Services was employed since it could be deployed out of path, so the bank's IT security team only engages with larger attacks that cross certain bandwidth thresholds. Despite establishing this threshold, shorter, low-bandwidth attacks (such as those associated with Burst attacks) are still detected and mitigated thanks to Radware's behavioral analysis capabilities, allowing the bank to get the best of both worlds.

Bigger and Better

Less than a year after its initial implementation, this financial services company upgraded its DefensePro units for advanced protection against a new wave of IoT botnet, DNS and Burst attacks. Specifically, DNS Water Torture and DNS Reflection/Amplification attacks required updated behavioral-based detection and real-time signature creation that could automatically understand DNS traffic behavior.

In addition, the bank now takes advantage of Radware's DefenseSSL module, which supports all common versions of SSL and TLS and protects against all forms of encrypted attacks, including TCP SYN Floods, SSL Negotiation, HTTPS Floods and encrypted web attacks. Because DefenseSSL supports asymmetric deployment where only ingress traffic is processed and flows through the solution, the bank can leverage it in cloud-based deployments, such as Radware's Cloud DDoS Protection Services and scrubbing centers. In addition, processing only inbound traffic minimizes latency on network traffic.

Finally, the bank subscribed to Radware's ERT Active Attackers Feed, a threat intelligence feed that identifies and blocks IP addresses in real time to offer pre-emptive protection. This service complements the bank's in-house cybersecurity expertise by providing threat intel from Radware's Cloud Security Services and Global Deception Network to allow this financial institution to "know its enemies."

The ERT attacker feed was able to block a bad actor who knew exactly what to target on the backend of our banking app"

– Senior Network Architect, EMEA multinational bank

Benefits

Over the past year, this financial services company has successfully maintained business continuity and service availability despite experiencing a four-fold increase in Burst attacks. This has also included an increase in multivector attack campaigns. One such assault leveraged small (only 2–3 Gbps) attacks but lasted over four hours and gradually evolved in several stages. It then evolved into attacks on 16,000 SYN connections, which were mitigated via Radware DefensePro. After the SYN attack, an HTTP Flood leveraging over 2,000 sources was used, which was also successfully mitigated.

Ransom threats by groups such as the Armada Collective and Lizard Squad have been proactively mitigated upon receiving ransom notes. A ransom email from the Armada Collective was quickly followed by a teaser attack that the bank detected and mitigated. This flood attack was detected and immediately network traffic was diverted to Radware's local scrubbing center for cleanup.

As a precaution, when we receive a flood attack and ransom note, we divert network traffic to the Radware scrubbing center before the payment deadline. It sends a clear message to ransom groups: we won't be victimized."

– Senior Network Architect, EMEA multinational bank